

CA Database Management Solutions for IMS for z/OS

Installation Guide

Version 15.0.00, Fifth Edition

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the "Documentation") is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2013 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

CA Technologies Product References

This document references the following CA Technologies products:

- CA Compress™ Data Compression for IMS (CA Compress Data Compression for IMS)
- CA Database Analyzer for IMS™ for IMS for z/OS (CA Database Analyzer for IMS)
- CA Database Copier™ for IMS for z/OS (CA Database Copier)
- CA Database Organizer™ for IMS for z/OS (CA Database Organizer)
- CA Datacom®/AD (CA Datacom/AD)
- CA Datacom®/DB (CA Datacom/DB)
- CA Dataquery™ for CA Datacom® (CA Dataquery for CA Datacom)
- CA High Performance Recovery for IMS for z/OS (CA High Performance Recovery)
- CA Mainframe Configuration Manager for IMS for z/OS (CA Mainframe Configuration Manager)
- CA Mainframe Extended Terminal Manager for IMS for z/OS (CA Mainframe Extended Terminal Manager)
- CA Mainframe Program Restart Manager for IMS for z/OS (CA Mainframe Program Restart Manager)
- CA Chorus™ Software Manager (CA MSM)
- CA Secondary Index for IMS for z/OS (CA Secondary Index)
- CA Secondary Index Builder for IMS for z/OS (CA Secondary Index Builder)

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

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

Documentation Changes

The following documentation updates have been made in the fifth edition of this guide:

- [CA Compress Data Compression for IMS Customization](#) (see page 118)—Added a limitation note about Compress/2.

The following documentation updates have been made in the fourth edition of this guide:

- [Software Requirements](#) (see page 18)—Added the IBM z/OS 2.1.
- [Resolve Multiple IMS Partner Product User Exits](#) (see page 65)—Added this new procedure.
- [How to Enable Online Reorg Processing in CA Database Organizer](#) (see page 70)—Added the step for resolving multiple IMS partner product user exits.
- [Customize Each IMS where CA Mainframe Extended Terminal Manager Will Be Used](#) (see page 102)—Added the step for resolving multiple IMS partner product user exits.
- [CA Compress Data Compression for IMS Customization](#) (see page 118)—Changed the step for enabling compression support for a non-IMS environment to mandatory.
- [Enable Compression Support for a Non-IMS Environment](#) (see page 125)—Changed this step to mandatory.
- [Sample Parameter Library Member Names](#) (see page 160)—Added the DSAPARMS and HPOREORG global parameter members.

The following documentation updates have been made in the third edition of this guide:

- [Software Requirements](#) (see page 18)—Updated the z/OS requirements to 1.12 and 1.13.
- The Apply IBM APARs topic has been removed.

The following documentation updates have been made with the second edition of this documentation:

- [Create Bypass Table](#) (see page 111)—Updated to describe more granular options for excluding objects from CA Mainframe Program Restart Manager processing.

The following documentation updates have been made since the last release of this documentation:

- [Software Requirements](#) (see page 18)—Added support for IMS V12, IBM z/OS version requirements, and to CA Datacom/AD r12.
- [Storage Requirements](#) (see page 21)—Added requirements for the CA Transaction Management Solutions for IMS for z/OS.
- [Installing Your Product Using CA MSM](#) (see page 27)—Updated for new CA MSM release requirements.
- [Prepare the SMP/E Environment for Pax Installation](#) (see page 50)—Updated member names to comply with new standards:
 - SEDIT to IMTSEEDIT
 - SMPALLOC to IMT1ALL
 - SMPECSI to IMT2CSI
- [Run the Installation Jobs for a Pax Installation](#) (see page 52)—Updated member names to comply with new standards:
 - SEDIT to IMTSEEDIT
 - ESDRECD to IMT3RECD
 - SMPEAPP to IMT4APP
 - SMPEACC to IMT5ACC
- [Apply Maintenance](#) (see page 53)—New topic that references new tape members for maintenance:
 - IMT6RECP (receive downloaded PTF packages)
 - IMT7APYP (apply downloaded PTF packages)
 - IMT8ACCP (accept downloaded PTF packages)
- [Prepare the SMP/E Environment for Tape Installation](#) (see page 59)—Updated member names to comply with new standards:
 - SEDIT to IMTSEEDIT
 - SMPALLOC to IMT1ALL
 - SMPECSI to IMT2CSI
- [Run the Installation Jobs for a Tape Installation](#) (see page 60)—Updated member names to comply with new standards:
 - SEDIT to IMTSEEDIT
 - SMPEREC to IMT3RECT
 - SMPEAPP to IMT4APP
 - SMPEACC to IMT5ACC

- The following sections have been added to describe how to customize newly implemented products:
 - [CA Mainframe Configuration Manager Customization](#) (see page 73)
 - [CA Mainframe Extended Terminal Manager Customization](#) (see page 99)
 - [CA Mainframe Program Restart Manager Customization](#) (see page 107)
 - [CA Compress Data Compression for IMS Customization](#) (see page 118)
 - [Command Control Manager Customization](#) (see page 126)
- [DISPLAY ACTIVE Command](#) (see page 152)—Updated to reflect the extended use.
- [Set Up the IIR Historical Reporting Application](#) (see page 170)—New procedure that describes how to set up the IIR ISPF application.

Contents

Chapter 1: Overview 13

Audience	13
How the Installation Process Works	14

Chapter 2: Preparing for Installation 17

Hardware Requirements	17
Software Requirements	18
CA Mainframe Extended Terminal Manager Software Requirements	18
Snapshot General Services Software Requirements	18
CA Common Services Requirements	19
LMP Key Requirements	19
Security Requirements	19
APF Authorization Requirements	20
UNIX System Services (USS) Security Requirements	20
BMP Pause ITK STC PPT Entry	20
Storage Requirements	21
UNIX System Services (USS) File Space	21
Target and Distribution Libraries	22
Other Requirements	22
IMS Version Requirements	23
ITK STC Dispatching Priority	23
Health Checks	23
Data Set Naming Conventions	24
HALDB Database Considerations	25
IMS Physical Logger Replacement	25
Concurrent Releases	25

Chapter 3: Installing Your Product Using CA MSM 27

How to Use CA MSM: Scenarios	27
How to Acquire a Product	27
How to Install a Product	28
How to Maintain Existing Products	29
How to Deploy a Product	30
How to Configure a Product	31
Access CA MSM Using the Web-Based Interface	32

Chapter 4: Installing Your Product from Pax-Enhanced ESD 33

How to Install a Product Using Pax-Enhanced ESD	33
How the Pax-Enhanced ESD Download Works	35
ESD Product Download Window	35
USS Environment Setup	38
Allocate and Mount a File System	39
Copy the Product Pax Files into Your USS Directory	42
Download Using Batch JCL	43
Download Files to Mainframe through a PC	46
Create a Product Directory from the Pax File	47
Sample Job to Execute the Pax Command (Unpackage.txt)	48
Copy Installation Files to z/OS Data Sets	48
How to Install Products Using Native SMP/E JCL	49
Prepare the SMP/E Environment for Pax Installation	50
Run the Installation Jobs for a Pax Installation	52
Clean Up the USS Directory	52
Apply Maintenance	53
HOLDDATA	54

Chapter 5: Installing Your Product from Tape 57

Unload the Sample JCL from Tape	58
How to Install Products Using Native SMP/E JCL	59
Prepare the SMP/E Environment for Tape Installation	59
Run the Installation Jobs for a Tape Installation	60
Apply Maintenance	61
HOLDDATA	62

Chapter 6: Starting Your Product 63

How to Configure Without CA MSM	63
How to Enable Environment Specific Product Customizations	63
Create Library Data Set Name Aliases for the CA Database Management Solutions for IMS	64
Resolve Multiple IMS Partner Product User Exits	65
How to Implement the ISPF Interface for CA Database Management Solutions for IMS for z/OS	66
CA Database Analyzer for IMS Customization	68
CA Database Copier Customization	68
CA Database Organizer Customization	69
CA High Performance Recovery Customization	72
CA Mainframe Configuration Manager Customization	73
CA Mainframe Extended Terminal Manager Customization	99
CA Mainframe Program Restart Manager Customization	107

CA Compress Data Compression for IMS Customization	118
Command Control Manager Customization	126
Preparing to Start CA Database Management Solutions for IMS for z/OS.....	138
Verify the Installation.....	138
ITK STC Started Task Considerations	139
BMP Pause and Resume Functionality.....	156

Appendix A: Global Parameter Processing 157

Global Parameters.....	157
How Global Parameter Processing Works.....	157
How To Activate Global Parameter Processing	159
Customize Global Parameter Members	159
Assemble the DFSMDA for the Parmlib	161

Appendix B: Installing the IMS Information Repository 163

IMS Information Repository	163
How To Install IIR.....	164
How To Install the CA Datacom/AD Environment.....	164
How To Install the IIR Database	165
Start the CA Datacom/AD Environment.....	166
Define the IIR Database and Tables	166
Catalog the IIR Database and Tables.....	167
Initialize the Data Areas and Prepare the IIR Tables	168
Back Up the CA Datacom/AD Environment	168
Stop the CA Datacom/AD Environment	169
Add New Tables to an Existing IIR Installation	169
Set Up the IIR Historical Reporting Application.....	170
How To Establish a Data Sharing Environment	171

Appendix C: Using Snapshot General Services 173

Snapshot Overview	173
Initialize Snapshot General Services.....	174
Reinitialize Snapshot General Services.....	175
IBM Shark and Hitachi Data Systems Devices	175
Determine Whether a Device is FlashCopy II-Compatible	176
Initialization Parameters	176
Parameter Statements	178
BCVGROUP Statement	178
DSNGROUP Statement	179
VOLGROUP Statement	181

OPTIONS Statement	183
Appendix D: Snapshot General Services Health Checks	187
DB2_TGR_CHECK_FCII_DEVS@xmanxxxx	187
Appendix E: Snapshot General Services Health Checks	189
DB2_TGR_CHECK_FCII_DEVS@xmanxxxx	189
Appendix F: CA Database Organizer Health Checks	191
IMST_ITK_STC_ABEND@jobname	191
Chapter 7: Index	193

Chapter 1: Overview

This guide describes how to install and implement CA Database Management Solutions for IMS for z/OS.

This section contains the following topics:

Audience.....

How the Installation Process Works.....

Audience

This guide is meant for database administrators or systems programmers that perform mainframe installations. Readers of this guide should have knowledge in the following areas:

- JCL
- TSO/ISPF
- IMS for z/OS
- z/OS environment and installing software in this environment
- Your organization's IT environment, enterprise structure, and region structure

You may need to work with the following personnel:

- Systems programmer for z/OS and VTAM definitions
- Storage administrator, for DASD allocations
- Security administrator for access to installation data sets

How the Installation Process Works

CA Technologies has standardized product installations across all mainframe products. Installation uses the following process:

- Acquisition—Transports the software to your z/OS system.
- Installation using SMP/E—Optionally creates a CSI environment and runs the RECEIVE, APPLY and ACCEPT steps. The software is untailored.
- Deployment—Copies the target libraries to another system or LPAR.
- Configuration—Creates customized load modules, bringing the software to an executable state.

CA MSM provides a web-based interface to make the standardized installation process easier. Using CA MSM, someone with limited knowledge of JCL and SMP/E can install a product.

Note: If you do not have CA MSM, you can download it from the Download Center at [the CA Support Online website](#). Follow the installation instructions in the CA Mainframe Software Manager documentation bookshelf on the CA Mainframe Software Manager product page. The standardized installation process can also be completed manually.

To install your product, do the following tasks:

1. Prepare for the installation by [confirming that your site meets all installation requirements](#) (see page 17).
2. Use one of the following methods to acquire the product:
 - [Download the software from CSO using CA MSM](#) (see page 27).
 - [Download the software from CSO using Pax-Enhanced Electronic Software Delivery \(ESD\)](#) (see page 33).
 - Order a tape or a DVD.
3. Perform an SMP/E installation using one of the following methods:
 - If you used CA MSM to acquire the product, start the SMP/E step from the SMP/E Environments tab in CA MSM.
 - If you used ESD to acquire the product, you can install the product in the following ways:
 - Install the product manually.
 - Use the Insert New Product option in CA MSM to complete the SMP/E installation.
 - If you used a [tape](#) (see page 57) or DVD, install the product manually.

Note: If a CA Recommended Service (CA RS) package is published for your product, install it before continuing with deployment.

4. Deploy the target libraries using one of the following methods:
 - If you are using CA MSM, deployment is required; it is a prerequisite for configuration.
 - If you are using a manual process, deployment is an optional step.

Note: Deployment is considered part of [starting your product](#) (see page 63).

5. Configure your product using CA MSM or manually.

Note: Configuration is considered part of [starting your product](#) (see page 63).

Chapter 2: Preparing for Installation

This section describes what you need to know and do before you install the product.

This section contains the following topics:

- Hardware Requirements
- Software Requirements.....
- CA Common Services Requirements
- LMP Key Requirements
- Security Requirements
- Storage Requirements
- Other Requirements
- Concurrent Releases.....

Hardware Requirements

Snapshot General Services supports the following series of devices:

- IBM Shark 2105 ESS and 2107 ESS
- IBM Shark DS6000 and DS8000
- EMC Symmetrix
- Hitachi Data Systems 9990V and USP V
- Sun Storage Tek 9990V
- HP StorageWorks XP20000 and XP24000

Note: The IBM, Hitachi Data Systems, Sun Storage Tek, and HP StorageWorks devices come in two versions: FlashCopy I and FlashCopy II. FlashCopy II is more flexible, which helps reduce the amount of overall DASD needed and operational complexity. We recommend using the FlashCopy II version of these devices if possible.

Software Requirements

The following software is required for the CA Database Management Solutions for IMS for z/OS:

- IMS V10, V11, or V12

Note: For the most current IMS version support information, see [IMS Compatibilities](#) on CA Support Online.

- IBM z/OS 1.12, 1.13, or 2.1

Note: For the most current operating system support information see [Database Management z/OS Release Compatibilities](#) on CA Support Online.

- CA Datacom/AD r12 for the IMS Information Repository (IIR) component

Additional software requirements exist for CA Mainframe Extended Terminal Manager and Snapshot General Services.

CA Mainframe Extended Terminal Manager Software Requirements

If you perform CA Mainframe Extended Terminal Manager setup and customization by using the online transaction (EMTRAN) or the batch update utility (ETMUD1U0), the 3270 emulator on your PC must be set to use the US code page. This emulator setting is necessary because the hex values that the other code pages use for wildcards are different from the hex values that the US code page uses.

Snapshot General Services Software Requirements

Additional software requirements exist for some devices to be used with Snapshot General Services:

- Hitachi Data Systems and Sun Storage Tek devices require the Hitachi Compatible Mirroring for IBM FlashCopy feature.
- HP StorageWorks devices require HP StorageWorks XP for FlashCopy Mirroring.
- EMC Symmetrix DMX devices may need additional maintenance applied. If you are running V5.2 or V5.3, apply maintenance PTFs as needed for the resource pack library and base. V5.4 of the resource pack base does not have these requirements.

Note: If CAIRIM is used to initialize Snapshot General Services, ensure that all related maintenance has been applied to ensure correct parameter parsing. Otherwise, TGRPAR011E messages may be received on valid parameters.

Extended Address Volumes (EAV) are supported for FlashCopy II devices.

CA Common Services Requirements

The following CA Common Services are used with CA Database Management Solutions for IMS for z/OS:

- CAIRIM
- CA LMP

Note: If other CA Technologies products are installed at your site, some of these services are already installed.

LMP Key Requirements

The CA License Management Program (CA LMP) tracks licensed software in a standardized and automated way. CA LMP uses common real-time enforcement software to validate the user configuration. CA LMP reports on activities related to the license, usage, and financials of CA Technologies products.

The CA Database Management Solutions for IMS for z/OS are licensed with an LMP key. You acquire the LMP key with one of the following methods:

- From your product media
- With Pax ESD
- From CA Support at <http://ca.com/support>

Note: For more information about LMP keys, see the CA Common Services for z/OS documentation.

Security Requirements

Review the security requirements for the following areas:

- Library authorization
- IMS version considerations
- UNIX System Services (USS) requirements
- BMP Pause ITK STC PPT entry

APF Authorization Requirements

The CA Database Management Solutions for IMS for z/OS require APF authorization to run. The CA Database Management Solutions for IMS for z/OS load library (CMTLOAD) and all other libraries concatenated in STEPLIB must also be APF-authorized. The only exception is the Application Program Interface (API) mode in CA Database Organizer.

UNIX System Services (USS) Security Requirements

To download pax files for the SMP/E installation as part of the Pax-Enhanced ESD process, you must have write authority to the UNIX System Services (USS) directories used for the ESD process.

BMP Pause ITK STC PPT Entry

The BMP Pause component of the ITK STC has hooks in all IMS systems on which it is requested to operate. Therefore, the STC must have as much protection as possible from outside intervention. Canceling it can lead to ABENDs in IMS control and dependent regions.

Instead of canceling the ITK STC, use the z/OS STOP command as follows:

```
/P stcname
```

If dependent regions are left in a paused state, use the following z/OS MODIFY command to resume them:

```
/F stcname,RES
```

We strongly recommend that the ITK STC be protected through the setting up of a PPT entry as follows that marks its jobstep program as noncancelable:

```
PPT PGMNAME(HPOINIT)
      NOCANCEL
      KEY(8)
      NOSWAP
      NOPRIV
      SYST
      DSI
      PASS
      AFF(NONE)
      NOPREF
```

Storage Requirements

Ensure that you have the following storage available for the CA Database Management Solutions for IMS for z/OS:

- If installing with CA MSM or ESD, 27,530 tracks or 1838 cylinders with the following allocations:
 - 206 cylinders for the downloaded files
 - 206 cylinders to create the REL files
 - 1426 cylinders for target, distribution, and SMP/E files

Note: This total does not include the data sets that are created as part of post-install processing. 6,152 tracks of data will be deleted after the install completes.

Verify that the following storage is available for installation and setup of the CA Mainframe Transaction Management Solutions for IMS:

- Installation (Target/Dlib)—43 cylinders
- SMP/E libraries—684 cylinders
- Download files—10 cylinders
- Temporary SMP/E files—30 cylinders

Snapshot General Services requires approximately 275 KB in 31-bit CSA.

UNIX System Services (USS) File Space

To download pax files for the SMP/E installation as part of the Pax-Enhanced ESD process, you must have enough UNIX System Services (USS) file space available before you start the installation process using ESD. You need approximately 3.5 times the pax file size in free space.

If you do not have sufficient free space, you receive error message EDC5133I.

Target and Distribution Libraries

The target and distribution libraries have changed to conform to new CA packaging standards with CA MSM. The lowest data set level qualifier of the installed data sets has changed as noted in the following table:

Old Target	Old Distribution	New Target	New Distribution
CLIST	ACLIST	CIMTCLSO	AIMTCLSO
LOADLIB	n/a	CIMTLOAD	n/a
n/a	AOBJLIB	n/a	AIMTMOD0
PARMLIB	APARMLIB	CIMTPARM	AIMTPARM
SAMPLIB	ASAMPLIB	CIMTSAMP	AIMTSAMP
SPFHLIB	ASPFHLIB	CIMTPNLO	AIMTPNLO
SPFMLIB	ASPFMLIB	CIMTMSG0	AIMTMSG0
SPFPLIB	ASPFPLIB	CIMTPNLO	AIMTPNLO
SPFSLIB	ASPFSLIB	CIMTSKLO	AIMTSKLO
		CDBALOAD	ADBALOAD
		CDBAPARM	ADBAPARM
		CDBASRC	ADBASRC

Note: Use the [INSALIAS](#) (see page 64) job provided in *high-level.CIMTSAMP* to create library data set name aliases. This job creates aliases relating the old and new library names that have changed in this release to conform to new CA Technologies packaging standards.

Other Requirements

Review the following requirements:

- [IMS version requirements](#) (see page 23)
- [ITK STC dispatching priority](#) (see page 23)
- [CA Database Organizer health check](#) (see page 23)
- [Data set naming conventions](#) (see page 24)

- [HALDB database considerations](#) (see page 25)
- [IMS physical logger replacement](#) (see page 25)

IMS Version Requirements

You must concatenate the IMS SDFSRESL to the STEPLIB DD and allocate it under the DFSRESLB DD to execute the CA Database Management Solutions for IMS for z/OS.

If you are using the products in batch with IMS, perform the following steps:

1. Concatenate the load library ahead of the IMS SDFSRESL in STEPLIB.
2. Define a DFSRESLB DD that points at IMS SDFSRESL.

Note: Ensure SDFSRESL is APF-authorized.

ITK STC Dispatching Priority

The ITK STC must be set to run at as high a dispatching priority as possible to allow it to keep pace with updates coming in from IMS control regions.

Health Checks

CA Database Organizer and Snapshot General Services are now integrated with the IBM Health Checker for z/OS through the CA Health Checker Common Service, and automatically check for the following potential problems:

ITK_STC_ABEND@jobname

The ITK started task attaches many tasks on which work can be dispatched. It is critical that all tasks are available and running normally. This health check verifies that each subtask is running normally and that there are no abending tasks. When all subtasks are operating, the health check generates a message that indicates the ITK STC is operating normally and that there are no abending tasks.

DB2_TGR_CHECK_FCII_DEVS@xmanxxxx

The Snapshot General Services check looks for FlashCopy II-capable devices that are defined to Snapshot General Services as FlashCopy I devices. Redefining them as FlashCopy II devices can greatly reduce the number of needed disk volumes.

This check runs when XManager is initialized, and every time a Snapshot General Services subsystem is initialized or reinitialized.

More information:

IMST_ITK_STC_ABEND@jobname.....
DB2_TGR_CHECK_FCII_DEVS@xmanxxxx

Data Set Naming Conventions

During product installation, the term *high-level* denotes the node-names concatenated to the low-level data set name qualifier library name as shown in the following examples:

- Single high-level node-name (PROD concatenated to a load library):
PROD.CIMTLOAD
- Multiple high-level node-names (PROD.R12SP1.SMPE concatenated to a load library):
PROD.R12SP1.SMPE.CIMTLOAD

Use the following rules for assigning these values:

- SDM DATALVL and EXECLVL data sets can share the same high-level, but must be different from the SMP/E TARGET and TEMP high-level.
- SMP/E TARGET data sets high-level must be different than the SMP/E TEMP data sets high-level.

The following data set names reflect this convention:

PROD.R12SP1.SDM	SDM DATALVL and EXECLVL high-level
PROD.R12SP1.SMPE	SMP/E TARGET high-level
PROD.R12SP1.SMPE.TEMP	SMP/E TEMP high-level

Note: We recommend that you use the same high-level as SDM DATALVL and EXECLVL for the SAMPJCL data set.

HALDB Database Considerations

To run High Availability Large Databases (HALDB), make the following JCL changes, if necessary:

1. Use IMS DD to point to DBDLIB.
2. Add RECON DDs or dynamically allocate them.

IMS Physical Logger Replacement

A replacement for the IMS Physical Logger is now provided. This replacement improves batch performance of IMS jobs writing to the IEFDER and IEFDER2 data sets to buffered tape devices.

The following message appears when the replacement activates:

ITK9800I PHYSICAL LOGGER IS ACTIVE

If you do not want to use the IMS Physical Logger replacement, include a DD card for NOPLOG and set it to DUMMY in all affected JCL.

Concurrent Releases

You can install this release of CA Database Management Solutions for IMS for z/OS and continue to use an older release in another SMP/E CSI environment. If you plan to continue to run a previous release, consider the following points:

- When installing into an existing SMP/E environment, this installation deletes previous releases in that environment.
- If you acquired your product from tape or with Pax-Enhanced ESD, select different target and distribution zones for your new release from where your current release is installed. The new zones use different libraries than your current release.

Note: CA MSM installs into a new CSI by default.

- Define DDDEF entries in your new zones to point SMP/E to the proper libraries for installation. Ensure that they point to the new release libraries.

Chapter 3: Installing Your Product Using CA MSM

These topics provide information to get you started managing your product using CA MSM. You can use the online help included in CA MSM to get additional information.

Before using these topics, you must already have CA MSM installed at your site. If you do not have CA MSM installed, you can download it from the Download Center at [the CA Support Online website](#), which also contains links to the complete documentation for CA MSM.

How to Use CA MSM: Scenarios

Imagine that your organization has started using CA MSM to simplify the installation of CA Technologies products and unify their management. You have also licensed a new CA Technologies product. In addition, you have a number of existing CSIs from previously installed CA Technologies products.

You can use the following scenarios to guide you through the process:

1. [Acquire the new product](#) (see page 27).
2. [Install the new product](#) (see page 28).
3. [Maintain products already installed in your environment](#) (see page 29).
4. [Deploy the product to your target systems](#) (see page 30).
5. [Configure the deployed product to your target systems](#) (see page 31).

How to Acquire a Product

The *Product Acquisition Service (PAS)* facilitates the acquisition of mainframe products and the service for those products, such as program temporary fixes (PTFs). PAS retrieves information about products to which your site is entitled. Then it records these entitlements in a software inventory that is maintained on your driving system.

You can use the PAS component of CA MSM to acquire a CA Technologies product.

Follow these steps:

1. Set up a CA Support Online account.

To use CA MSM to acquire or download a product, you must have a CA Support Online account. If you do not have an account, you can create one on [the CA Support Online website](#).

2. Determine the CA MSM URL for your site.

To [access CA MSM](#) (see page 32), you require its URL. You can get the URL from your site's CA MSM administrator and log in using your z/OS credentials. When you log in for the first time, you are prompted to create a CA MSM account with your credentials for [the CA Support Online website](#). This account enables you to download product packages.

3. Log in to CA MSM and go to the Software Catalog page to locate the product that you want to manage.

After you log in to CA MSM, you can see the products to which your organization is entitled on the Software Catalog tab.

If you cannot find the product you want to acquire, update the catalog. CA MSM refreshes the catalog through [the CA Support Online website](#) using the site IDs associated with your credentials for [the CA Support Online website](#).

4. Download the product installation packages.

After you find your product in the catalog, you can download the product installation packages.

CA MSM downloads (acquires) the packages (including any maintenance packages) from the CA FTP site.

After the acquisition process completes, the product is ready for you to install or maintain.

How to Install a Product

The *Software Installation Service (SIS)* facilitates the installation and maintenance of mainframe products in the software inventory of the driving system. This facilitation includes browsing downloaded software packages, managing SMP/E consolidated software inventories on the driving system, and automating installation tasks.

You can use the SIS component of CA MSM to install a CA Technologies product.

Follow these steps:

1. Initiate product installation and review product information.
2. Select an installation type.
3. Review installation prerequisites if any are presented.

4. Take *one* of the following steps to select an SMP/E environment:
 - Create an SMP/E environment:
 - a. Set up the global zone.
 - b. Create a target zone.
 - c. Create a distribution zone.
 - Use an existing SMP/E environment from your working set:
 - a. Update the global zone.
 - b. Set up the target zone: Either create a target zone or use an existing target zone.
 - c. Set up the distribution zone: Either create a distribution zone or use an existing distribution zone.
5. Review the installation summary and start the installation.

Note: If you install a product or its components into an existing target or distribution zone, older versions are deleted from the zone and associated data sets. We recommend that you use new target and distribution zones for this installation so that you can apply maintenance to your current version, if necessary.

After the installation process completes, check for and install available product maintenance. The product is ready for you to deploy. Sometimes there are other steps to perform manually outside of CA MSM before beginning the deployment process.

How to Maintain Existing Products

If you have existing CSIs, you can bring those CSIs into CA MSM so that you can maintain all your installed products in a unified way from a single web-based interface.

You can use the PAS and SIS to maintain a CA Technologies product.

Follow these steps:

1. Migrate the CSI to CA MSM to maintain an existing CSI in CA MSM.
During the migration, CA MSM stores information about the CSI in the database.
2. Download the latest maintenance for the installed product releases from the Software Catalog tab.

If you cannot find a release (for example, because the release is old), you can add the release to the catalog manually and then update the release to download the maintenance.

3. Apply the maintenance.

Note: You can also install maintenance to a particular CSI from the SMP/E Environments tab.

After the maintenance process completes, the product is ready for you to deploy. You may have to perform other steps manually outside of CA MSM before beginning the deployment process.

How to Deploy a Product

The *Software Deployment Service (SDS)* facilitates the mainframe product deployment from the software inventory of the driving system to the target system. This facilitation includes deploying installed products that are policy-driven with a set of appropriate transport mechanisms across a known topology.

You can use the SDS component of CA MSM to deploy a CA Technologies product that you have already acquired and installed.

Follow these steps:

1. Set up the system registry:
 - a. Determine the systems you have at your enterprise.
 - b. Set up remote credentials for those systems.
 - c. Set up the target systems (non-sysplex, sysplex or monoplex, shared DASD cluster, and staging), and validate them.
 - d. Add network information, including data destination information, to each system registry entry.

2. Set up methodologies.

3. Create the deployment, which includes completing each step in the New Deployment wizard.

After creating the deployment, you can save it and change it later by adding and editing systems, products, custom data sets, and methodologies, or you can deploy directly from the wizard.

Note: If you must deploy other products to the previously defined systems using the same methodologies, you must create a separate deployment.

4. Deploy the product, which includes taking a snapshot, transmitting to target, and deploying (unpacking) to your mainframe environment.

After the deployment process completes, the product is ready for you to configure. You may have to perform other steps manually outside of CA MSM before beginning the configuration process.

How to Configure a Product

The *Software Configuration Service (SCS)* facilitates the mainframe product configuration from the software inventory of the driving system to targeted z/OS operating systems.

You can use the SCS component of CA MSM to configure a CA Technologies product that you have already acquired, installed, and deployed.

Follow these steps:

1. Select a deployed product to configure from the Deployments tab to open the Create Configuration wizard.
2. Create the configuration, which includes completing each step in the Create Configuration wizard, including the following:
 - a. Define a configuration name and select a target system.
 - b. Select configuration functions and options.
 - c. Define system preferences.
 - d. Create target settings.
 - e. Select and edit resources.
3. Build the configuration. The last step of the Create Configuration wizard lets you build the configuration.
4. Implement the configuration. The implementation process in CA MSM is a step-by-step process that carefully guides you and provides detailed instructions to start, stop, and manage the steps of the implementation process.

After the configuration process completes, the product is ready for you to use. You may have to perform other steps manually outside of CA MSM.

Note: You cannot use CA MSM to configure a product to a staging system.

Access CA MSM Using the Web-Based Interface

You access CA MSM using the web-based interface. Obtain the URL of CA MSM from the CA MSM administrator.

Follow these steps:

1. Start your web browser, and enter the access URL.

The login page appears.

Note: If the Notice and Consent Banner appears, read and confirm the provided information.

2. Enter your z/OS login user name and password, and click the Log in button.

The initial page appears. If you log in for the first time, you are prompted to define your account on [the CA Support Online website](#).

Note: For more information about the interface, click the online help link at the top right corner of the page.

3. Click New.

You are prompted for the credentials to use on [the CA Support Online website](#).

Important! The account to which the credentials apply *must* have the Product Display Options set to BRANDED PRODUCTS. You can view and update your account preferences by logging into [the CA Support Online website](#) and clicking My Account. If you do not have the correct setting, you are not able to use CA MSM to download product information and packages.

4. Specify the credentials, click OK, and then click Next.

You are prompted to review your user settings.

Note: These settings are available on the User Settings page.

5. Change the settings or keep the defaults, and then click Finish.

A dialog shows the progress of the configuration task. You can click Show Results to view the details of the actions in a finished task.

Important! If your site uses proxies, review your proxy credentials on the User Settings, Software Acquisition page.

Chapter 4: Installing Your Product from Pax-Enhanced ESD

This section contains the following topics:

How to Install a Product Using Pax-Enhanced ESD	33
Allocate and Mount a File System	39
Copy the Product Pax Files into Your USS Directory	42
Create a Product Directory from the Pax File	47
Copy Installation Files to z/OS Data Sets	48
How to Install Products Using Native SMP/E JCL	49
Clean Up the USS Directory	52
Apply Maintenance	53

How to Install a Product Using Pax-Enhanced ESD

This section describes the Pax-Enhanced ESD process. We recommend that you read this overview and follow the entire procedure the first time you complete a Pax-Enhanced ESD installation. For experienced UNIX users, the *Pax-Enhanced ESD Quick Reference Guide* has sufficient information for subsequent installations.

Important! Downloading pax files for the SMP/E installation as part of the Pax-Enhanced ESD process requires write authority to the UNIX System Services (USS) directories that are used for the ESD process.

If you prefer not to involve all CA Technologies product installers with z/OS UNIX System Services, assign a group familiar with USS to perform Steps 1 through 4 and provide the list of the unpacked MVS data sets to the product installer. USS is not required for the actual SMP/E RECEIVE of the product or for any of the remaining installation steps.

To install files using Pax-Enhanced ESD, use the following process:

1. Allocate and mount the file system. This process requires a USS directory to receive the pax file and to perform the unpack steps. We recommend that you allocate and mount a file system that is dedicated to Pax-Enhanced ESD and create the directory in this file system. Ensure that all users who will be working with pax files have write authority to the directory.

2. Copy the product pax files into your USS directory. To download files, choose one of the following options:

- Download a zip file from CA Support Online to your PC, unzip the file, and then upload the product pax files to your USS file system.
- FTP the pax files from CA Support Online directly to your USS directory.

Note: Perform Steps 3 through 6 for each pax file that you upload to your USS directory.

3. Create a product directory from the pax file. Set the current working directory to the directory containing the pax file, and create a directory in your USS directory by entering the following command:

```
pax -rvf pax-filename
```

4. Use the SMP/E GIMUNZIP utility to create z/OS installation data sets. The file UNZIPJCL in the directory that the pax command created in Step 3 contains a sample JCL to GIMUNZIP the installation package. Edit and submit the UNZIPJCL JCL.
5. Receive the SMP/E package. Use the data sets that GIMUNZIP created in Step 4. Perform a standard SMP/E RECEIVE using the SMPPTFIN and SMPHOLD (if applicable) DASD data sets. Also, specify the high-level qualifier for the RELFILES on the RFPREFIX parameter of the RECEIVE command.
6. Proceed with product installation. Consult product-specific documentation, including AREADME files and installation notes to complete the product installation.
7. (Optional) Clean up the USS directory. Delete the pax file, the directory that the pax command created, all of the files in it, and the SMP/E RELFILES, SMPMCS, and HOLDDATA data sets.

More Information:

USS Environment Setup.....	
Allocate and Mount a File System.....	
Copy the Product Pax Files into Your USS Directory	
Create a Product Directory from the Pax File.....	
Copy Installation Files to z/OS Data Sets	

How the Pax-Enhanced ESD Download Works

Important! To download pax files for the SMP/E installation as part of the Pax-Enhanced ESD process, you must have write authority to the UNIX System Services (USS) directories used for the ESD process and available USS file space before you start the procedures in this guide.

Use the following process to download files using Pax-Enhanced ESD:

1. Log in to <https://support.ca.com/>, and click Download Center.

The CA Support Online web page appears.

2. Under Download Center, select Products from the first drop-down list, and specify the product, release, and genlevel (if applicable), and click Go.

The CA Product Download window appears.

3. Download an entire CA Technologies product software package or individual pax files to your PC or mainframe. If you download a zip file, you must unzip it before continuing.

For both options, [The ESD Product Download Window](#) (see page 35) topic explains how the download interface works.

Note: For traditional installation downloads, see the *Traditional ESD User Guide*. Go to <https://support.ca.com/>, log in, and click Download Center. A link to the guide appears under the Download Help heading.

4. Perform the steps to install the product based on the product-specific steps.

The product is installed on the mainframe.

ESD Product Download Window

You can download CA Technologies product ESD packages multiple ways. Your choices depend on the size of the individual files and the number of files that you want to download. You can download the complete product with all components, or you can select individual pax and documentation files for your product or component.

The following illustration shows sample product files. The illustration lists all components of the product. You can use the Download Cart by selecting one or more components that you need, or selecting the check box for Add All to cart. If you prefer to immediately download a component, click the Download link.

CA Earl - MVS

- [Pax Enhanced Electronic Software Delivery \(ESD\) Guide](#)
- [Pax Enhanced Electronic Software Delivery \(ESD\) Quick Reference Guide](#)
- [Traditional Electronic Software Delivery \(ESD\) Guide](#)
- [Learn more about Using pkzip with your Downloaded Mainframe Products](#)
- [Learn more about downloading components of CA product](#)
- [Mounting ISO Images with OpenVMS](#)

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

Note: Related Published Solutions are available on the other results tab on this page. You must add these solutions to your Download Cart to include them with your product files for download.

[View Download Cart](#)

				☐ Add All to cart	
Product Components				Add to cart	Download
CCS - LEGACY - ESD ONLY 140000AW030.pax.Z	14.0 /0000	07/06/2011	4.89MB	☐	Download
CCS - MFNSM - ESD ONLY 140000AW040.pax.Z	14.0 /0000	07/06/2011	202.01MB	☐	Download
CCS - BASE - ESD ONLY 140001AW010.pax.Z	14.1 /0000	06/05/2012	27.44MB	☐	Download
CCS - OPTIONAL - ESD ONLY 140001AW020.pax.Z	14.1 /0000	06/05/2012	14.49MB	☐	Download
CA EARL PRODUCT PACKAGE 610106AEO00.pax.Z	6.1 /0106	10/30/2008	1.85MB	☐	Download
EARL PIPPACK AEO61010600.pdf	6.1 /0106	01/29/2010	93.92KB	☐	Download
CA EASYTRIEVE PRODUCT PACKAGE B60000ESA00.pax.Z	11.6 /0000	07/05/2011	6.12MB	☐	Download
DATACOM/AD PROD INFO PACKET CAIE00000P0.pdf	14.0 /0000	06/01/2012	220.53KB	☐	Download
DATACOM/AD XPRESS INSTALL				☐	Download

Figure 2: This illustration shows an example of a Product Component sample from CA Support online.

Clicking the link for an individual component takes you to the Download Method page.

Download Method

Please choose a download method to complete your download request. [Learn More](#)

HTTP via Download Manager

This is the CA recommended method for download. The Download Manager allows you to download your files faster and more efficiently.

[Download](#)

HTTP via Internet Browser

If Download Manager cannot be used or fails to start you may access your file(s) via your internet browser.

[View File Link\(s\)](#)

FTP

This method allows you to download your file(s) via FTP from CA's content delivery network or via native FTP servers.
Note: Processing is required and an email notification will be sent when your request is ready for downloading.

[FTP Request](#)

Figure 3: This illustration shows a sample Download Method window from CA Support Online.

Depending on the size and quantity of ordered product files, the Download Method screen could also have these options:

Note: For mainframe downloads using this HTTP method, click the Learn More link.

Download Method

Please choose a download method to complete your download request. [Learn More](#)

HTTP via Download Manager

This is the CA recommended method for download. The Download Manager allows you to download your files faster and more efficiently.

[Download](#)

Create a Zip File

This method allows you to bundle your download files into one or more zip files of up to 3.5 GB each. These zip files can then be downloaded via HTTP or FTP.
Note: Processing is required and an email notification will be sent when your request is ready for downloading.

[Create Zip](#)

FTP

This method allows you to download your file(s) via FTP from CA's content delivery network or via native FTP servers.
Note: Processing is required and an email notification will be sent when your request is ready for downloading.

[FTP Request](#)

Figure 4: This figure shows a sample Download Method window from CA Support Online.

The HTTP method lets you start downloading immediately. The FTP method takes you to the Review Orders page that displays your order, first in a Pending status changing to Ready when your order has been processed.

Preferred FTP uses the new content delivery network (CDN). Alternate FTP uses the CA Technologies New York-based FTP servers.

The Create a Zip File option first creates the zip, and when ready, offers the options that the Zip Download Request examples show in the next illustration.

Review Download Requests

Below is a list of the FTP and large HTTP downloads that have been requested by your site. When status is set to **'Ready'** a link will appear.

- For FTP requests, click on the FTP link to view the path information for your download. For more information view our [FTP Help document](#)
- For HTTP requests, click on the HTTP link to initiate your download.
- To view the details of your request, click on the desired order number.

Today's Downloads

Order #	Status	Description	Date Placed	Download Options
10000961	Ready	FTP Download Request	04/30/2010	Preferred FTP ▼ Alternate FTP ▼

Previous 6 day Download History

Order #	Status	Description	Date Placed	Download Options
10000949	Ready	ZIP Download Request	04/29/2010	HTTP via DLM Preferred FTP ▼ Alternate FTP ▼
10000948	Ready	ZIP Download Request	04/29/2010	HTTP via DLM Preferred FTP ▼ Alternate FTP ▼

Figure 5: This illustration shows a sample Review Download Requests window from CA Support online.

USS Environment Setup

You need a UNIX System Services (USS) directory and a file system with adequate space to perform the following tasks:

- Receive product pax files from CA Support Online.
- Perform utility functions to unpack the pax file into MVS data sets that you can use to complete the product installation.

We recommend that you allocate and mount a file system that is dedicated to Pax-Enhanced ESD. The amount of space that you need for the file system depends on the following variables:

- The size of the pax files that you intend to download.
- Whether you plan to keep the pax files after unpacking them. We do not recommend this practice.

We recommend that you use one directory for downloading and unpacking pax files. Reusing the same directory minimizes USS setup. You need to complete the USS setup only one time. You reuse the same directory for subsequent downloads. Alternatively, you can create a directory for each pax download.

Important! Downloading pax files for the SMP/E installation as part of the Pax-Enhanced ESD process requires write authority to the UNIX System Services (USS) directories that are used for the ESD process. The USS file system that is used for Pax-Enhanced ESD must have sufficient free space to hold the directory that the pax command created, and its contents. You need approximately 3.5 times the pax file size in free space to download the pax file and unpack its contents. For example, to download and unpack a 14 MB pax file, you need approximately 49 MB of free space in the file system hosting your ESD directory.

Allocate and Mount a File System

You can use the zSeries File System (zFS) or hierarchical file system (HFS) for ESD downloads.

This procedure describes how to perform the following tasks:

- Allocate a zFS or an HFS.
- Create a mount point in an existing maintenance USS directory of your choice.
- Mount the file system on the newly created mount point.

Note: You must have either SUPERUSER authority, or the required SAF profile setting to allow you to issue the USS mount command for the file system.

- Optionally, permit write access to anyone in the same group as the person who created the directory.

Important! USS commands are case-sensitive.

Follow these steps:

1. Allocate the file system by customizing one of the following samples to your site requirements:

- On a zFS, use the following sample:

```
//DEFINE EXEC PGM=IDCAMS
//SYSPRINT DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//AMSDUMP DD SYSOUT=*
//SYSIN DD *
  DEFINE CLUSTER ( +
    NAME(your_zFS_data_set_name) +
    STORAGECLASS(class) +
    LINEAR +
    CYL(primary secondary) +
    SHAREOPTIONS(3,3) +
  )
/*
//FORMAT EXEC PGM=IOEAGFMT,REGION=0M,
// PARM=(' -aggregate your_zFS_data_set_name -compat' )
//SYSPRINT DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//STDOUT DD SYSOUT=*
//STDERR DD SYSOUT=*
//CEEDUMP DD SYSOUT=*
/*
```

- On an HFS, use the following sample:

```
//ALCHFS EXEC PGM=IEFBR14
//CAESD DD DSN=yourHFS_data_set_name,
// DISP=(NEW,CATLG,DELETE),UNIT=3390,
// DSN TYPE=HFS,SPACE=(CYL,(primary,secondary),1)
```

The file system is allocated.

Note: Ensure that the zFS or HFS data set name that you use conforms to your data set naming conventions for USS file systems. If the allocation of the file system data set fails, it is because of environmental settings not allowing for the allocation. On an HFS, try using the ISPF 3.2 Data Set Utility to allocate your HFS data set.

2. Create a mount point for the file system. This example shows how to create a /CA/CAESD directory in an existing directory, /u/maint. From the TSO OMVS shell, enter the following commands:

```
cd /u/maint/  
mkdir CA  
cd CA  
mkdir CAESD
```

Note: This document refers to this structure as *yourUSSESDdirectory*.

The mount point is created.

3. Mount the file system by customizing one of the following samples to your site requirements:

- On a zFS, use the following sample:

```
MOUNT FILESYSTEM('your_zFS_data_set_name')  
      MOUNTPOINT('yourUSSESDdirectory')  
      TYPE(ZFS)  MODE(RDWR)  
      PARM(AGGROW)
```

- On an HFS, use the following sample:

```
MOUNT FILESYSTEM('your_HFS_data_set_name')  
      MOUNTPOINT('yourUSSESDdirectory')  
      TYPE(HFS)  MODE(RDWR)
```

The file system is mounted.

4. (Optional) Set security permissions for the directory. You can use the chmod command to let other users access the ESD directory and its files. For example, to allow write access to the ESD directory for other users in your USS group, from the TSO OMVS shell, enter the following command:

```
chmod -R 775 /yourUSSESDdirectory/
```

Write access is granted.

Note: For more information about the chmod command, see the IBM *z/OS UNIX System Services User Guide* (SA22-7802).

Copy the Product Pax Files into Your USS Directory

To begin the CA Technologies product installation procedure, copy the product pax file into the USS directory that you set up. Use one of the following methods:

- Download the product pax files directly from the CA Support Online FTP server to your z/OS system.
- Download the product pax file from the CA Support Online FTP server to your computer, and upload it to your z/OS system.
- Download the product file from CA Support Online to your computer. If your download included a zip file, unzip the file, and upload the unzipped pax files to your z/OS system.

This section includes a sample batch job to download a product pax file from the CA Support Online FTP server directly to a USS directory on your z/OS system and sample commands to upload a pax file from your computer to a USS directory on your z/OS system.

Important! The FTP procedures vary due to local firewall and other security settings. Consult your local network administrators to determine the appropriate FTP procedure to use at your site.

Ensure that sufficient free space is available in the USS file system that you are using for Pax-Enhanced ESD to hold the product pax file. If you do not have sufficient free space, error messages similar to the following appear:

```
EZA1490I Error writing to data set
EZA2606W File I/O error 133
```

When the download finishes, the pax file size in your USS directory matches the value in the Size column for the corresponding pax file on the CA Technologies Products Download window.

More Information:

How the Pax-Enhanced ESD Download Works
ESD Product Download Window

Download Using Batch JCL

Use this process to download a pax file from the CA Support Product Downloads window by running batch JCL on the mainframe. Use the sample JCL attached to the PDF file as CAt>Mainframe.txt to perform the download.

Important! To simplify the Pax-Enhanced ESD process, the PDF version of this guide includes a sample JCL job that you can copy directly to the mainframe. To access this job, click the paper clip icon at the left of the PDF reader. A window displaying attachments opens. Double-click the file to view the sample JCL.

Note: We recommend that you follow the preferred method as described on CA Support Online. This procedure is our preferred download method; however, we do include the procedure to download to the mainframe through a PC in the next section.

Follow these steps:

1. Supply a valid JOB statement.
2. Replace *yourTCPIP.PROFILE.dataset* with the name of the TCP/IP profile data set for your system. Consult your local network administrators, if necessary.

The job points to your profile.

3. Replace *YourEmailAddress* with your email address.

The job points to your email address.

4. Replace *yourUSSESDdirectory* with the name of the USS directory that you use for ESD downloads.

The job points to your USS directory.

5. Locate the product component to download on the CA Support Product Download window.

You have identified the product component to download.

6. Click Download for the applicable file.

Note: For multiple downloads, add files to a cart.

The Download Method window opens.

7. Click FTP Request.

The Review Download Requests window displays any files that you have requested to download.

Note: We send you an email when the file is ready to download or a link appears in this window when the file is available.

8. Select one of the following methods:

Preferred FTP

Uses CA Technologies worldwide content delivery network (CDN). If you cannot download using this method, review the security restrictions for servers that company employees can download from that are outside your corporate network.

Host Name: ftp://ftpdownloads.ca.com

Alternate FTP

Uses the original download servers that are based on Long Island, New York.

Host Name: ftp://scftpd.ca.com for product files and download cart files and ftp://ftp.ca.com for individual solution files.

Both methods display the host, user name, password, and FTP location, which you then can copy into the sample JCL.

Note: The following links provide details regarding FTP: the FTP Help document link in the Review Download Requests window and the Learn More link available in the Download Methods window.

9. Submit the job.

Important! If your FTP commands are incorrect, it is possible for this job to fail and still return a zero condition code. Read the messages in the job DDNAME SYSPRINT to verify the FTP succeeded.

After you run the JCL job, the pax file resides in the mainframe USS directory that you supplied.

Example: CAtoMainframe.txt, JCL

The following text appears in the attached CAtoMainframe.txt JCL file:

```
//GETPAX JOB (ACCOUNTNO),'FTP GET ESD PACKAGE',
//          MSGCLASS=X,CLASS=A,NOTIFY=&SYSUID
//*****
/* This sample job can be used to download a pax file directly from *
/* CA Support Online to a USS directory on your z/OS system.      *
/*                                                                *
/* When editing the JCL ensure that you do not have sequence numbers *
/* turned on.                                                    *
/*                                                                *
/* This job must be customized as follows:                        *
/* 1. Supply a valid JOB statement.                               *
/* 2. The SYSTCPD and SYSFTPD JCL DD statements in this JCL may be *
/*    optional at your site. Remove the statements that are not  *
/*    required. For the required statements, update the data set  *
/*    names with the correct site-specific data set names.       *
/* 3. Replace "Host" based on the type of download method.       *
/* 4. Replace "YourEmailAddress" with your email address.       *
/* 5. Replace "yourUSSESDdirectory" with the name of the USS     *
/*    directory used on your system for ESD downloads.          *
/* 6. Replace "FTP Location" with the complete path              *
/*    and name of the pax file obtained from the FTP location   *
/*    of the product download page.                             *
//*****
//GETPAX EXEC PGM=FTP,PARM='(EXIT',REGION=0M
//SYSTCPD DD DSN=yourTCPIP.PROFILE.dataset,DISP=SHR
//SYSFTPD DD DSN=yourFTP.DATA.dataset,DISP=SHR
//SYSPRINT DD SYSOUT=*
//OUTPUT DD SYSOUT=*
//INPUT DD *
Host
anonymous YourEmailAddress
lcd yourUSSESDdirectory
binary
get FTP_location
quit
```

Download Files to Mainframe through a PC

If you download pax or zip files from CA Support Online to your PC, use this procedure to upload the pax file from your PC to your z/OS USS directory.

Follow these steps:

1. Follow the procedures in How the Pax-Enhanced ESD Download Works to download the product pax or zip file to your PC. If you download a zip file, first unzip the file to use the product pax files.

The pax or zip file resides on your PC.

2. Open a Windows command prompt.

The command prompt appears.

3. Customize and enter the FTP commands with the following changes:
 - a. Replace *mainframe* with the z/OS system IP address or DNS name.
 - b. Replace *userid* with your z/OS user ID.
 - c. Replace *password* with your z/OS password.
 - d. Replace *C:\PC\folder\for\thePAXfile* with the location of the pax file on your PC.
 - e. Replace *yourUSSESDdirectory* with the name of the USS directory that you use for ESD downloads.
 - f. Replace *paxfile.pax.Z* with the name of the pax file to upload.

The pax file is transferred to the mainframe.

Example: FTP Commands

This list is a sample of FTP commands to upload the pax file from your PC to your USS Pax-Enhanced ESD directory:

```
ftp mainframe
userid
password
bin
lcd C:\PC\folder\for\thePAXfile
cd /yourUSSESDdirectory/
put paxfile.pax.Z
quit
exit
```

Create a Product Directory from the Pax File

Use the sample job attached to the PDF file as Unpackage.txt to extract the product pax file into a product installation directory.

Important! To simplify the Pax-Enhanced ESD process, the PDF version of this guide includes a sample JCL job that you can copy directly to the mainframe. To access this job, click the paper clip icon at the left of the PDF reader. A window displaying attachments opens. Double-click the file to view the sample JCL.

Follow these steps:

1. Supply a valid JOB statement.
2. Replace *yourUSSESDdirectory* with the name of the USS directory that you use for ESD downloads.

The job points to your specific directory.

3. Replace *paxfile.pax.Z* with the name of the pax file.

The job points to your specific pax file.

4. Submit the job.

The job runs and creates the product directory.

Note: If the PARM= statement exceeds 71 characters, uncomment and use the second form of UNPAXDIR instead. This sample job uses an X in column 72 to continue the PARM= parameters to a second line.

Sample Job to Execute the Pax Command (Unpackage.txt)

The following text appears in the attached Unpackage.txt JCL file:

```
//ESDUNPAX JOB (ACCOUNTNO),'UNPAX ESD PACKAGE ',
// MSGCLASS=X,CLASS=A,NOTIFY=&SYSUID
//*****
/* This sample job can be used to invoke the pax command to create *
/* the product-specific installation directory. *
/* *
/* This job must be customized as follows: *
/* 1. Supply a valid JOB statement. *
/* 2. Replace "yourUSSESDdirectory" with the name of the USS *
/* directory used on your system for ESD downloads. *
/* 3. Replace "paxfile.pax.Z" with the name of the pax file. *
/* NOTE: If you continue the PARM= statement on a second line, make *
/* sure the 'X' continuation character is in column 72. *
//*****
//UNPAXDIR EXEC PGM=BPXBATCH,
// PARM='sh cd /yourUSSESDdirectory/; pax -rvf paxfile.pax.Z'
/*UNPAXDIR EXEC PGM=BPXBATCH,
/* PARM='sh cd /yourUSSESDdirectory/; pax X
/* -rvf paxfile.pax.Z'
//STDOUT DD SYSOUT=*
//STDERR DD SYSOUT=*
```

Copy Installation Files to z/OS Data Sets

Use this procedure to invoke the SMP/E GIMUNZIP utility to create MVS data sets from the files in the product-specific directory.

Follow these steps:

1. Locate and read the product readme file or installation notes, if applicable, which resides in the product-specific directory that the pax command created. This file contains the product-specific details that you require to complete the installation procedure.

You have identified the product-specific installation details.

2. Use ISPF EDIT or TSO ISHELL to edit the UNZIPJCL sample job. You can perform this step in one of the following ways:
 - Use ISPF EDIT. Specify the full path name of the UNZIPJCL file.
 - Use TSO ISHELL. Navigate to the UNZIPJCL file and use the E line command to edit the file.

The job is edited.

3. Change the SMPDIR DD PATH to the product-specific directory created by the pax command.

Your view is of the product-specific directory.

4. If ICSF is not active, perform the following steps:
 - a. Change the SMPJHOME DD PATH to your Java runtime directory. This directory varies from system to system.

Note: The default Java location is the following:

`/usr/lpp/java/Java_version`

- b. Perform one of the following steps:
 - Change the SMPCPATH DD PATH to your SMP/E Java application classes directory, typically `/usr/lpp/smp/classes/`.
 - Change HASH=YES to HASH=NO on the GIMUNZIP parameter.

One of the following occurs: ICSF is active, or you are using Java.

5. Change all occurrences of *yourHLQ* to the high-level qualifier (HLQ) for z/OS data sets that the installation process uses. We suggest that you use a unique HLQ for each expanded pax file to identify uniquely the package. Do *not* use the same value for *yourHLQ* as you use for the SMP/E RELFILES.

All occurrences of *yourHLQ* are set to your high-level qualifier for z/OS data sets.

6. Submit the UNZIPJCL job.

The UNZIPJCL job completes with a zero return code. Messages GIM69158I and GIM48101I in the output and IKJ56228I in the JES log are acceptable.

GIMUNZIP creates z/OS data sets with the high-level qualifier that you specified in the UNZIPJCL job. You use these data sets to perform the product installation. The pax file and product-specific directory are no longer needed.

Note: For more information, see the IBM *SMP/E for z/OS Reference (SA22-7772)*.

How to Install Products Using Native SMP/E JCL

The following steps describe the process to install products using native SMP/E JCL:

1. Allocate product data sets and SMP/E data sets.
2. Create SMP/E CSI.
3. Receive base functions.
4. Apply base functions.
5. Accept base functions.
6. Configure the product according to your site requirements.

Prepare the SMP/E Environment for Pax Installation

The members in this procedure prepare the data sets, initialize the zones, and create the DDDEFs for the CA Database Management Solutions for IMS for z/OS products. DDDEF data sets are required. The default is NULLFILE.

For information about the members, see the comments in the JCL.

Follow these steps:

1. Customize the macro IMTSEDIT with your site-specific information and then copy the macro to your syslib location. Replace the rightmost parameters for each ISREDIT CHANGE macro command. Each time you edit an installation member, type IMTSEDIT on the TSO command line, and press Enter to replace the defaults with your specifications.

The macro is ready to customize the *yourHLQ*.SAMPJCL members.

Notes:

- Set the DASD HLQ to the same value specified for *yourHLQ* for the unzip to DASD ESD JCL.
 - Set the NULLFILE HLQ and use it for the IMS, HSSR, and CICS DDDEF specifications if valid libraries do not exist in your environment.
 - The following steps include instructions to execute the IMTSEDIT macro each time you open a new SAMPJCL member. To edit all SAMPJCL members simultaneously, read and follow the instructions in the IMTEDALL member.
2. Open the SAMPJCL member IMT1ALL in an edit session and execute the IMTSEDIT macro from the command line.

IMT1ALL is customized.
 3. Submit IMT1ALL.

This job produces the following results:
 - The target and distribution data sets for CA Database Management Solutions for IMS for z/OS are created.
 - Unique SMPLTS, SMPMTS, SMPSCDS, and SMPSTS data sets for this target zone are created.
 4. Open the SAMPJCL member IMT2CSI in an edit session and execute the IMTSEDIT macro from the command line.

IMT2CSI is customized.

Note: Be sure that the IMS, HSSR, and CICS DDDEF values specify a valid library. If one is not available in the environment, use the NULLFILE value specified in DBA1ALL.

5. Submit IMT2CSI.

This job produces the following results:

- The CSI data set is defined.
- The SMPPTS and SMPLOG data sets are allocated.
- The global, target, and distribution zones are initialized.
- The DDDEF entries for your product are created.
- The DDDEFs for the required SMP/E data sets are created.

Example: External Library Definitions

This example shows some of the DDDEF names that may be defined:

DDDEF	Data Set Name	Description
CICS	<i>high-level.SDFHLOAD</i>	CICS SDFHLOAD
CSPC	<i>high-level.SEDCSPC</i>	IBM C SEDCSPC
DB2	<i>high-level.SDSNLOAD</i>	DB2 SDSNLOAD
HSSR	<i>high-level.SFABLMDO</i>	IMS HSSR
IMS	<i>high-level.RESLIB</i>	IMS RESLIB

The following are common DDDEF specifications for CSPC and SCEELKED:

DDDEF	Data Set Name	Description
CSPC	CEE.SEDCSPC or CEE.SCEESPC	IBM C SEDCSPC
SCEELKED	CEE.SCEELKED	Language Environment SCEE

Run the Installation Jobs for a Pax Installation

Submit and run these *yourHLQ*.SAMPJCL members in sequence. Do not proceed with any job until the previous job has completed successfully.

Follow these steps:

1. Open the SAMPJCL member IMT3RECD in an edit session, and execute the IMTSEDIT macro from the command line.
IMT3RECD is customized.
2. Submit the *yourHLQ*.SAMPJCL member IMT3RECD to receive SMP/E base functions.
Third-Party Software for CA Database Management Solutions for IMS for z/OS is received and now resides in the global zone.
3. Open the SAMPJCL member IMT4APP in an edit session, and execute the IMTSEDIT macro from the command line.
IMT4APP is customized.
4. Submit the *yourHLQ*.SAMPJCL member IMT4APP to apply SMP/E base functions.
Third-Party Software for CA Database Management Solutions for IMS for z/OS is applied and now resides in the target libraries.
5. Open the SAMPJCL member IMT5ACC in an edit session, and execute the IMTSEDIT macro from the command line.
IMT5ACC is customized.
6. Submit the *yourHLQ*.SAMPJCL member IMT5ACC to accept SMP/E base functions.
Third-Party Software for CA Database Management Solutions for IMS for z/OS is accepted and now resides in the distribution libraries.

Clean Up the USS Directory

Important! This procedure is optional. Do not use this procedure until you complete the entire installation process.

To free file system disk space for subsequent downloads after downloading and processing the pax files for your CA Technologies product, we recommend removing the files from your USS directory and deleting unnecessary MVS data sets. You can delete the following items:

- Pax file
- Product-specific directory that the pax command created and all of the files in it
- SMP/E RELFILES, SMPMCS, and HOLDDATA MVS data sets

These data sets have the HLQ that you assigned in the UNZIPJCL job.

Note: Retain non-SMP/E installation data sets such as *yourHLQ*.INSTALL.NOTES for future reference.

Follow these steps:

1. Navigate to your Pax-Enhanced ESD USS directory.

Your view is of the applicable USS directory.

2. Delete the pax file by entering the following command:

```
rm paxfile
```

paxfile

Specifies the name of the CA Technologies pax file that you downloaded.

The pax file is deleted.

3. Delete the product-specific directory by entering the following command:

```
rm -r product-specific_directory
```

product-specific_directory

Specifies the product-specific directory that the pax command created.

The product-specific directory is deleted.

Note: You can also use TSO ISHELL to navigate to the pax file and product-specific directory, and delete them using the D line command.

Apply Maintenance

CA Support Online has maintenance and HOLDDATA published since the installation data was created. After the maintenance process completes, the product is ready to deploy.

Follow these steps:

1. Check CA Support Online and download any PTFs and HOLDDATA published since this release was created. If the base release was created recently, no PTFs or HOLDDATA will have been published yet.

2. Transfer the downloaded files to two separate FB 80 sequential data sets. Use one data set to contain the PTFs and the other to contain the HOLDDATA.

The PTFs and HOLDDATA become accessible to the *yourHLQ*.SAMPJCL maintenance members.

3. The IMTSEDIT macro was customized in the installation steps. Verify that you still have the values from the base installation.

4. Open the SAMPJCL member IMT6RECP in an edit session and execute the IMTSEDIT macro from the command line.

IMT6RECP is customized with your JOB statement, CSI location, and zone names.

5. Customize the IMT6RECP SMPPTFIN and SMPHOLD DD statements to reference the FB 80 data sets for the PTFs and HOLDDATA.

6. Submit IMT6RECP.

The PTFs and HOLDDATA are received.

7. Open the SAMPJCL member IMT7APYP in an edit session and execute the IMTSEDIT macro from the command line.

IMT7APYP is customized.

8. Submit IMT7APYP.

The PTFs are applied.

9. (Optional) Open the SAMPJCL member IMT8ACCP in an edit session and execute the IMTSEDIT macro from the command line.

IMT8ACCP is customized.

10. (Optional) Submit *yourHLQ*.SAMPJCL member IMT8ACCP.

The PTFs are accepted.

Note: You do not have to submit the job at this time. You can accept the PTFs according to your site policy.

HOLDDATA

When you apply maintenance, you typically encounter SMP/E HOLDDATA. We use HOLDDATA to notify your SMP/E system of SYSMODs that have errors or special conditions. We support system and external HOLDDATA.

System HOLDDATA

System HOLDDATA indicates data that is an in-stream part of the SYSMOD, informing you of special conditions. The following reasons are used with SYSTEM HOLDDATA for your product:

ACTION

Indicates that you must perform special processing before or after you apply this SYSMOD.

AO

Affects automated operations. It changes either the message identifier or the displacement of a field inside the message.

DB2BIND

Indicates that DBRMs have changed and packages need to be rebound.

DDDEF

Indicates that data sets and DDDEFs are being added or modified.

DELETE

Deletes the SYSMOD load module. You cannot reverse this type of SYSMOD with the SMP/E RESTORE command.

DEP

Indicates a dependency for this SYSMOD that you must externally verify.

DOC

Indicates a documentation change with this SYSMOD.

DYNACT

Describes the steps to dynamically activate this fix without performing an IPL.

EC

Indicates that this SYSMOD requires a hardware engineering change. An EC hold SYSMOD usually does not affect the product unless the EC is present on the hardware device.

ENH

Introduces a small programming enhancement. The hold contains the instructions to implement the enhancement. If no action is needed to implement the enhancement, give a summary of the enhancement.

EXIT

Indicates that changes delivered by this SYSMOD require reassembly of user exits.

EXRF

Indicates that the SYSMOD must be installed in both the Active and Alternate Extended Recovery Facility Systems.

IPL

Indicates that an IPL is required for this SYSMOD to take effect. This is used only when there is no alternative for dynamic activation.

MSGSKEL

Indicates that the SYSMOD contains internationalized message versions that must be run through the message compiler for each language.

MULTSYS

Apply this SYSMOD to multiple systems for either pre-conditioning, coexistence, or exploitation.

RESTART

Indicates that after applying this SYSMOD, the site must perform a special restart as opposed to a routine restart.

SQLBIND

Indicates that a bind is required for a database system other than DB2.

SYSMOD

Indicates that some or all of the elements that this SYSMOD delivers are to be downloaded to a workstation.

Code a bypass operand on your APPLY command to install SYSMODs that have internal holds. Code the bypass operand only after you have performed the required action, or if you are performing the action after the APPLY, if that is appropriate.

External HOLDDATA

External HOLDDATA is not part of the PTF. The HOLDDATA resides in a separate file. The HOLDDATA is commonly used for SYSMODs that have been distributed and later are discovered to cause problems.

Download the external HOLDDATA from CA Support to a DASD file, and allocate the file to the SMPHOLD DD statement. To take care of the external HOLDDATA, receive it into your SMP/E environment. SMP/E receives the HOLDDATA from CA-supplied jobs.

If a SYSMOD has an unresolved hold error, SMP/E does not install it unless you add a bypass to your APPLY command. You can bypass an error hold in situations that are not applicable to you. Error holds that are not applicable to you can include a problem that happens only with a hardware device that you do not have or in a product feature that you do not use.

When CA Technologies publishes a SYSMOD that resolves the hold, the resolving SYSMOD supersedes the hold error. This action lets you apply the original SYSMOD in conjunction with the fixing SYSMOD.

A special HOLDDATA class that is called ERREL exists. We have determined that the problem fixed by the SYSMOD is more important than the one that it causes. We recommend that you apply these SYSMODs.

The only manual task is running a REPORT ERRSYSMODS. This report identifies the following:

- Any held SYSMODs already applied to your system
- Any resolving SYSMODs that are in RECEIVE status

SMP/E identifies the SYSMOD to apply to correct the situation.

Chapter 5: Installing Your Product from Tape

This section contains the following topics:

Unload the Sample JCL from Tape.....	58
How to Install Products Using Native SMP/E JCL	59
Apply Maintenance	61

Unload the Sample JCL from Tape

To simplify the process, the PDF version of this guide includes a sample JCL job that you can copy directly to the mainframe. To access this job, click the paper clip icon at the left of the PDF reader. A window displaying attachments opens. Double-click the UnloadJCL.txt file to view the sample JCL job.

Note: The sample JCL to install the product is also provided in the CAI.SAMPJCL library on the distribution tape.

Follow these steps:

1. Run the following sample JCL:

```
//COPY      EXEC  PGM=IEBCOPY,REGION=4096K
//SYSPRINT DD   SYSOUT=*
//SYSUT1    DD   DSN=CAI.SAMPJCL,DISP=OLD,UNIT=unitname,VOL=SER=nnnnnnn,
//          LABEL=(1,SL)
//SYSUT2    DD   DSN=yourHLQ.SAMPJCL,
//          DISP=(,CATLG,DELETE),
//          UNIT=sysda,SPACE=(TRK,(15,3,6),RLSE)
//SYSUT3    DD   UNIT=sysda,SPACE=(CYL,1)
//SYSIN     DD   DUMMY
```

unitname

Specifies the tape unit to mount the tape.

nnnnnnnn

Specifies the tape volume serial number.

yourHLQ

Specifies the data set prefix for the installation.

sysda

Specifies the DASD where you want to place the installation software.

The SAMPJCL data set is created and its contents are downloaded from the tape.

2. Continue with one of the following options:
 - If you already have set up the SMP/E environment, go to Run the Installation Jobs for a Tape Installation.
 - If you have *not* set up the SMP/E environment, go to Prepare the SMP/E Environment for Tape Installation.

How to Install Products Using Native SMP/E JCL

The following steps describe the process to install products using native SMP/E JCL:

1. Allocate product data sets and SMP/E data sets.
2. Create SMP/E CSI.
3. Receive base functions.
4. Apply base functions.
5. Accept base functions.
6. Configure the product according to your site requirements.

Prepare the SMP/E Environment for Tape Installation

The members in this procedure prepare the data sets, initialize the zones, and create the DDDEFs for CA Database Management Solutions for IMS for z/OS. External DDDEF data sets are required. The default is NULLFILE.

Prior to beginning this procedure, confirm whether your product uses UNIX System Services (USS). If it does, establishing a hierarchical file system (HFS) may be required as part of the product installation or required as a feature of the product.

For information about the members, see the comments in the JCL.

Follow these steps:

1. Customize the macro IMTSEDIT with your site-specific information and then copy the macro to your syslib location. Replace the rightmost parameters for each ISREDIT CHANGE macro command. Each time you edit an installation member, type IMTSEDIT on the TSO command line, and press Enter to replace the defaults with your specifications.

The macro is ready to customize your IMT.SAMPJCL members.

Note: The following steps include instructions to execute the IMTSEDIT macro each time you open a new SAMPJCL member. To edit all SAMPJCL members simultaneously, read and follow the instructions in the IMTEDALL member.

2. Open the SAMPJCL member IMT1ALL in an edit session and execute the IMTSEDIT macro from the command line.

IMT1ALL is customized.

3. Submit IMT1ALL.

This job produces the following results:

- The target and distribution data sets for CA Database Management Solutions for IMS for z/OS are created.
- Unique SMPPLTS, SMPMTS, SMPSCDS, and SMPSTS data sets for this target zone are created.

4. Open the SAMPJCL member IMT2CSI in an edit session and execute the IMTSEDIT macro from the command line.

IMT2CSI is customized.

5. Submit IMT2CSI.

This job produces the following results:

- The CSI data set is defined.
- The SMPPTS and SMPLOG data sets are allocated.
- The global, target, and distribution zones are initialized.
- The DDDEF entries for your product are created.
- The DDDEFs for the required SMP/E data sets are created

Run the Installation Jobs for a Tape Installation

Submit and run these SAMPJCL members in sequence. Do not proceed with any job until the previous job has completed successfully.

Follow these steps:

1. Open the SAMPJCL member IMT3RECT in an edit session and execute the IMTSEDIT macro from the command line.

IMT3RECT is customized.

2. Submit the *yourHLQ*.SAMPJCL member IMT3RECT to receive SMP/E base functions.

CA Database Management Solutions for IMS for z/OS is received and now resides in the global zone.

3. Open the SAMPJCL member IMT4APP in an edit session and execute the IMTSEDIT macro from the command line.

IMT4APP is customized.

4. Submit the *yourHLQ*.SAMPJCL member IMT4APP to apply SMP/E base functions.

Your product is applied and now resides in the target libraries.

5. Open the SAMPJCL member IMT5ACC in an edit session and execute the IMTSEDIT macro from the command line.

IMT5ACC is customized.

6. Submit the *yourHLQ*.SAMPJCL member IMT5ACC to accept SMP/E base functions.

Your product is accepted and now resides in the distribution libraries.

Apply Maintenance

CA Support Online has maintenance and HOLDDATA published since the installation data was created. After the maintenance process completes, the product is ready to deploy.

Follow these steps:

1. Check CA Support Online and download any PTFs and HOLDDATA published since this release was created. If the base release was created recently, no PTFs or HOLDDATA will have been published yet.

2. Transfer the downloaded files to two separate FB 80 sequential data sets. Use one data set to contain the PTFs and the other to contain the HOLDDATA.

The PTFs and HOLDDATA become accessible to the *yourHLQ*.SAMPJCL maintenance members.

3. The IMTSEDIT macro was customized in the installation steps. Verify that you still have the values from the base installation.

4. Open the SAMPJCL member IMT6RECP in an edit session and execute the IMTSEDIT macro from the command line.

IMT6RECP is customized with your JOB statement, CSI location, and zone names.

5. Customize the IMT6RECP SMPPTFIN and SMPHOLD DD statements to reference the FB 80 data sets for the PTFs and HOLDDATA.

6. Submit IMT6RECP.

The PTFs and HOLDDATA are received.

7. Open the SAMPJCL member IMT7APYP in an edit session and execute the IMTSEDIT macro from the command line.

IMT7APYP is customized.

8. Submit IMT7APYP.

The PTFs are applied.

9. (Optional) Open the SAMPJCL member IMT8ACCP in an edit session and execute the IMTSEDIT macro from the command line.

IMT8ACCP is customized.

10. (Optional) Submit *your*HLQ.SAMPJCL member IMT8ACCP.

The PTFs are accepted.

Note: You do not have to submit the job at this time. You can accept the PTFs according to your site policy.

Note: We recommend that you check for available maintenance; however, you may find that none is available.

HOLDDATA

When you apply maintenance, you typically encounter SMP/E HOLDDATA. We use HOLDDATA to notify your SMP/E system of SYSMODs that have errors or special conditions. We support system and external HOLDDATA.

Chapter 6: Starting Your Product

This section describes what you need to do to start CA Database Management Solutions for IMS for z/OS.

This section contains the following topics:

How to Configure Without CA MSM
Preparing to Start CA Database Management Solutions for IMS for z/OS

How to Configure Without CA MSM

The topics in this section describe the manual tasks you perform if you are not configuring your product using CA MSM.

How to Enable Environment Specific Product Customizations

You can use the ITKOPTN macro to maintain environment specific product customizations. This macro replaces the special ZAPs that have been previously provided to customize product environments. These ZAPS often needed to be reapplied or were regressed when additional maintenance was performed.

The following files are provided in the sample library (*h/q.CIMTSAMP*) to customize this special option processing:

- ITKOPTN macro
- ITKOPTN0 source member
- JCLOPTNA JCL member

To maintain environment specific product customizations, follow these steps:

1. Copy members ITKOPTN0 and ITKOPTN from CIMTSAMP to a new source library.
2. Modify ITKOPTN0 to select the options you want to make active (set to Y).
3. Modify JCLOPTNA to reference the source library where you copied ITKOPTN0 and ITKOPTN and to specify a load library.
4. Execute JCLOPTNA to assemble and link ITKOPTN0.
5. Copy the module to your runtime library.

If the ITKOPTN0 load module is present during execution, the specific settings are interpreted and the optional processing is used as requested. The processing logic produces a message with the active options found.

A version validation is also built into this process. If a change is required of one of the options, and maintenance introduces a need for a new version, a message is generated indicating verification failure.

Create Library Data Set Name Aliases for the CA Database Management Solutions for IMS

Due to packaging changes with CA MSM, new names are now used for installation libraries. For example, *high-level*.LOADLIB is now *high-level*.CIMTLOAD. To enable reuse of your existing JCL from an earlier release of CA Database Management Solutions for IMS for z/OS, you can create aliases relating the old library names to the new library names that now exist.

Follow these steps:

1. Edit the INSALIAS job located in *high-level*.CIMTSAMP to change the prefixes of the old libraries (following) as they exist at your site and save your changes:

- CLIST
- LOADLIB
- PARMLIB
- SAMPLIB
- SPFHLIB
- SPFMLIB
- SPFPLIB
- SPFSLIB
- SRCLIB

The JCL is customized.

2. Type **SUBMIT** on the command line and press Enter.

A job is generated that creates aliases for the old library names:

- CLIST to CIMTCLSO
- LOADLIB to CIMTLOAD
- PARMLIB to CIMTPARM
- SAMPLIB to CIMTSAMP
- SPFHLIB to CIMTPNLO

- SPFMLIB to CIMTMSG0
- SPFPLIB to CIMTPNLO
- SPFSLIB to CIMTSKLO
- SRCLIB to CIMTSRC

Resolve Multiple IMS Partner Product User Exits

The IMS regions where CA Database Organizer or CA Mainframe Extended Terminal Manager will be executed require executing the CA Database Management Solutions for IMS for z/OS version of the IMS Partner Product exit routine, IDIPPUE0.

The IDIPPUE0 module that is distributed in *hlq.CIMTLOAD* also loads and calls the following PPUE modules:

- HPOPPUE0—CA Database Organizer version of PPUE.
- ETMPPEUZ—CA Mainframe Extended Terminal Manager version of PPUE.
- DFSPPUE2 (if found in the STEPLIB concatenation)— and the DFSPPUE0 in *hlq.CIMTLOAD* will call the renamed exit.

Note: In the CA Database Management Solutions for IMS for z/OS load library (*hlq.CIMTLOAD*), DFSPPUE0 is an alias of IDIPPUE0.

Follow these steps:

1. If you have another product with a DFSPUE0 exit, rename the module of that product to DFSPUE2.

Create an ETM_{imsid} IMS PROCLIB member (see the *hlq.CIMTSAMP(ETMIMSID)* member as a guide) and specify the new names of the renamed DFSPUE0 in the member.
 2. To execute IDIPPUE0, perform either of the following:
 - To execute IDIPPUE0 at the IMS startup, specify the *hlq.CIMTLOAD* library first in the STEPLIB concatenation.
 - To execute IDIPPUE0 using the IMS Tools Generic Partner Exit (GPR), follow these steps:
 1. Create a GPR PROCLIB member:

```
EXITDEF(TYPE(PARTNER) EXITNAME(IDIPPUE0) LOADLIB(hlq.CIMTLOAD))
```
 2. Delete or rename the DFSPUE0 alias in the *hlq.CIMTLOAD*.
- Note:** Do not create a GPR member for ETMPUEZ in the GPR PROCLIB member.

The FFOR call intercept load modules (HPODDLE0, HPODDL00, HPODLA00, and HPOFXC50) front-end the corresponding DFS-prefixed load modules. During an full function online recovery, These load modules collect information about DLI updates and rollbacks that are performed against an online database in the process of being reorganized. This information is inserted into the online reorg call repository.

How to Implement the ISPF Interface for CA Database Management Solutions for IMS for z/OS

Several of the products and components of the CA Database Management Solutions for IMS for z/OS contain ISPF interfaces. An ISPF panel is available to set up the environment required for accessing these ISPF interfaces. You can customize the ISPF environment for the following products and components:

- CA Database Copier
- Database Surgeon component of CA Database Analyzer for IMS
- Control Block Validity Manager component of CA Database Analyzer for IMS
- Recovery Analyzer component of CA High Performance Recovery
- CA Mainframe Configuration Manager
- CA Mainframe Program Restart Manager
- CA Compress Data Compression for IMS

- IMS Information Repository (IIR) Historical Reporting
- Command Control Manager

To implement the ISPF interface for CA Database Management Solutions for IMS for z/OS, follow these steps:

1. [Customize the \\$ITK CLIST](#) (see page 67).
2. (Optional) [Update the ISPF primary menu](#) (see page 68).

Note: For more information about additional steps, see the Customization section for each particular product.

Set Up the \$ITK CLIST

Setting up the CA Database Management Solutions for IMS for z/OS CLIST lets you access the CA Database Management Solutions for IMS for z/OS products and components through the ISPF interface.

Follow these steps:

1. Specify the following parameters in the CLIST:

HILVLQ

Specifies the high-level qualifier of target or deployment libraries for CA Database Management Solutions for IMS for z/OS.

CONFIGDS

Specifies the [Config PDS](#) (see page 72) that is used by ISPF interfaces of CA Database Copier or the Recovery Analyzer component of CA High Performance Recovery.

RESLIB

Specifies the IMS RESLIB data set name that is used by the Command Control Manager ISPF interface when accessing IMS regions using the OM/SCI interface.

2. (Optional) To invoke the CLIST, do *any* of the following:
 - Copy the CLIST from *hlq.CIMTSL0(\$ITK)* to a CLIST library available to your TSO session.
 - Execute the following TSO command from ISPF option 6:


```
EX 'hlq.CIMTCLS0($ITK)' 'CONFIGDS(CAIMS.CFGDS) RESLIB(IMSSYS.SDFSRESL)'
```

Update the ISPF Primary Menu

Update the ISPF primary menu to provide quick and convenient access to the products and components of CA Database Management Solutions for IMS for z/OS.

Follow these steps:

1. Add the following line in the)BODY section:

```
% TK +IMS Toolkit - CA Database Management Solutions for IMS
```

2. Add the following line in the)PROC section:

```
TK, 'CMD($ITK) '
```

CA Database Analyzer for IMS Customization

You can customize CA Database Analyzer for IMS to execute as an exit from the IBM IMS image copy utility. To do this, execute an SMP/E RECEIVE, ACCEPT, and APPLY on the IMS system where DFSUDMP0 is located using the DBAICE member in *high-level*.CIMTSAMP as input. This performs a complete analysis, including pointer checking, at the same time a regularly scheduled image copy is performed.

Note: DBAICE applies across many releases of IMS. This means that there are no ++PRE or ++REQ statements. Because of this, you might receive SMP/E messages GIM41902I and GIM31902I. You can ignore these messages.

CA Database Copier Customization

You can perform the following steps to customize CA Database Copier:

- Configure CA Database Copier to run in IMS (DFSUICP0) compatibility mode
- Configure Snapshot General Services
- Configure BMP pause and resume

How to Configure CA Database Copier to Run in IMS Compatibility Mode

To run CA Database Copier in IMS (DFSUICP0) compatibility mode, you must update the jobs that perform DFSUICP0 compatibility mode processing to place the CA Database Management Solutions for IMS load library ahead of the IMS SDFSRESL library in the STEPLIB concatenation.

This update is shown in the following sample JCL:

```
//STPCOPY EXEC PGM=DFSRR00,PARM='BMP,DFSUICP0,BVAS660C,, '  
//STEPLIB DD DISP=SHR,DSN=CTR.CAI.TOOLKIT.CIMTLOAD  
//DFSUCKPT DD DUMMY  
//SYSPRINT DD SYSOUT=*
```

```
//IMS DD DSN=BLIB.DBD,DISP=SHR
//VAS06600 DD DISP=SHR,DSN=DBA.VAS.VAS06600
//DATAOUT0 DD DISP=(,CATLG,DELETE),DSN=CTR.VAS06600(+1),
//          SPACE=(CYL,(50,10),RLSE),UNIT=(DISK,1),DCB=DSCB
//SYSIN DD *
DD1 DVAS6600 VAS06600 DATAOUT0
/*
```

How to Configure Snapshot General Services in CA Database Copier

To use Snapshot General Services, a subsystem must be running on the target system where the IMS specified in the IMSID runs. The batch image copy job must run on this same system. This subsystem must be started once at IPL or anytime thereafter, and remains until the next IPL.

More information:

Initialize Snapshot General Services
 Reinitialize Snapshot General Services

How to Configure BMP Pause and Resume in CA Database Copier

The BMP Pause and Resume provides the automated operator interface (AOI) to stop and start the database automatically. To use AOI, the ITK started task (STC) must be running on the same system as the target IMS systems. In a data sharing environment, all systems that are involved in the data sharing must have an ITK STC running. The ITK STC procedure is provided in the STCITK member in the sample library (*hlq.CIMTSAMP*).

Important! To prevent an LXC4 - SOC4 abend through LXC4MAIN, verify that all current LXC4MAIN-related APARs are applied. Related APARs are accessible from the CA Support Online website.

CA Database Organizer Customization

You can customize CA Database Organizer to run in API mode, use online reorg, and to use the batch log tracker.

Configure CA Database Organizer to Run in API Mode

You can execute CA Database Organizer in API mode without statically linking the CA call interceptor.

Note: For more information about running in API mode, see the *CA Database Organizer Reference Guide*.

Follow these steps:

1. Edit the API processing jobs as follows and save your edits:
 - Place the CA Database Management Solutions for IMS load library ahead of the IMS SDFSRESL library in the STEPLIB concatenation.
 - Add the necessary DD statements and control statements to the jobs.

The API processing jobs are updated.

2. Submit the jobs for execution.

CA Database Organizer processing occurs in API mode.

How to Enable Online Reorg Processing in CA Database Organizer

Online reorg support is provided for Full Function HALDB databases (FFOR) and Fast Path DEDB databases (FPOR). Online reorg contains a data collector and executes in an IMS control region and in an IMS DBCTL region.

Important! To prevent database corruption and an LXC - SOC4 abend through LXCMAIN, verify that all current CA Resource Initialization Manager (Comm - CAIRIM) and LXCMAIN-related APARs are applied before you begin. These APARs are accessible from <http://ca.com/support>.

Follow these steps:

1. APF-authorize the online reorg load library (using the operator command, SETPROG, or by updating IEAAPFxx).
2. Add one ITK started task (STC) to a JES-accessible proclib.

Note: See a sample ITK started task JCL in the *hlq.CIMTSAMP(STCITK)* member.

Code the ITK STC control statements in a member of the CIMTPARM data set whose name matches the STC name. For example, if the STC name is FFOR, make the member name FFOR. When you first execute the ITK STC, it interactively requests values for parameters that have not yet been coded. Null replies are accepted.

3. Verify that your security package lets the online reorg batch job copy a member into the active ACBLIB data set and then delete that member.
4. [Resolve multiple IMS partner product user exits \(PPUE\)](#) (see page 65).
5. Add the CA Technologies product load library (*hlq.CIMTLOAD*) to the STEPLIB concatenation of the IMS/DC control region, *before* the SDFSRESL data set.

Note: The product load library must also be APF-authorized.

More information:

ITK STC Communication

STC Control Statements.....

Online Reorg Upgrade Considerations

Review the following upgrade considerations before you upgrade online reorg from an earlier release to the current release:

- You no longer need to specify INTRMICx, and ICWHILEOFFLINE is no longer supported because all image copy activities occur while the database is online.
- To recover a database to its state immediately prior to having been placed online after the reorganization, recover to the time stamp in DBRC that is after the creation of the replay log (IEFRDER) and before the /STA that placed the database online.
- BMPPAUSE=YES is the default, which causes CA Database Organizer online reorganization to automatically pause and resume BMPs that are active against the target database when exclusive control of the database is needed.
- The ITK STC started task is required for Full Function and HALDB online reorganization along with the installation of call intercept code into the IMS systems. Only one ITK STC should be run on a given z/OS image. A single ITK STC per z/OS image where IMS systems reside will work for all functions that use it.

Note: The started task sample is provided in the parmlib member STCITK.

How to Install the Batch Log Tracker

To ensure that logs are allocated and that the databases are available before the batch program executes, you can install and use the batch log tracker in CA Database Organizer.

Follow these steps:

1. Create ITLTRACK (a CSECT that has some installation defaults). Edit, modify, and submit the JCLBLTRK member of the sample library.
2. Create the OLE (the KSDS name you provided in ITLTRACK). Edit, modify, and submit the JCLMKOLE member of the sample library.

3. (Optional) Use the Uberutility to create dynamic allocation model records in the OLE.
4. Add the batch log tracker load library in the STEPLIB in the DLIBATCH procedure, before the SDFSRESL data set.
5. Add a DD DUMMY statement to the DLIBATCH procedure using the ddname that you specified on the MONDD statement when you created ITLTRACK.

CA High Performance Recovery Customization

You can perform the following customization of CA High Performance Recovery after installation:

- Configure CA High Performance Recovery to run in compatibility mode
- Maintain the Config PDS data set

How to Run CA High Performance Recovery in IMS Compatibility Mode

To run CA High Performance Recovery in IMS compatibility mode, update the jobs that perform IMS compatibility mode processing to place the CA Database Management Solutions for IMS load library ahead of the IMS SDFSRESL library in the STEPLIB concatenation.

How to Maintain the Config PDS Data Set

The Recovery Analyzer ISPF interface uses a data set called the Config PDS. The configuration member contains information about each IMS system. If you are a new user, a new Config PDS is built for you during the first invocation of Recovery Analyzer. However, if you are an existing user, we recommend that you copy your current Config PDS and IEBCOPY it to a new Config PDS to be used as input. The new Config PDS is not compatible with older releases of Recovery Analyzer.

Note: For information about starting Recovery Analyzer using the ISPF interface, see the *CA High Performance Recovery Reference Guide*.

Example: IEBCOPY JCL

Use the following sample JCL to copy the current Config PDS to a new Config PDS:

```
//          JOB
//COPY      EXEC PGM=IEBCOPY
//IN1       DD  DISP=SHR,DSN=YOUR.CURRENT.HILVLQ.RMGCNFG
//OT1       DD  DISP=(NEW,CATLG),SPACE=(CYL,(5,1,300),RLSE),
//          DCB=(LRECL=80,BLKSIZE=27920,RECFM=FB),
//          DSN=XXX.YYY.RMGCNFG
//SYSPRINT  DD  SYSOUT=*
//SYSUT3    DD  UNIT=3390,SPACE=(CYL,(25,25))
//SYSUT4    DD  UNIT=3390,SPACE=(CYL,(25,25))
//SYSIN     DD  *
C I=IN1,0=OT1,LIST=NO
//
```

CA Mainframe Configuration Manager Customization

If you have installed CA Mainframe Configuration Manager, you must configure the product. To customize CA Mainframe Configuration Manager, follow these steps:

1. [Add and activate the PSB.](#) (see page 75)
2. Enable IMS online change for MODBLKS on all IMS systems. You can enable local online change or global online change.

Note: Each IMS system must have a unique MODBLKSA and MODBLKSB data set. If they share these data sets, enqueue issues will occur when online changes are performed.

3. Allocate the following data sets:

CFMPDS

Stores all resource update lists. Allocate one CFMPDS per sysplex.

CFMOPT

Contains load modules that describe the environment of each IMS system. Allocate one CFMOPT per sysplex.

The CFMOPT data set must be present on the z/OS system where the IMS system runs and on any z/OS system where a TSO user accesses that IMS system with CA Mainframe Configuration Manager. We recommend that you have the z/OS systems on a shared DASD.

CFMLOG

Contains history logs. Allocate one CFMLOG data set for each IMS system.

Note: The the CFMALLOC job is provided in the CA Database Management Solutions for IMS for z/OS samplib for allocation of CFMPDS and CFMOPT data sets. The CFMALLOC job is provided in the CA Database Management Solutions for IMS for z/OS samplib for allocation of CFMLOG data set.

4. [Configure APPC/MVS](#) (see page 76):

- a. Verify that APPC/MVS is installed and active. CA Mainframe Configuration Manager uses this application to communicate across systems.
- b. Define one APPC symbolic definition for each LPAR where an IMS system executes. The CFMSIADD job in the CIMTSAMP library is provided for this purpose.
- c. Define the APPC TP profile on each LPAR where an IMS system executes. The CFMTPADD job in the CIMTSAMP library is provided for this purpose.

Note: The default TP profile name is CFMR14_CA_CONFIG_MGR. If you change the profile name after installation, you must specify the new name in every IMS system's IMSID options in the APPC/MVS CA Config TPName field.

5. Customize the ISPF interface:

- a. Update the CFMXISPF EXEC in the CIMTCLS0 library to reflect the names of the ISPF libraries and CFMPDS and CFMOPT data sets.
- b. Copy the CFMXISPF EXEC from the CIMTCLS0 library to a CLIST or EXEC library that is accessible to all users.

Optionally, [set up the ISPF interface](#) (see page 66) to invoke CA Mainframe Configuration Manager through the CA Database Management Solutions for IMS for z/OS main menu.

6. [Define the required security profiles](#) (see page 80).

The CFMACF2, CFMTSS, and CFMRACF jobs are provided in the CA Database Management Solutions for IMS for z/OS sample library for this purpose.

7. (Optional) [Define an authorized user ID for CA Mainframe Configuration Manager](#) (see page 80).
8. Review the following settings in the DFSPBxxx member of PROCLIB:
 - IMS online system parameters AOIS must be A, C, or R if you use the IMS Common Service Layer (CSL) in a sysplex environment with global online change enabled (that is, you used IMS command INITIATE OLC instead of /MODIFY PREPARE).
 - CMDMCS must be any value other than N.
9. Configure the APPC/MVS security settings:
 - Specify SECACPT=ALREADYV or AVPV in the VTAMLST definition for the APPC base LU.
 - Specify other settings, such as APPCLU class profiles, as needed to conform to your security environment.
10. [Create IMSID list entries](#) (see page 81).
11. (Optional) [Assign IMS systems to groups](#) (see page 92).
12. (Optional) [Define authorization profiles and assign user IDs to them](#) (see page 94).

Add and Activate PSB

Follow these steps:

1. Add the CA Mainframe Configuration Manager PSB to the IMS stage 1 deck for each IMS that CA Mainframe Configuration Manager will manage. See *high-level.CIMTSAMP(CFMSYSGN)* for a sample.
2. Perform a MODBLKS gen and restart IMS, or use online change to activate the new PSB.

The CA Mainframe Configuration Manager PSB is active.

APPC/MVS Considerations

APPC/MVS is primarily used to implement client-server communications across mainframe systems. CA Mainframe Configuration Manager requires APPC/MVS, even in a single-system environment, for the following reasons:

- To provide APF authorization within TSO sessions. CA Mainframe Configuration Manager requires this authorization to perform various functions. APF authorization is difficult to set up through TSO; however, APPC/MVS is an APF-authorized program, and therefore provides the necessary authorizations when using CA Mainframe Configuration Manager TSO sessions.
- To communicate across z/OS images. This capability lets users update resource definitions in IMS systems on different z/OS images.
- To let the CA Mainframe Configuration Manager ISPF interface issue authorized IMS commands and display the responses.

Note: If APPC/IMS is installed, CA Mainframe Configuration Manager uses it.

APPC/MVS is part of the base MVS product, and is typically already installed before you install CA Mainframe Configuration Manager. For CA Mainframe Configuration Manager to use APPC/MVS, you must set up side information entries and a TP profile. You can perform these tasks by running the JCL jobs provided with CA Mainframe Configuration Manager.

Note: For more information about installing APPC/MVS, see the IBM *MVS Planning: APPC Management*.

How to Enable ALREADYV Security for APPC/MVS LUs

The APPC/MVS LUs used by CA Mainframe Extended Terminal Manager and CA Mainframe Configuration Manager must use ALREADYV security. These LUs include the following:

- APPC/MVS base LU on the z/OS system where the IMS is located
- APPC/MVS base LU on the z/OS system where IMS is running
- APPC/IMS LU

To enable ALREADYV security for APPC/MVS LUs, do *one* of the following to override the SECACPT= value in the VTAM APPL definition in VTAMLST:

- Specify SECACPT=ALREADYV or SECACPT=AVPV for the LUs.
- Define security profiles to override the SECACPT= value.

Rules for Defining Security Profiles

Profiles must be defined in the APPCLU class to override session conversation security—SESSION(CONVSEC(ALREADYV)). APPCLU profiles let you override the SECACPT= value for a conversation between two specific LU names. The profile name, which includes both LU names involved in the session, has a format that is determined as follows:

If the LU names specify NQN=NO, the following profile name format is used:

network-id.local-lu-name.remote-lu-name

If the LU names specify NQN=YES, the following profile name format is used:

network-id.local-lu-name.network-id.remote-lu-name

Note: You can optionally define both forms of the APPCLU profiles. If this is done when the profiles are initially defined, a change in the NQN specification will not require changes in the defined security profiles.

To find the LU names and determine which profile name format to use, you can issue a D APPC,LU,ALL command and review the output. To determine which LU names are needed in the profile names, find the base LU for APPC/MVS and the IMS APPC LU. The base LU will show SCHED=ASCH and BASE=YES. The IMS APPC LU name will show SCHED=*imsid* and BASE=YES.

Note: You can also obtain the network ID by issuing the D NET,ID=*lu_name* display command.

More information:

Sample Output from D APPC,LU,ALL Command.....
Conversational Security Settings for Profiles

Obtaining the Network ID for a Security Profile Name

You can obtain the network ID to be used in a security profile name by issuing the following display command:

D NET,ID=*lu_name*

In the resulting output, the IST075I message shows the network name before the LU name.

More information:

Sample Output from the D NET,ID=*lu_name* Command.....

Conversational Security Settings for Profiles

When defining your security profiles, specify a value for SESSION CONVSEC of ALREADYV (or AVPV). If you use RACF, use the following command format to define these profiles (for an NQN=NO environment):

```
RDEFINE ADCD.MVSLU01.MVSLU01 UACC(NONE) -SESSION(CONVSEC(ALREADYV))
```

```
RDEFINE ADCD.MVSLU01.IMS9PPC UACC(NONE) -SESSION(CONVSEC(ALREADYV))
```

```
RDEFINE ADCD.IMS9PPC.MVSLU01 UACC(NONE) -SESSION(CONVSEC(ALREADYV))
```

If you have VERIFY=REQUIRED on the VTAM APPL definitions in VTAMLST, you may also require session key definitions in the RACF commands.

Note: For more information about session keys, see the IBM *z/OS MVS Planning: APPC/MVS Management* and *z/OS Security Server RACF Command Language Reference*.

More information:

Rules for Defining Security Profiles

Defining Multiple Profiles for Multiple LPARs

If you have multiple LPARs, each LPAR must have a different APPC/MVS base LU name. For example, if you have two LPARs and you want to use CA Mainframe Extended Terminal Manager (or CA Mainframe Configuration Manager) from LPAR 1 to access an IMS subsystem that runs on LPAR 2, you need to create multiple profiles.

Example: Define Multiple Profiles to Access IMS Systems from LPARs

LPAR SYS1 has APPC/MVS base LU name MVSLU01, and LPAR SYS2 has APPC/MVS base LU name MVSLU02. In response, you create the following profiles (for a NQN=NO environment):

```
ADCD.MVSLU01.MVSLU02
```

```
ADCD.MVSLU02.MVSLU01
```

```
ADCD.MVSLU01.MVSLU01
```

```
ADCD.MVSLU02.MVSLU02
```

The preceding profiles let you access IMS systems on SYS1 from SYS1 or SYS2 and access IMS systems on SYS2 from SYS2 or SYS1.

Sample Output from D APPC,LU,ALL Command

You can use the D APPC,LU,ALL display command to find the LU names and determine which format to use for a security profile name. The following content is sample output from the command:

```
D APPC,LU,ALL
ATB121I 12.05.30 APPC DISPLAY 796
  ACTIVE LU'S      OUTBOUND LU'S      PENDING LU'S      TERMINATING LU'S
    00006          00000          00006          00000
SIDEINFO=SYS1.APPCSI
LLUN=IMS9PPC      SCHED=IMS9          BASE=YES          NQN=NO
STATUS=ACTIVE      PARTNERS=00001      TPLEVEL=SYSTEM    SYNCPT=NO
GRNAME=*NONE*      RMNAME=*NONE*
TPDATA=SYS1.APPCTP
PLUN=ADCD.MVSLU01
LLUN=MVSLU01      SCHED=ASCH          BASE=YES          NQN=NO
STATUS=ACTIVE      PARTNERS=00004      TPLEVEL=SYSTEM    SYNCPT=NO
GRNAME=*NONE*      RMNAME=*NONE*
TPDATA=SYS1.APPCTP
PLUN=ADCD.IMSHPPC
PLUN=ADCD.IMS0PPC
PLUN=ADCD.IMS9PPC
PLUN=ADCD.MVSLU01
```

The display output shows all LU names defined to APPC on the LPAR.

More information:

Rules for Defining Security Profiles

Sample Output from the D NET,ID=lu_name Command

You can use the D NET,ID=*lu_name* display command to obtain the network ID to be used in the profile name. The following content is sample output from the command:

```
D NET,ID=MVSLU01
IST097I DISPLAY ACCEPTED
IST075I NAME = ADCD.MVSLU01, TYPE = APPL 803
```

The preceding sample shows LU name MVSLU01 and network ID ADCD. For the preceding examples, you could define the NQN=NO profiles as follows:

```
ADCD.MVSLU01.MVSLU01
ADCD.MVSLU01.IMS9PPC
ADCD.IMS9PPC.MVSLU01
```

You could also define the NQN=YES profiles as follows:

ADCD.MVSLU01.ADCD.MVSLU01

ADCD.MVSLU01.ADCD.IMS9PPC

ADCD.IMS9PPC.ADCD.MVSLU01

The preceding profiles show the profiles required for a single z/OS LPAR and single IMS environment. If you have multiple IMS subsystems, you will need multiple profiles. For each IMS subsystem, you need only one set of profiles for the APPC/IMS LU name and the APPC/MVS base LU name on the LPAR where IMS runs.

Security Profiles

You can use security profiles to control which users can perform which CA Mainframe Configuration Manager functions. The *high-level*.CIMTSAMP library contains the following sample jobs for defining security profiles:

- CFMACF2 (for CA ACF2)
- CFMTSS (for CA Top Secret)
- CFMRACF (for IBM RACF)

For the profiles that end with *imsid*, you can enter specific IMSIDs or you can create generic profiles by specifying an asterisk for the IMSID (to match all IMSIDs) or for part of the IMSID (such as DEV* or PRD*).

Note: For information about the available profiles and their usage, see the sample jobs.

Authorized User ID

Installing a CA Mainframe Configuration Manager resource update list involves updating APF-authorized libraries such as MODBLKS and issuing IMS commands. Instead of configuring each user ID with the required authorizations, you can create a single authorized user ID that lets all users create and install resource update lists regardless of their individual user ID settings.

Note: If all CA Mainframe Configuration Manager users already have the required authorities to install a resource update list, you can skip the creation of the authorized user ID and specify an asterisk (*) for the authorized user ID in the IMSID setup options. When an asterisk is specified, CA Mainframe Configuration Manager uses the requesting user ID instead of the authorized user ID to perform a resource update list install.

The new user ID must have the following authorities:

- Authority to issue all IMS commands
- Authority to update the MODBLKS and MATRIX data sets
- Authority to read MODSTAT, OLCSTAT, and all libraries in the IMS STEPLIB

The following considerations apply to the authorized user ID:

- It is used only in the APPC/MVS initiator address space.
- We suggest using CFMAPPC for the ID name because this name matches the job name used in the APPC/MVS initiator.
- The user ID must be present on the z/OS system where the IMSID is currently running.
- After you create the user ID, you must enter it in the Authorized Userid field when you use CA Mainframe Configuration Manager to create an IMSID list and set the options for each IMS system.

IMSID List

Before you can update IMS resources, you must create a list of the IMS systems to be updated by CA Mainframe Configuration Manager. After you create the list, you can update each system individually or assign the systems to groups and update all systems in a group concurrently.

Define an IMSID

The IMSID list identifies the IMS systems that are present, defines the configuration options for each IMS system, and specifies how CA Mainframe Configuration Manager will communicate with those systems. After you identify the IMS systems, you can optionally assign them to groups.

Each IMSID that you add to the IMS list is stored in a separate member of the CFMOPT options data set.

Note: The IMS systems must be started and available for you to follow these steps.

To define an IMSID

1. Display the main menu.
2. Select option **0** (Setup) and press Enter.

The Setup panel appears.

3. Select option **1** (IMSID) and press Enter.

The Setup IMS Systems panel appears.

4. Do *one* of the following:

- Type **S** *new_imsid* and press Enter.
- Type **S** next to an existing IMSID and press Enter.

The ADD IMSID or EDIT IMSID panel appears, depending on your selection.

5. Complete the following fields:

Authorized Userid

Specifies the user ID to be used by the APPC/MVS task on the z/OS image where this IMS system executes. To permit any user to create and install resource update lists regardless of individual user ID authorizations, specify the authorized userid created during CA Mainframe Configuration Manager configuration. To restrict the users who can create and install lists, specify an asterisk (*) so that the requestor's user ID is used instead. Only those user IDs that have the proper authorization for the IMS data sets will be able to create and install lists.

SYSGEN PSB Name

Specifies the name of the PSB that has been included in the IMS sysgen for use by CA Mainframe Configuration Manager.

AGN Name

(Optional) Specifies the AGN name that the installation has defined for the SYSGEN PSB name. If an AGN name has been defined, the authorized user ID must have access to it.

Note: This field applies only to IMS V9 systems in which AGN security is enabled. For IMS versions 10 and later, leave this field blank.

APPC/MVS SYSGEN TPName

Specifies the name of the APPC/MVS TP profile created during CA Mainframe Configuration Manager installation.

Default: CFMR14_CA_CONFIG_MGR

Limits: 64 characters or less

APPC Symbolic Dest

Specifies the APPC/MVS side information entry that was defined to access APPC/MVS (*not* APPC/IMS) on the z/OS system where this IMS system runs.

Press Enter.

The second ADD IMSID or EDIT IMSID panel appears with some of the data set names prepopulated.

6. Complete the following fields, entering the data set names as fully qualified names with no quotation marks:

CFMLOG

Specifies the log data set for this IMS system.

MODBLKS

Specifies the staging MODBLKS data set for this IMS system.

User MODBLKS

(Optional) Specifies a MODBLKS data set name that will be updated by the installation of resource update lists. You can use this field to enter the data set name of a backup MODBLKS data set.

MATRIX

(Optional) Specifies the staging MATRIX data set for this IMS system. Leave this field blank if you do not want CA Mainframe Configuration Manager to manage your security definitions.

Note: This field applies only to IMS V9 systems using SMU security. For IMS versions 10 and later, leave this field blank.

User MATRIX

(Optional) Specifies a MATRIX data set name that will be updated by the installation of resource update lists. You can use this field to enter the data set name of a backup MATRIX data set.

Note: This field applies only to IMS V9 systems using SMU security. For IMS versions 10 and later, leave this field blank.

Press Enter.

The third ADD IMSID or EDIT IMSID panel appears.

7. (Optional) Enter the IMS sysgen source information. These fields are needed only if you will use ISPF options 5 (Validate) and 6 (Fastgen).

The organization of the sysgen source determines how to enter this information on the panel:

- If the sysgen source does not contain assembler COPY statements, enter one sysgen data set and member name (if it is a member of a PDS) on each line.
- If the sysgen source contains COPY statements, enter the primary member name (which uses the COPY statements to call all other required members) in the Member field, and enter one PDS data set name (with no member names) on each line.

Enter fully qualified data set names with no quotation marks.

Press Enter.

The Setup IMS Systems panel reappears. You can now assign this IMS system to a group.

More information:

Define IMS Groups

Delete IMSIDs from the List

You can delete an IMSID for an IMS system that will not be updated using CA Mainframe Configuration Manager.

Note: Before you delete an IMSID, we recommend that you remove it from all IMS groups. Deleting an IMSID that is still assigned to a group renders that group unusable.

To delete IMSIDs

1. Display the main menu.
2. Select option **0** (Setup) and press Enter.
The Setup panel appears.
3. Select option **1** (IMSID) and press Enter.
The Setup IMS Systems panel appears.
4. Type **D** (Delete an IMSID) next to each IMSID to delete. Press Enter.
The IMSID Delete panel appears, displaying the first IMSID you selected.
5. Press Enter.

If you selected multiple IMSIDs, the IMSID Delete panel reappears and displays the next IMSID. You must press Enter for each IMSID.

If you selected one IMSID, the Setup IMS Systems panel reappears. The deleted IMSIDs no longer appear in the list.

More information:

Define IMS Groups

IMSID Setup Utility

You can use the IMSID Setup batch utility to view and update the IMSID list. The IMSID list identifies the IMS systems that are present, defines the configuration options for each IMS system, and specifies how CA Mainframe Configuration Manager will communicate with those systems. After you identify the IMS systems, you can optionally assign them to groups.

Each IMSID that you add to the IMS list is stored in a separate member of the CFMOPT options data set.

The IMSID Setup batch utility accesses the options data set to display and update the values assigned to an IMS system in the list.

You can access the IMSID Setup utility JCL by accessing *high-level.CIMTSAMP(CFMBIMS)*. This utility is not available through the U (Utilities) option on the main menu.

Note: You can also create IMSIDs by using option 0 (Setup) on the main menu.

Using the IMSID Setup utility instead of the ISPF interface to edit IMSID options has advantages and disadvantages. The ISPF interface automatically captures the data sets allocated to an IMS system, such as the RESLIB, MODSTAT, OLCSTAT, and MODBLKS data sets. However, the ISPF interface requires APPC/MVS to obtain the data set names, and also requires that the IMS system be running. The IMSID Setup utility can be used when IMS is not started or when APPC/MVS is not configured; however, you must specify all required data set names for the IMS system.

Note: Regardless of which method you use to edit IMSID option modules, APPC/MVS is required to use other CA Mainframe Configuration Manager functions.

EXEC Statement

The IMSID Setup batch utility requires the following EXEC statement:

```
//BIMS      EXEC PGM=CFMBIMS,PARM='&FUNCTION,IMSID=&IMSID'
```

The EXEC statement has the following parameters:

FUNCTION

Specifies the function to perform. The following values are valid:

LIST

Displays the current option values for the specified IMS system.

UPDATE

Creates or updates the option values for the specified IMS system.

Note: You can use the sample JCL in *high-level.CIMTSAMP(CFMBIMS)* for both the LIST and UPDATE functions. The JCL contains control statements to update option values but the utility does not read those statements when executing the LIST function.

IMSID

Specifies the IMS system to display or update.

Limits: Must be 4 characters

More information:

LIST Function Output.....
UPDATE Function Considerations.....

LIST Function Output

The LIST function produces an output report that shows the current option values for the specified IMS system. See the following sample report:

LIST OF OPTIONS VALUES FOR IMS xxxx

```
AUTH_USERID  = CFMAUTH
PSB_NAME     = CFMPSB
AGN_NAME     =
TP_NAME      = CFM220_IMS_CA_CONFIG
SYMDEST      = SYS1
SUFFIX       = 9
OLC          = LOCAL
CFMLOG       = IMS910.CFM.CFMLOG
RESLIB       = IMS910.SDFSRESL
MODSTAT      = IMS910.MODSTAT
MODBLKS      = IMS910.MODBLKS
MODBLKSA     = IMS910.MODBLKSA
MODBLKSB     = IMS910.MODBLKSB
USER_MODBLKS =
GEN_MEMBER   =
GEN_SOURCE    = IMS810.IMSGEN.CNTL(IMS8MACS)
               IMS810.IMSGEN.CNTL(END)
```

Note: GEN_SOURCE can have multiple data set names. In the preceding report sample, GEN_SOURCE has two data set names.

More information:

Control Statements

UPDATE Function Considerations

Consider the following when using the UPDATE function:

- Specify *all* options values in the IMSID options, not only the values you want to update. The utility replaces all IMSID option values in the options data set with the values specified in the job control statements.
- Use caution when specifying options values. CA Mainframe Configuration Manager does not perform any validation for the specified values other than syntax checking.

- All statements are coded in a “keyword = value” type of syntax. Blanks are permitted between the keyword, the equal sign, and the value but are not required. We suggest that you start the keywords in the first position of the statement to aid readability. An asterisk (*) in the first position of a statement designates it as a comment.
- Only GEN_SOURCE statements can be continued. To continue one of these statements, code a comma after the data set name and continue with the next data set name on the next statement. An example of continuation is shown in the sample job in *high-level.CIMTSAMP(CFMBIMS)*.

More information:

Control Statements

DD Statements

The IMSID Setup batch utility uses the following JCL DD statements:

STEPLIB

Specifies the CA Database Management Solutions for IMS for z/OS load library (CIMTLOAD).

CFMOPT

Specifies the CA Mainframe Configuration Manager options data set (CFMOPT).

Note: This data set must be a PDS with RECFM=U and a minimum block size of 4,096. When you use the LIST function to show currently defined options, this data set must contain a member named CFM@ followed by the IMSID. (That is, the IMS system must already be defined in the IMSID list.) When you use the UPDATE function, the utility creates or replaces the CFM@*imsid* member.

CFMPRINT

Specifies an output data set for the report generated by this utility.

Note: The data set must be defined with DCB attributes of RECFM=FBA and LRECL=133.

SYSABEND

(Optional) Specifies an output data set to contain a diagnostic dump if an abend occurs.

SYSIN

Specifies the input control statements. This DD statement is used only for the UPDATE function. You can point SYSIN to a data set that contains the control statements, or you can use SYSIN DD* and insert the statements here. When you use the UPDATE function, the utility uses the SYSIN specifications to perform the update.

Note: When you use the LIST function, SYSIN is not used and can be omitted.

Control Statements

The control statements for the IMSID Setup batch utility specify the new or updated values to apply to an IMS system. Use care when specifying control statements. An incorrect MODSTAT data set name, for example, can cause CA Mainframe Configuration Manager to update the wrong MODBLKS data set, which can cause the IMS to abend during the next restart.

The IMSID Setup batch utility supports the following control statements:

AUTH_USERID

Specifies the authorized user ID that is used to install CA Mainframe Configuration Manager resource update lists.

Limits: 8 characters or less

Note: This ID was created during CA Mainframe Configuration Manager configuration.

PSB_NAME

Specifies the PSB that has been included in the IMS sysgen for use by CA Mainframe Configuration Manager.

Limits: 8 characters or less

Note: This name was specified by the administrator during installation.

AGN_NAME

Specifies the application group name to use with the CA Mainframe Configuration Manager PSB name.

Limits: 8 characters or less

TP_NAME

Specifies the APPC TP name created for the CA Mainframe Configuration Manager APPC transaction program.

Limits: 64 characters or less

Note: This name was specified in the CFMTPADD job during CA Mainframe Configuration Manager configuration.

SYMDEST

Specifies the APPC symbolic destination associated with the MVS system where this IMS system runs.

Limits: 8 characters or less

Note: This name was specified in the CFMSIADD job during CA Mainframe Configuration Manager configuration.

SUFFIX

Specifies the IMS nucleus suffix. This suffix is the same as the value specified in the IMS control region PROC or in the DFSPBxxx member of the IMS PROCLIB data set.

Limits: 1 character

OLC

Specifies the IMS online change setting. This value must be specified as either LOCAL or GLOBAL.

Default: LOCAL

CFMLOG

Specifies the CA Mainframe Configuration Manager log data set used by this IMS system.

RESLIB

Specifies the RESLIB data set used by this IMS system. The RESLIB must contain modules DFSISDCx and DFSVNUCx (where x is the IMS nucleus suffix).

MODSTAT

(Optional) Specifies the IMS MODSTAT data set.

If the target IMS system uses global online change (and therefore uses OLCSTAT instead of MODSTAT), omit the MODSTAT DD statement and optionally include the OLCSTAT DD statement. When you include MODSTAT or OLCSTAT in your JCL, the utility uses the active MODBLKS data set (A or B). When you omit these DD statements, the utility uses the staging MODBLKS data set.

OLCSTAT

(Optional) Specifies the IMS OLCSTAT data set.

If the target IMS system uses local online change (and therefore uses MODSTAT instead of OLCSTAT), omit the OLCSTAT DD and optionally include the MODSTAT DD statement. When you include MODSTAT or OLCSTAT in your JCL, the utility uses the active MODBLKS data set (A or B). When you omit these DD statements, the utility uses the staging MODBLKS data set.

MODBLKS

Specifies the staging MODBLKS data set used by this IMS system.

MODBLKSA

Specifies the MODBLKSA data set used by this IMS system.

MODBLKSB

Specifies the MODBLKSB data set used by this IMS system.

USER_MODBLKS

(Optional) Specifies a backup data set for the current MODBLKS data set members.

GEN_MEMBER

(Optional) Specifies the member name of the base IMS sysgen source (which may contain assembler COPY statements). If you specify a GEN_MEMBER value, the data set names in the GEN_SOURCE variable must be PDS data sets without member names. If you do not specify a GEN_MEMBER value, then the GEN_SOURCE data sets must be sequential data sets or PDS data sets with member names specified.

GEN_SOURCE

Specifies the data sets where the IMS sysgen source is located. All data sets specified must have the same data set organization: sequential (or PDS with a member name) or PDS without a member name. When you specify PDS data sets without member names, you must specify a value for GEN_MEMBER because it contains the base sysgen source member (which may contain assembler COPY statements).

When you specify multiple GEN_SOURCE data sets, specify each data set completely on one line and insert a comma between data set names.

Limits: 30 data set names

More information:

CA Mainframe Configuration Manager Customization
LIST Function Output.....
UPDATE Function Considerations.....

Sample Output

When you execute the IMSID Setup batch utility, it generates a report showing the outcome of the execution.

See the following sample output:

```
PAGE      1  CA SYSGEN TOOLS  VERSION 14.0
          CFMBIMS - CA Config TOOLS IMSID SETUP
```

```
REQUEST TO UPDATE OPTIONS VALUES FOR IMS xxxx
```

```
STATEMENTS READ FROM SYSIN FILE:
```

```

*
* IMSID OPTIONS SETUP
*
AUTH_USERID  = CFMAUTH
PSB_NAME     = CFMPSTB
AGN_NAME     =
TP_NAME      = CFM220_IMS_CONFIG
SYMDEST      = SYS1
SUFFIX       = 9
OLC          = LOCAL
* DRD        = ENABLED
CFMLOG       = IMS910.CFM.CFMLOG
RESLIB       = IMS910.SDFSRESL
MODSTAT      = IMS910.MODSTAT
MODBLKS      = IMS910.MODBLKS
MODBLKSA     = IMS910.MODBLKSA
MODBLKSB     = IMS910.MODBLKSB
USER_MODBLKS =
GEN_MEMBER   =
GEN_SOURCE   = IMS810.IMGGEN.CNTL(IMS8MACS),
               IMS810.IMGGEN.CNTL(END)
               IMS810.IMGGEN.CNTL
               IMS810.IMGGEN.CNTL(REALEND)

```

Return Codes

The IMSID Setup batch utility indicates success or failure by the condition code presented at the end of the job step.

The following condition codes are possible:

0

Indicates that the utility completed successfully.

8

Indicates that an error occurred while the utility was running. Review the job output (in the CFMPRINT or JES job log) to determine the cause of the error.

12

Indicates that the utility encountered a critical error that forced immediate program termination. Analyze the output reports and correct any error conditions.

IMS Groups

CA Mainframe Configuration Manager lets you assign IMS systems to groups. After you create a group, you can verify and install resource update lists to every IMS system in the group concurrently.

Note: CA Mainframe Configuration Manager IMS groups are independent of IMSplex configurations and global online change configurations. CA Mainframe Configuration Manager does, however, support any configuration of an IMSplex with local online change, global online change, or a combination of both. If a CA Mainframe Configuration Manager group contains some, but not all, of the members of a global online change environment, CA Mainframe Configuration Manager updates only those IMS systems that are assigned to its group. Similarly, you can install an update list to one member of an IMSplex, all members of an IMSplex, or some members of multiple IMSplexes. IMS systems can be on the same or different z/OS systems.

Define IMS Groups

After you define your IMSID list, you can assign the IMS systems to groups. An IMS system can belong to more than one group.

Each group that you define is stored in a separate member of the CFMOPT options data set.

To define IMS groups

1. Display the main menu.
2. Select option **0** (Setup) and press Enter.

The Setup panel appears.

3. Select option **2** (Group) and press Enter.

The Setup Groups panel appears.

4. Do *one* of the following:

- Type **S** *new_group_name* and press Enter.

Note: The group name can be up to eight characters but cannot start with CFM.

- Type **S** next to an existing group name and press Enter.

The ADD a Group or EDIT a Group panel appears, depending on your selection. Both panels show all IMS systems that have been added to your IMSID list.

5. Enter any character (such as a slash) next to each IMSID to include in the group.

Note: You can delete the character next to an IMSID to remove it from the group.

Press PF3 (End).

The selected IMSIDs are saved as a group. The Setup Groups panel reappears, displaying the name of the group.

Delete IMS Groups

You can delete an IMS group that is no longer needed.

To delete IMS groups

1. Display the main menu.
2. Select option **0** (Setup) and press Enter.

The Setup panel appears.

3. Select option **2** (Group) and press Enter.

The Setup Groups panel appears.

4. Type **D** (Delete a Group) next to each group to delete. Press Enter.

The Group Delete panel appears, displaying the first group name you selected.

5. Press Enter.

If you selected multiple groups, the Group Delete panel reappears and displays the next group name. You must press Enter for each group name.

If you selected one group, the Setup Groups panel reappears. The deleted group names no longer appear in the list.

How to Set Up User Authorities

CA Mainframe Configuration Manager lets you control the resource definitions that users can update when working with resource update lists. For example, if your site does not allow conversational transactions, you can prohibit users from entering a value in the SPA size field and make the default SPA size blank. Also, if your site requires that all transactions be defined as MODE=SNGL, you can change the default from MODE=MULT to MODE=SNGL and prohibit specific users from changing the default value. You can also provide default values but permit users to override them.

You define these permissions by creating authorization profiles. A profile specifies the default values for each attribute and whether users can change those defaults. You can create several different profiles, with each one having different settings. After you create the profiles, you assign each user to a profile.

Note: Authorization profiles are optional. If no profiles exist, all users have access to all attributes.

To set up user authorities, do the following:

1. [Create an authorization profile](#) (see page 94).
2. [Assign users to the authorization profile](#) (see page 96).

Create or Edit an Authorization Profile

CA Mainframe Configuration Manager lets you define authorization profiles that specify which resource attributes can be updated, and the default value for each attribute. You can define multiple profiles. After you define a profile, you can define user IDs and assign them to the profile.

Important! Be careful when editing existing authorization profiles. Your edits can result in inadvertent changes to resource definitions. When you edit an existing authorization profile, the new settings are applied to any future resource update lists created by the profile's assigned users. For example, if you edit a profile to change SPA SIZE 16 to SPA SIZE blank, and then a user assigned to that profile creates and installs a new resource update list, CA Mainframe Configuration Manager forces the new SPA SIZE setting even if the user only intended to change another setting (for example, change MODE from MULT to SNGL).

Note: CA Mainframe Configuration Manager does not apply the settings in an authorization profile until you assign users to it and those users create resource update lists. Also, authorization profiles are optional. If no profiles exist, all users have access to all attributes.

The authorization profiles are stored in a member of the CFMOPT options data set.

To create or edit an authorization profile

1. Display the main menu.
2. Select option **0** (Setup) and press Enter.
The Setup panel appears.
3. Select option **3** (Profiles) and press Enter.
The List of Authorization Profiles panel appears.
4. Do *one* of the following:
 - Type **S** *new_profile_name* (for example, S NEWNAME) on the CMD line. The name can be up to eight characters.
 - Type **S** (Edit a Profile) next to an existing profile name.
 Press Enter.
 The Profile Authorizations panel appears, showing the default settings for the selected profile. This panel shows all resource attributes for database, program, transaction, and route code definitions.
5. Define the profile settings:
 - (Optional) Enter a meaningful description in the Profile Description field. This description appears in the profile list to identify the purpose of the profile.
 - Scroll through the panel, changing default values where needed and entering **Y** or **N** in the Allow Updates field to specify whether users assigned to this profile can change the default value when working with resource update lists.

Press Enter.

CA Mainframe Configuration Manager verifies that all values in the Default Value field are valid. If all values are valid, you will see no change. If you entered any invalid values, "Invalid Value" appears at the top of the panel and the cursor moves to the first invalid value so that you can correct it.

Note: If you exit the panel without correcting an invalid value, CA Mainframe Configuration Manager replaces the invalid value with question marks. If a user tries to install an update list with an invalid value the installation will fail.

Press PF3 (End).

CA Mainframe Configuration Manager saves your settings and displays the List of Authorization Profiles panel again. The profile name appears in the list. You can now assign users to the profile.

More information:

Assign Users to an Authorization Profile

Delete an Authorization Profile

You can delete authorization profiles that are not in use.

Note: If you try to delete a profile that still has assigned users, CA Mainframe Configuration Manager displays a "Profile in Use" message. Before you delete a profile, you can verify whether it has any assigned users by [viewing the user list](#) (see page 96).

To delete an authorization profile

1. Display the main menu.
2. Select option **0** (Setup) and press Enter.
The Setup panel appears.
3. Select option **3** (Profiles) and press Enter.
The List of Authorization Profiles panel appears.
4. Type **D** (Delete a Profile) next to each profile to delete. Press Enter.
The Authorization Profile Delete panel appears, displaying the first profile name you selected.
5. Press Enter.
If you selected multiple profiles, the Authorization Profile Delete panel reappears and displays the next profile name. You must press Enter for each profile name.
If you selected one profile, the List of Authorization Profiles panel reappears. The deleted profiles no longer appear in the list.

Assign Users to an Authorization Profile

After you create authorization profiles, you can create a list of users and assign each one to an appropriate profile. A user can be assigned to only one authorization profile. The assigned profile controls the default values that are applied to resource attributes when the user creates or edits a resource update list, and also controls which defaults the user can change.

Note: You can also follow the beginning of this procedure to view the user list, which is useful for verifying that no users are assigned to an authorization profile that you plan to delete.

You can enter generic user IDs in your list by using the pound sign (#) as a wildcard character. The pound sign matches one character of a TSO user ID. For example, enter `IMS#####` to create an entry that matches any user ID starting with `IMS`.

Note: When you enter user IDs with wildcards, their placement in the list affects how CA Mainframe Configuration Manager assigns users to authorization profiles.

The user IDs are stored in a member of the options data set specified on the CA Mainframe Configuration Manager Setup panel.

To assign users to an authorization profile

1. Display the main menu.
2. Select option **0** (Setup) and press Enter.
The Setup panel appears.
3. Select option **4** (Users) and press Enter.
The Setup User Profiles panel appears, showing any user IDs that have been created and their assigned authorization profiles.
4. Do *one* of the following:
 - Type **S** *new_user_name* (for example, `S USER01`) on the CMD line. The name can be up to eight characters.
 - Type **S** (Edit a user) next to an existing user name.
 - Type **I** (Insert new user) next to an existing user name.Press Enter.
The User Profile panel appears.
5. Complete the following fields:
 - Enter a new user name in the Userid field (if you specified **I** in the preceding panel).
 - Enter the name of an existing profile in the Profile field.

Press Enter.

CA Mainframe Configuration Manager verifies that the specified profile name exists. If the name does not exist, "Invalid Profile" appears at the top of the panel. You must enter a valid profile name to exit the panel. If the name exists, the Setup User Profiles panel reappears with the user name displayed in the list.

Note: If you specified **I** to insert a new user, the new user appears below the selected user name. Press F7 and F8 to scroll through the list.

Rearrange the Users in the List

The order of user entries in the user list is significant. CA Mainframe Configuration Manager searches the list in order and uses the first entry that matches the TSO user ID. If ##### (a user name consisting of all wildcards) is the first entry in the list, every TSO user will match this entry, and will use its assigned authorization profile. If ##### is the last entry in the list, its assigned profile will be used only for user IDs that do not match any of the preceding list entries.

To rearrange the users in the list

1. Display the main menu.
2. Select option **0** (Setup) and press Enter.
The Setup panel appears.
3. Select option **4** (Users) and press Enter.
The Setup User Profiles panel appears, showing any user IDs that have been created and their assigned authorization profiles.
4. Type **M** (Move a user) next to a user ID, and then type **B** (Before) or **A** (After) next to another user ID. Press Enter.
The first user ID is moved immediately before or after the second user ID.
5. Repeat step 4 as needed to rearrange other users in the list.
6. Press PF3 (End).
The rearranged list is saved and the Setup panel reappears.

Delete Users from the List

You can delete user IDs that are not in use.

To delete users from the list

1. Display the main menu.
2. Select option **0** (Setup) and press Enter.
The Setup panel appears.
3. Select option **4** (Users) and press Enter.
The Setup User Profiles panel appears, showing any user IDs that have been created and their assigned authorization profiles.

4. Type **D** (Delete user) next to each user ID to delete. Press Enter.

The User Delete panel appears, displaying the first user ID you selected.

5. Press Enter.

If you selected multiple user IDs, the User Delete panel reappears and displays the next user ID. You must press Enter for each user ID.

If you selected one user ID, the Setup User Profiles panel reappears. The deleted user IDs no longer appear in the list.

CA Mainframe Extended Terminal Manager Customization

If you have installed CA Mainframe Extended Terminal Manager, you must configure the product. To customize CA Mainframe Extended Terminal Manager, follow these steps:

1. [Allocate and initialize the options data set](#) (see page 99).
2. [Set up the online refresh capability](#) (see page 100).
3. [Set required parameters for IMS systems where the product will be used](#) (see page 102).
4. [Customize each IMS where the product will be used.](#) (see page 102)
5. (Optional) [Implement CA Mainframe Extended Terminal Manager Support for the IMS Build Security \(DFSBSEX0\) User Exit](#) (see page 103)

Allocate and Initialize the Options Data Set

To allocate and initialize the CA Mainframe Extended Terminal Manager VSAM options data set, you need to use the following members in *high-level.CIMTSAMP*:

- ETMD1MDA member (to build the dynamic allocation member for the options data set)
- ETMD1INI member (to allocate and initialize the options data set)

Note: The options data set may be unique to a single IMS system or shared between IMS systems that have similar customization requirements.

To allocate and initialize the options data set

1. Access member ETMD1MDA in *high-level.CIMTSAMP* and customize the member as needed.
2. Customize SET statements as needed to reflect your values.

Note: The options data set is a VSAM data set, so choose a naming convention that fits with your installation standards for a VSAM data set.

3. Execute the job defined in ETMD1MDA.

This job builds the dynamic allocation member and places it in the library specified by MDALIB in the JCL.

Note: The dynamic allocation member must reside in a data set that is accessible to all IMS message regions (MPRs) in which the CA Mainframe Extended Terminal Manager online transaction (EMTRAN) runs. The dynamic allocation member must reside in a STEPLIB library for the IMS control region.

4. Access member ETMD1INI in *high-level*.CIMTSAMP and customize the member as follows:

- Customize SET statements as needed to reflect your values.

Note: Make sure to use the same options data set name used in the previous job.

- Set a value for DB1TITL to display a title for this options data set.

5. Execute the job defined in ETMD1INI.

The options data set is allocated and initialized.

Enable Online Refresh Capability

CA Mainframe Extended Terminal Manager can refresh the options data set by using one of the following:

- EMTRAN transaction (which uses APPC/MVS and APPC/IMS to dynamically refresh the ECSA tables from the options data set)

CA Mainframe Extended Terminal Manager uses APPC/MVS to communicate across systems.

- Batch job (which does *not* require APPC/MVS or APPC/IMS)

If you do not want to use APPC/MVS, you can use the batch refresh job (on each LPAR) instead of the online refresh function.

If you want to use the EMTRAN refresh, you must add a TP profile entry and a side information entry.

Note: You also need a VTAM mode name that can be used for APPC (LU 6.2). The VTAM support personnel in your organization might know a mode table entry name that can be used for this purpose.

Follow these steps:

1. Verify that APPC/MVS is installed and active by issuing the following z/OS commands:

D APPC,LU,ALL

 Informs you whether APPC is active, reveals the name of the APPC TP profile data set, and reveals the name of the APPC/MVS base LU on the LPAR.

D ASCH,ALL

 Reveals the APPC scheduler class name that is in place on the LPAR.

2. Customize member ETMSIDEI in *high-level.CIMTSAMP* to define one APPC symbolic definition for each LPAR where an IMS system executes.
3. Customize member ETMTPADD in *high-level.CIMTSAMP* to define the APPC TP profile on each LPAR where an IMS system executes.
4. Specify SECACPT=ALREADYV or SECACPT=AVPV in the VTAMLST definition for the APPC base LU.
5. Specify any site-specific settings (such as APPCLU class profiles) as needed to conform to your security environment.
6. Activate APPC/IMS by doing the following.

Note: If APPC/IMS is already active in IMS, no additional definitions are required.

- Customize the ETMAPPC member in the sample library to add an APPC/IMS LU definition to the z/OS PARMLIB member APPCCMxx.

Note: The SCHED value must be the IMSID of the IMS system.

- Customize the ETMVTAM member in the sample library to add an LU definition to SYS1.VTAMLST for the ACBNAME specified in the LU definition.

Note: The label on the ACBNAME statement and the ACBNAME= parameter must match the ACBNAME on the LU definition.

More information:

APPC/MVS.....
How to Enable ALREADYV Security for APPC/MVS LUs.....

Set ETO and APPC Parameters for IMS Systems Where CA Mainframe Extended Terminal Manager Is Used

In your DFSPBxxx PROCLIB member, verify that the following parameter specifications are active for IMS systems where CA Mainframe Extended Terminal Manager is used:

ETO=Y

Specifies that IMS ETO is active.

APPC=Y

Specifies that APPC/IMS is active.

Customize Each IMS where CA Mainframe Extended Terminal Manager Will Be Used

To customize each IMS where CA Mainframe Extended Terminal Manager will be used, follow these steps:

- Update the IMS control region JCL to specify the CA Mainframe Extended Terminal Manager load library in the STEPLIB concatenation.

This load library does not have to be specified before the IMS SDFSRESL data set; however, if you are using any of the following IMS exits, they must be renamed to names supported by CA Mainframe Extended Terminal Manager:

- DFSINTX0
- DFSCCMD0
- DFSGMSG0
- DFSSGNX0
- DFSSGFX0
- DFSINSX0
- DFSPPU0
- DFSLGNX0
- DFSLGFX0

- For any message region where the CA Mainframe Extended Terminal Manager transaction can execute, update the IMS message region JCL to contain the CA Database Management Solutions for IMS for z/OS load library.

- Add the CA Mainframe Extended Terminal Manager transaction EMTRAN to your IMS system.

Note: For the IMS sysgen definition, see the samplib member ETMGEN02.

- Add a member ETMIimsid to the PROCLIB data set used by the IMS system where you want to activate CA Mainframe Extended Terminal Manager. Specify ETM=YES in the ETMIimsid member and restart the IMS system to activate CA Mainframe Extended Terminal Manager.

More information:

Resolve Multiple IMS Partner Product User Exits

Implement Support for the IMS Build Security (DFSBSEX0) User Exit

The IMS Build Security user exit (DFSBSEX0) determines how to build the security environment in an IMS dependent region for certain call types. You can implement CA Mainframe Extended Terminal Manager support for the DFSBSEX0 user exit.

To enable CA Mainframe Extended Terminal Manager to help manage the DFSBSEX0 user exit, execute the job defined in the *hlq.CIMTSAMP(ETMBSEXZ)* member.

APPC/MVS

APPC/MVS is primarily used to implement client-server communications across mainframe systems. CA Mainframe Extended Terminal Manager requires APPC/MVS, even in a single-system environment, for the following reasons:

- APPC/MVS provides APF authorization, which CA Mainframe Extended Terminal Manager requires to perform various functions.
- APPC/MVS enables communication across z/OS images, which lets users refresh the CA Mainframe Extended Terminal Manager options data set in IMS systems on different z/OS images.

APPC/MVS is part of the base z/OS product and is typically already installed before you install CA Mainframe Extended Terminal Manager. For CA Mainframe Extended Terminal Manager to use APPC/MVS, you must set up side information entries and a TP profile. You can perform these tasks by running the JCL jobs provided with CA Mainframe Extended Terminal Manager.

Note: For more information about installing APPC/MVS, see the IBM *MVS Planning: APPC Management* document.

More information:

Enable Online Refresh Capability

How to Enable ALREADYV Security for APPC/MVS LUs

The APPC/MVS LUs used by CA Mainframe Extended Terminal Manager and CA Mainframe Configuration Manager must use ALREADYV security. These LUs include the following:

- APPC/MVS base LU on the z/OS system where the IMS is located
- APPC/MVS base LU on the z/OS system where IMS is running
- APPC/IMS LU

To enable ALREADYV security for APPC/MVS LUs, do *one* of the following to override the SECACPT= value in the VTAM APPL definition in VTAMLST:

- Specify SECACPT=ALREADYV or SECACPT=AVPV for the LUs.
- Define security profiles to override the SECACPT= value.

Rules for Defining Security Profiles

Profiles must be defined in the APPCLU class to override session conversation security—SESSION(CONVSEC(ALREADYV)). APPCLU profiles let you override the SECACPT= value for a conversation between two specific LU names. The profile name, which includes both LU names involved in the session, has a format that is determined as follows:

If the LU names specify NQN=NO, the following profile name format is used:

network-id.local-lu-name.remote-lu-name

If the LU names specify NQN=YES, the following profile name format is used:

network-id.local-lu-name.network-id.remote-lu-name

Note: You can optionally define both forms of the APPCLU profiles. If this is done when the profiles are initially defined, a change in the NQN specification will not require changes in the defined security profiles.

To find the LU names and determine which profile name format to use, you can issue a D APPC,LU,ALL command and review the output. To determine which LU names are needed in the profile names, find the base LU for APPC/MVS and the IMS APPC LU. The base LU will show SCHED=ASCH and BASE=YES. The IMS APPC LU name will show SCHED=*imsid* and BASE=YES.

Note: You can also obtain the network ID by issuing the D NET,ID=*lu_name* display command.

Obtaining the Network ID for a Security Profile Name

You can obtain the network ID to be used in a security profile name by issuing the following display command:

```
D NET, ID=lu_name
```

In the resulting output, the IST075I message shows the network name before the LU name.

More information:

Sample Output from the D NET, ID=lu_name Command

Conversational Security Settings for Profiles

When defining your security profiles, specify a value for SESSION CONVSEC of ALREADYV (or AVPV). If you use RACF, use the following command format to define these profiles (for an NQN=NO environment):

```
RDEFINE ADCD.MVSLU01.MVSLU01 UACC(NONE) -SESSION(CONVSEC(ALREADYV))
```

```
RDEFINE ADCD.MVSLU01.IMS9PPC UACC(NONE) -SESSION(CONVSEC(ALREADYV))
```

```
RDEFINE ADCD.IMS9PPC.MVSLU01 UACC(NONE) -SESSION(CONVSEC(ALREADYV))
```

If you have VERIFY=REQUIRED on the VTAM APPL definitions in VTAMLST, you may also require session key definitions in the RACF commands.

Note: For more information about session keys, see the IBM *z/OS MVS Planning: APPC/MVS Management* and *z/OS Security Server RACF Command Language Reference*.

More information:

Rules for Defining Security Profiles

Defining Multiple Profiles for Multiple LPARs

If you have multiple LPARs, each LPAR must have a different APPC/MVS base LU name. For example, if you have two LPARs and you want to use CA Mainframe Extended Terminal Manager (or CA Mainframe Configuration Manager) from LPAR 1 to access an IMS subsystem that runs on LPAR 2, you need to create multiple profiles.

Example: Define Multiple Profiles to Access IMS Systems from LPARs

LPAR SYS1 has APPC/MVS base LU name MVSLU01, and LPAR SYS2 has APPC/MVS base LU name MVSLU02. In response, you create the following profiles (for a NQN=NO environment):

ADCD.MVSLU01.MVSLU02

ADCD.MVSLU02.MVSLU01

ADCD.MVSLU01.MVSLU01

ADCD.MVSLU02.MVSLU02

The preceding profiles let you access IMS systems on SYS1 from SYS1 or SYS2 and access IMS systems on SYS2 from SYS2 or SYS1.

Sample Output from D APPC,LU,ALL Command

You can use the D APPC,LU,ALL display command to find the LU names and determine which format to use for a security profile name. The following content is sample output from the command:

```
D APPC,LU,ALL
ATB121I 12.05.30 APPC DISPLAY 796
  ACTIVE LU'S      OUTBOUND LU'S      PENDING LU'S      TERMINATING LU'S
    00006          00000          00006          00000
SIDEINFO=SYS1.APPCSI
LLUN=IMS9PPC      SCHED=IMS9      BASE=YES      NQN=NO
STATUS=ACTIVE      PARTNERS=00001      TPLEVEL=SYSTEM      SYNCPT=NO
GRNAME=*NONE*      RMNAME=*NONE*
TPDATA=SYS1.APPCTP
PLUN=ADCD.MVSLU01
LLUN=MVSLU01      SCHED=ASCH      BASE=YES      NQN=NO
STATUS=ACTIVE      PARTNERS=00004      TPLEVEL=SYSTEM      SYNCPT=NO
GRNAME=*NONE*      RMNAME=*NONE*
TPDATA=SYS1.APPCTP
PLUN=ADCD.IMSHPPC
PLUN=ADCD.IMS0PPC
PLUN=ADCD.IMS9PPC
PLUN=ADCD.MVSLU01
```

The display output shows all LU names defined to APPC on the LPAR.

More information:

Rules for Defining Security Profiles

Sample Output from the D NET,ID=lu_name Command

You can use the D NET,ID=*lu_name* display command to obtain the network ID to be used in the profile name. The following content is sample output from the command:

```
D NET,ID=MVSLU01

IST097I DISPLAY ACCEPTED

IST075I NAME = ADCD.MVSLU01, TYPE = APPL 803
```

The preceding sample shows LU name MVSLU01 and network ID ADCD. For the preceding examples, you could define the NQN=NO profiles as follows:

```
ADCD.MVSLU01.MVSLU01

ADCD.MVSLU01.IMS9PPC

ADCD.IMS9PPC.MVSLU01
```

You could also define the NQN=YES profiles as follows:

```
ADCD.MVSLU01.ADCD.MVSLU01

ADCD.MVSLU01.ADCD.IMS9PPC

ADCD.IMS9PPC.ADCD.MVSLU01
```

The preceding profiles show the profiles required for a single z/OS LPAR and single IMS environment. If you have multiple IMS subsystems, you will need multiple profiles. For each IMS subsystem, you need only one set of profiles for the APPC/IMS LU name and the APPC/MVS base LU name on the LPAR where IMS runs.

More information:

Defining Multiple Profiles for Multiple LPARs
Obtaining the Network ID for a Security Profile Name

CA Mainframe Program Restart Manager Customization

If you have installed CA Mainframe Program Restart Manager, you must configure the product.

To configure CA Mainframe Program Restart Manager, follow these steps:

1. [Remove pause features](#) (see page 108).
2. [Prepare the JCL library](#) (see page 109).
3. [Allocate the libraries](#) (see page 110).

4. [Allocate and initialize the options data set](#) (see page 110).
5. (Optional) [Define checkpoint IDs](#) (see page 110).
6. (Optional) [Create a bypass table](#) (see page 111).
7. [Secure the data sets](#) (see page 111).
8. (Optional) [Create test libraries](#) (see page 112).
9. [Install the IMS usermod](#) (see page 113).
10. [Set up the ISPF interface](#) (see page 66).
11. [Set the CA Mainframe Program Restart Manager options](#) (see page 113).
12. [Verify the installation](#) (see page 113).
13. [Make the CA Mainframe Program Restart Manager libraries available](#) (see page 117).

Remove Pause Features

The pause features in the following products must be removed before installing CA Mainframe Program Restart Manager because they cause conflicts:

- IBM IMS Program Restart Facility
This product provides the same functionality as CA Mainframe Program Restart Manager.
- IBM IMS Online Reorg Facility
Note: For instructions to remove the BMP pausing feature of this product, see the *IBM IMS Online Reorganization Facility User's Guide*.
- IBM IMS Recovery Expert for z/OS
Note: For instructions to remove the BMP interface in this product, see the *IBM IMS Recovery Expert for z/OS User's Guide*.
- IBM IMS Batch Backout Manager
This product provides the same functionality as CA Mainframe Program Restart Manager.

Prepare JCL Library

This is not a required step, but it can save you time when editing the JCL used in subsequent steps. If you have a tool to perform mass changes to PDS JCL, such as CA PDSMAN, copy the CIMTSAMP library to another library and use the utility to change the following in all JCL members:

Change this JCL Value:	To this:
(ACCT)	Your JOB statement account value
CLASS=F	Your preferred JOB class
MSGCLASS=R	Your preferred JOB message class
IMS.ACBLIB	Your ACBLIB data set name
IMS.DBDLIB	Your DBDLIB data set name
IMS.MDALIB	Your MDALIB data set name
IMS.PSBLIB	Your PSBLIB data set name
IMS.SDFSMAC	Data set name of IMS maclib
IMS.SDFSRESL	Data set name of IMS reslib
<i>hlq</i> .CIMTLOAD	Data set name of CA Mainframe Program Restart Manager loadlib
<i>hlq</i> .CIMTSAMP	Data set name of CA Mainframe Program Restart Manager samplib
IMS.PRMUSRL	Data set name for site-specific modules
IMS.PRMRESL	Data set name for IMS release-specific modules
IMS.PRMOPTS	Data set name for site-specific options

Allocate Libraries

Modify and execute the following sample jobs to allocate load module libraries:

PRMAUSRL

Allocates the PRMUSRL library that contains user-supplied load modules, including PRM#CNTL.

PRMARESL

Allocates the PRMRESL library that contains IMS release-specific modules.

PRMCRESL

(Optional) Copies the modules that the PRM SMP/E usermods updated from the SDFSRESL library to the PRMRESL library.

Allocate and Initialize the Options Data Set

To allocate and populate the options data set, use the sample JCL in sample library member PRMAOPTS. (The options used initially are near the bottom of the JCL.)

You can modify the options before submitting the JCL or wait until the ISPF interface has been set up and modify them there.

Define Checkpoint IDs (Optional)

You can optionally define a checkpoint ID table to apply CA Mainframe Program Restart Manager processing options to batch jobs based on a particular checkpoint ID. This table lets you dynamically apply restart options by specifying one of the checkpoint IDs in a batch job's JCL.

For example, you can set up an entry in the checkpoint ID table called NOXRST681 that disables automatic restart and sets the CA Mainframe Program Restart Manager processing option CKPTID=NOMSG681. Then you can code CKPTID=NOXRST681 in the job's JCL. When the job runs, two things happen automatically:

- CA Mainframe Program Restart Manager does not restart the job.
- DFS681 messages are not issued.

Note: For more information about processing options like CKPTID, see the *CA Mainframe Program Restart Manager User Guide*.

A sample job to create a checkpoint ID table is provided in the *hlq.CIMTSAMP* member *PRM#CPID*. It defines four special checkpoint IDs that can be specified in a batch job's JCL. The CA Mainframe Program Restart Manager options defined in the checkpoint ID table are used when any of those four checkpoint IDs is encountered in a batch job's JCL.

Note: If a checkpoint ID table is not defined, CA Mainframe Program Restart Manager does not provide any automatic checkpoint ID overrides.

Before submitting the sample library member, update the assembler source statements that follow the *//SYSIN DD* statement to reflect the special checkpoint ID values and the CA Mainframe Program Restart Manager options to be associated with them at your site. The checkpoint IDs are specified by using the *CKPTID=* parameter when executing the *DLIBATCH*, *DBBATCH*, *IMSBATCH*, or *DFSJBP* procedure.

Create Bypass Table (Optional)

Bypass table stores ddnames with the specification which CA Mainframe Program Restart Manager processing to bypass if the ddname is found in the job. CA Mainframe Program Restart Manager checks the bypass table as each job is initialized. If the job JCL includes a ddname that is listed in the table, CA Mainframe Program Restart Manager bypasses the functions defined in the bypass table. Each ddname listed in the bypass table can be defined to force the bypassing of batch backout processing, program restart processing, or of all CA Mainframe Program Restart Manager processing.

Note: For more information about excluding objects from CA Mainframe Program Restart Manager processing, see the *CA Mainframe Program Restart Manager User Guide*. For a sample JCL to create the bypass table, see the member *PRM#IGNR* in the *hlq.CIMTSAMP* library.

Secure the Data Sets

Create the specified level of security for the following data sets:

Options Data Set

READ Access

All jobs processed by CA Mainframe Program Restart Manager.

Anyone using the ISPF interface for CA Mainframe Program Restart Manager administration.

ALTER Access

Anyone authorized to update the options.

Checkpoint Tracking Data Sets (CTDS)

CA Mainframe Program Restart Manager records checkpoint information for each batch job in two small checkpoint tracking data sets (CTDSs). CA Mainframe Program Restart Manager dynamically allocates the CTDSs when a batch job starts, and deletes CTDSs after the job restarts and runs to completion. CA Mainframe Program Restart Manager retains CTDSs only when the job abends. The high-level qualifier for the CTDS is set initially by the CTDSHLQ parameter in the PRMAOPTS sample library job. Users must have the following permissions to access the CTDSs:

READ Access

Anyone using the ISPF interface for CA Mainframe Program Restart Manager administration.

ALTER Access

All jobs processed by CA Mainframe Program Restart Manager.

Anyone using the ISPF interface to change restart parameters.

Batch Backout Data Sets (BBDS)

CA Mainframe Program Restart Manager tracks the need for backout using a small batch backout data set (BBDS). CA Mainframe Program Restart Manager dynamically allocates the BBDS before a batch job starts, and deletes the BBDS when the job runs successfully or when batch backout is successful or not needed after an application program failure. CA Mainframe Program Restart Manager retains BBDS only when a job abends. The high-level qualifier for the BBDS is set initially by the BBDSHLQ parameter in the PRMAOPTS sample library job. Users must have the following permissions to access the BBDS:

READ Access

Anyone using the ISPF interface for CA Mainframe Program Restart Manager administration.

ALTER Access

All jobs processed using the batch backout features of CA Mainframe Program Restart Manager.

Create Test Libraries (Optional)

If you are installing the product on a temporary (trial) basis, you can modify the IMS modules to create libraries with which you can test the product.

To create the test libraries, modify and submit the sample job that is provided in the *hlq.CIMTSAMP(PRMTSTnn)* member, where *nn* indicates the version number of IMS you use for testing.

Install the IMS Usermod

If you are not using test libraries, install the IMS usermod that updates IMS program DFSRRC00 to call CA Mainframe Program Restart Manager.

Modify and submit these sample jobs in the CIMTSAMP library:

PRMSRCV

Receives the usermod.

PRMSAPP

Applies the usermod.

Set the CA Mainframe Program Restart Manager Options

Use the CA Mainframe Program Restart Manager ISPF interface or the ISPF Edit function to edit the processing options.

Note: For information about using the CA Mainframe Program Restart Manager ISPF interface and about the processing options, see the *CA Mainframe Program Restart Manager User Guide*.

Verify the Installation

An installation verification program (IVP) allows you to perform basic testing of the CA Mainframe Program Restart Manager features and functions after installation to confirm that CA Mainframe Program Restart Manager is installed properly. It uses the IMS PART database (DI21PART) created during the IMS installation process and a GSAM database created during CA Mainframe Program Restart Manager IVP setup.

The IVP supports both DL/I batch and BMP job execution.

You can also allow other applications to test with CA Mainframe Program Restart Manager installed by changing the IMS batch job JCL for these applications to add the PRMUSRL, PRMRESL (if job PRMTSTxx is used), and CIMTLOAD data sets to their STEPLIB concatenations.

Note: These libraries *must* come before the IMS RESLIB data set.

To verify the installation, follow these steps:

1. (BMP mode) [Add the IVP PSB to the IMS sysgen](#) (see page 114).
2. [Generate IVP DBD and PSBs](#) (see page 114).
3. [Allocate and initialize IVP data sets](#) (see page 114).
4. [Allocate and load the PART database](#) (see page 114).
5. (BMP mode) [Perform an ACBGEN for the IVP PSB](#) (see page 115).

6. (BMP mode) [Activate the IVP ACBLIB members](#) (see page 115).
7. [Run the IVP](#) (see page 115).
8. [Change the IVP options](#) (see page 116).
9. [Test the processing options](#) (see page 117).

Add the IVP PSB to the IMS SYSGEN

This step is optional. It is required only if you want to execute the IVP in BMP mode.

Note: You can continue the IVP if updating your IMS sysgen will take some time, but you cannot execute the BMP IV job PRMIVBMP until this definition is in place.

Add the following application program definition (also found in CIMTSAMP library member PRMIVS1M) to your IMS sysgen:

```
APPLCTN PSB=PRMIVPS1,PGMTYPE=BATCH
```

Generate IVP DBD and PSBs

Modify and submit the PRMIVDEF sample library job to define IVP DBD PRMIVGS1 for the GSAM database, PSB PRMIVPLD to load the PART database, and PSB PRMIVPS1 to access the database and create the GSAM database.

Allocate and Initialize IVP Data Sets

Sample job PRMIVINI in the CIMTSAMP data set contains sample JCL to allocate the IVP GSAM database data set and define a GDG to be used for IMS logs created during the IVP. The job also removes any existing GDG entries, GDG base, or IVP database that currently exists.

The job sets the high-level qualifier of the database and GDG base to the submitting TSO user's ID. You can change this high-level qualifier to any data set name prefix you choose.

Allocate and Load the PART Database

This step is required only if you do not have the IMS IVP PART database. This might be the case if you deleted the IVP components after the IMS installation.

Note: Skip this step if the PART database is created and a DFSMDA member points to the database data sets.

Sample job PRMIVBLD in the CIMTSAMP data set contains sample JCL to allocate and load the database.

Perform an ACBGEN for the IVP PSB

This step is required only if you want to execute the IVP in BMP mode.

Use the PRMIVACB sample job in the *hlq.CIMTSAMP* library to perform the ACBGEN process.

Note: The DBDLIB specified must contain not only the DBD generated above, but also the DI21PART DBD from the IMS installation IVP.

Activate the IVP ACBLIB Members

This step is required only if you want to execute the IVP in BMP mode.

Use the ACBLIB update process defined for your site to make the IVP ACB members available to the IMS online system. You can use IMS online change for ACBLIB to implement the updated ACBLIB members.

Run the IVP

Running the installation verification program (IVP) in DL/I or BMP mode helps you verify that CA Mainframe Program Restart Manager is installed and working properly. This procedure describes how to run the IVP with or without the batch backout features.

Follow these steps:

1. Run the IVP using the following sample jobs:
 - PRMIVDL1—Runs the IVP in DL/I mode with batch backout feature.
The job abends with a U3619 abend code the first time it runs, after performing a batch backout.
 - PRMIVDL2—Runs the IVP in DL/I mode without batch backout feature.
The job abends with a U3619 abend code the first time it runs.
 - PRMIVBMP—Runs the IVP in BMP mode.
The job abends with a U3619 abend code when run first time.
Note: If you ran job PRMIVBLD to create the PART database, uncomment the two DD statements near the bottom of PRMIVDLn before submitting the job.
2. See the JES log and verify that CA Mainframe Program Restart Manager was processing the job.
 - If you run the IVP in DL/I mode with batch backout feature, the following messages appear:

PRM2001I AUTOBK0 SUPPORT ENABLED FOR JOB PRMIVDL1

If the program restart features are being used, the following message appears:

PRM0001I CKPTID TRACKING IS ACTIVE

After the application program abends, IMS issues the following message:

```
DFS036A BATCH BACKOUT IS REQUIRED FOR PRMIVDL1
```

Then CA Mainframe Program Restart Manager invokes batch backout and when it completes, the following messages appear:

```
PRM2006I DFSBB000 RC=00000000
```

```
PRM2044I AUTOBK0 FOR SUBSYSTEM PRMIVDL1 COMPLETE
```

If you are *not* using the program restart features, the verification is complete. Otherwise, proceed to step 4.

- If you run the IVP in DL/I mode without batch backout feature or in BMP mode, the following message appears:

```
PRM0001I CKPTID TRACKING IS ACTIVE
```

3. If you run the IVP in BMP mode, restart the program by issuing the following IMS command:

```
/STA PGM PRMIVPS1
```

4. Resubmit the job.

The application restarts and the job completes without abending.

5. See the JES log and verify that CA Mainframe Program Restart Manager passed the last valid checkpoint to the IVP program.

The following messages appear:

```
PRM0017I LAST VERIFIED XRST CKPTID=00000003
```

```
DFS0540I *XRST IN PROGRESS
```

```
* PROGRAM=PRMIVPGM, CKPTID=00000003
```

Change IVP Options

You can set some of the IVP options by changing the values in the //IVPSYSIN DD statement coded in either the PRMIVDLI or PRMIVBMP job. Change the following IVP options to suit your testing requirements:

SETRC=rc

Specifies the return code (*rc*) that the IVP job uses. You can specify this keyword to test CA Mainframe Program Restart Manager processing options such as RCABEND= and RCERROR=.

GBCNT=n

Specifies how many times (*n*) the IVP reads through the DI21PART database.

Example: Specify **0** or **1** to run the program until it gets the first GB status code indicating that the end of the DI21PART database has been reached. Specify a higher number to force the IVP to read the database multiple times.

ABENDCNT=*n*

Specifies the number of checkpoints (*n*) that the IVP takes before it abends with a U3619 abend code. This option only affects IVP executions that are not restarted. If the job is restarted, the abend does not occur.

Example. Specify **0** for no abend to occur.

REPL=Y|N

Specifies whether the IVP performs DLI REPL operations on segments read from the DI21PART database.

Y

Specifies that the IVP replaces segments. This is the default.

N

Specifies that the IVP does not replace segments. Specify REPL=N to avoid the need to backout uncommitted updates to the DI21PART database.

Test Processing Options

You can test the CA Mainframe Program Restart Manager processing options while running the IVP jobs. To do this, add a //PRMCTRL DD * to the IVP jobs and specify CA Mainframe Program Restart Manager processing options and values that are to be active for that job execution only. This lets you test the impact of various processing options before you implement them in your environment.

Note: For more information about which processing options to specify, see the *CA Mainframe Program Restart Manager User Guide*. It describes all the options and tells you which options are required for specific CA Mainframe Program Restart Manager features.

Make CA Mainframe Program Restart Manager Libraries Available

The following libraries must be in the STEPLIB concatenation of the IMS batch jobs where CA Mainframe Program Restart Manager is to be used:

- PRMLOAD library (*hlq.CIMTLOAD*)
- PRMUSRL library
- PRMRESL library

In the STEPLIB DD statement, specify the PRMLOAD library in front of the PRMRESL, and the PRMRESL library in front of the DFSRESL library. Include the PRMRESL library in the DFSRESLB DD statement in front of the DFSRESL library.

If standards for your environment include a program product library that every IMS batch job uses, you can copy these libraries to the program product library, or you can copy these libraries to the live IMS RESLIB data set.

After you copy these libraries, CA Mainframe Program Restart Manager processes every IMS batch job except for those jobs with a //PRM\$EXCL DD statement or jobs excluded from CA Mainframe Program Restart Manager processing.

Note: For more information about how to exclude jobs from processing, see the *CA Mainframe Program Restart Manager User Guide*.

Important! If the PRM#INCL module (created by submitting the PRMAOPTS sample library member) is not available to an IMS batch job, CA Mainframe Program Restart Manager bypasses all processing for that job without issuing any error messages. If you fail to copy the PRMUSRL library to a library available to all IMS batch jobs, no CA Mainframe Program Restart Manager processing occurs.

More information:

Allocate Libraries
Allocate and Initialize the Options Data Set

CA Compress Data Compression for IMS Customization

You can perform the following customization of CA Compress Data Compression for IMS after installation:

- [Configure the interactive dialog](#) (see page 118).
- [Enable compression support for a non-IMS environment](#) (see page 125).
- (Optional) [Set the active file descriptor table \(FDT\) parameter](#) (see page 125)

Note: The Compress/2 subroutines and utilities are not integrated into the CA Database Management Solutions for IMS for z/OS. To use these subroutines and utilities, install CA Compress Data Compression Release 5.5. For more information about installing CA Compress Data Compression, see the *CA Compress Data Compression User Guide*.

How to Configure the Interactive Dialogs

Complete the following steps to configure the interactive dialogs:

1. [Allocate the PDS libraries](#) (see page 119) (GENLIB and FDTLIB).
2. [Initialize the interactive dialog control file](#) (see page 120) and define a primary TSO user.
3. [Modify selected ISPF members](#) (see page 121).
4. [Set up the ISPF interface](#) (see page 66).
5. [Activate the Interactive Dialog](#) (see page 122).
6. [Authorize users for the interactive dialog](#) (see page 124).

Note the following additional considerations:

- If you also have CA Compress Data Compression for IMS for z/OS installed, you must have separate dialog control files and ISPF libraries for the dialog component to maintain independent release levels for each product.
- The control word ENQ has been changed to RESERVE throughout the interactive dialog JCL procedures. This change prevents multiple CPU updates from causing problems with the interactive dialog control file.
- Users in installations that use a global shared resource control product (like, MSX and GRS), must make the following modifications to these products:
 - Add the SHRINKFE QNAME.
 - Add the RNAME of the data set name that was chosen for the interactive dialog control file.

If these changes are not made, you might have reserve contention problems (“deadly embrace”).

Allocate GENLIB and FDTLIB Libraries

The first step in configuring the interactive dialogs is to create the required libraries for GENLIB and FDTLIB:

- GENLIB is a PDS library with a RECFM of FB and a LRECL of 80. The BLKSIZE is determined by the installer. This data set contains all generated JCL and access method control blocks (DBDs, clusters, and so on) generated by the interactive dialog.
- FDTLIB is a normal PDS library whose DCM information should conform to the standards in your environment.

These libraries are allocated by running the SHRINS02 member of the JCL library after modifying the data set names to conform to the requirements at your site.

Follow these steps:

1. Edit SHRINS02 in *high-level.CIMTSAMP* as described in the member and save your changes.

SHRINS02 is updated.

2. Submit SHRINS02 for execution.

The GENLIB and FDTLIB libraries are allocated.

Allocate and Initialize the Interactive Dialog Control File

You must allocate and initialize the interactive dialog control file after you allocate the required libraries for the interactive dialogs.

Follow these steps:

1. Modify SHRINS03 in *high-level.CIMTSAMP* as follows and save your changes:
 - a. Update the ALLOC step to modify the IDCAMS control statements in the SYSIN data set to specify the correct data set names at your site.
 - b. Update the INIT step to modify the input control statements.SHRINS03 is updated.
2. Submit SHRINS03 for execution.
The interactive dialog control file is allocated and initialized.

Example: Input Control Statements

The format of the first input control statement follows:

C

Indicates that this is company data (a constant).

y (controlled) or n (open to general use)

Defines the access to various interface support services.

O

Reserved.

deftdasd

Specifies the default DASD device type.

name

Specifies the name of the installation site. the company name.

Limits: 50 characters (including spaces).

The format of the second input control statement follows:

A

Indicates a constant for the authority code.

tsoid

Specifies the TSO logon ID of the primary authorized user to install and implement the interactive dialog.

lastname,firstname mi

Specifies the name of the primary authorized user. Include the comma to separate the last name from the first name.

Limits: 25 characters

username

Specifies the authorized user. This is the name the interactive dialog addresses during processing and can represent user name or user code developed at your site.

Limits: 15 characters

Modify Selected ISPF Members

Before you can logon to the interactive dialog, modify the ISPPLIB, ISPFSLIB, and CIMTPARM libraries to conform to the standard naming conventions of your site.

Follow these steps:

1. Modify member SFEP\$UUI in the ISPPLIB library. This panel must be modified to contain the name or position title, or both, of the person that has been assigned the responsibility of identifying authorized users of the product.
2. Modify the ISPSLIB as follows:
 - a. Supply the correct data set name for the SORTLIB DD statement in the SFESSORT skeleton. If the SORTLIB data set is part of the installation LINKLST, delete the SORTLIB DD statement.
 - b. (Optional) Update the SFEEXSCD skeleton member if your processing environment uses a sort facility other than DFSORT. The SFEEXSCD member contains the SORT control statements necessary for the SORT JCL in SFESSORT.
 - c. Update skeleton SFEVSAMP to conform to your VSAM buffer pool requirements. SFEVSAMP is used within data sample extract JCL generated for an IMS database using the batch DL/I batch method.
3. Modify member SHRISPF in the CIMTPARM library as follows:
 - Change the CONTROL variable to reflect the actual data set name of the Interactive Dialog control file.
 - Change the FDTLIB variable to reflect the actual data set name of the FDTLIB you allocated.
 - Change the GENLIB variable to reflect the actual data set name of the GENLIB you allocated.
 - Change the SYSOUT variable to specify the default SYSOUT class used by the interactive dialog.

Activate the Interactive Dialog

After set up the ISPF application for CA Compress Data Compression for IMS, activate the Interactive Dialog.

Important! The primary authorized user, established earlier by the execution of the [SHRINS03 job](#) (see page 120), must activate the system.

Follow these steps:

1. Open the CA Database Management Solutions for IMS for z/OS main menu and select CA Compress Data Compression for IMS.

The Primary Services Menu appears.

2. Select Option 9 to perform control maintenance.

The Control Maintenance Menu appears.

3. Select Option 1.

The Maintain Installation Control Parameters panel appears.

4. Verify and modify the following fields:

INSTALLATION NAME

Specifies the name used on all interactive dialog reports and in various dialog panels.

SECURED CA-COMPRESS SERVICES

Indicates whether services are to be protected from unauthorized use.

CA-COMPRESS LEVEL

Indicates whether you have installed the full (F) or the Express (E) product.

DEFAULT DASD UNIT

Specifies the default DASD unit. You can change the value in this field when the control file is initialized. You can also modify it on the panel. The value should be the unit specification used for any DASD device when work files are allocated or JCL is generated.

Default: SYSDA

DEFAULT TAPE UNIT

Specifies the normal tape unit is TAPE. You can change the default value on this panel.

CURRENT DFP LEVEL

Specifies the current DFP level. This field has no initial default value. It must be specified during the dialog initialization process, and must be changed whenever the installation upgrades its DFP level. This value must be current because it affects the space and cost calculations performed by the test compression program.

CURRENCY UNIT

Specifies the currency type that you want to appear in your costing reports (For example, dollars, pounds). Enter the name of the currency unit, not the symbol.

DASD PURCHASE COST

Specifies the amount that you spend to acquire new DASD devices, calculated for 1 MB. Enter the amount to the hundredth of the currency unit.

DASD CHARGE/MO

Specifies the amount that your company charges its users for the use of 1 MB of DASD space for one month. Specify the amount in hundredths of the currency unit.

PRIME BATCH CPU CHARGE

Specifies the amount that your company charges for one hour of CPU time to run batch jobs during prime time.

PRIME ON-LINE CPU CHARGE

Specifies the amount that your company charges for one hour of CPU time to run online applications during prime time hours.

PRIME TIME EXCP CHARGE

Specifies the amount that your company charges for one thousand EXCPs during prime time.

NIGHT BATCH CPU CHARGE

Specifies the amount that your company charges for one hour of CPU time to run batch jobs during non-prime time hours.

NIGHT ON-LINE CPU CHARGE

Specifies the amount that your company charges for one hour of CPU time to run online applications during non-prime time hours.

NIGHT TIME EXCP CHARGE

Specifies the amount that your company charges for one thousand EXCPs during non-prime time hours.

PROCESSOR SPEED

Specifies the speed of one of the processors in your CPU. The processor speed is entered in millions of instructions per second (MIPs). For example, if you have a 32 MIP CPU and the CPU has two processors, you calculate 32 MIP divided by 2 processors; the processor speed would be 16. If you have a 32 MIP CPU and the CPU has 4 processors, you calculate 32 MIP divided by 4 processors; the processor speed would be 8.

Press Enter.

The installation control parameters are updated.

5. Select Option 2.

The User Maintenance Menu appears.

6. Select Option C, enter your own TSO ID, and press Enter.

The User Data Maintenance panel appears.

7. Indicate which Interactive Dialog Services you are using by placing **Y** in the appropriate fields and pressing Enter.

The User Maintenance Menu reappears.

8. Exit the User Maintenance Menu to return to the Control Maintenance Menu.

9. Select Option 3.

The Maintain Default Data Set Name panel appears.

10. Complete both sections of the panel.

The interactive dialog is ready for use by authorized users.

Authorize a User for the Interactive Dialog

Each user of the interactive dialog must be identified as an authorized user to the system. You can also update the user data and delete authorized users in the control file.

Follow these steps:

1. Go to the Primary Services Menu and select Option 9 (Maintain CA-Compress Interactive Dialog Control Data).

The Control Maintenance Menu appears.

2. Select Option 2.

Note: Select Option L to select from a list of authorized users. Press the END key to print.

The User Maintenance Menu appears.

3. Enter the new user's TSO ID, **A** for the type of maintenance desired, and press Enter.

The User Data Maintenance panel appears.

Note: Select Option C first to update an existing user or D to delete an authorized user from the control file.

4. Complete the following fields:
 - Enter the name of the new user (last, first, middle initial) in the FULL NAME field.
 - Enter the name by which the user prefers to be called in the MESSAGE NAME field.
 - Enter **Y** after each basic service the user is to be authorized to use.

When the maintenance is complete, press Enter to save the changes.

Enable Compression Support for the Non-IMS Environment

You can enable CA Compress Data Compression for IMS compression when executing a utility where a valid IMS environment does not exist. This support is provided by a unique load library (IMSUT.LOAD) that contains the special version of the IMSHRINK program.

To install the IMSUT.LOAD library, execute the JCL that is provided in the *hlq.CIMTSAMP(SHRINS04)* member.

Specify the IMSUT.LOAD library first in the STEPLIB concatenation in any unload or reload utility jobs for databases that also use CA Compress Data Compression for IMS.

Set the Active File Descriptor Table Parameter

Each segment type to be compressed has an associated file descriptor table (FDT), which can be shared between segment types. However, if the number of shared FDTs in use during the period in which the system is up exceeds 350 (the default maximum), IMS terminates with a user abend and message. To prevent this error, increase the default SHRINKCB CSECT. You can set the active file descriptor table parameter during the initial configuration or at any time.

Follow these steps:

1. Modify the SHRMAXN member in *hlq.CIMTSAMP* to increase the maximum number of different FDTs from 350.

SHRMAXN is updated.

2. Assemble and linkedit the SHRINKCB load module using the SHRINS01 JCL in *hlq.CIMTSAMP*. Set the SRC, ASML, CBLIB, and SDFSMLIB libraries to match your environment and execute the JCL.

The maximum number of different FDTs is updated.

Command Control Manager Customization

To configure Command Control Manager (CCM), follow these steps:

1. Consider your environment, and decide how to configure CCM. The [command routing techniques](#) (see page 126) you choose determine the steps you must perform to configure CCM.
2. Perform the configuration steps:
 - [Make required IMS changes](#) (see page 128)
 - [Update IMS Sysgen](#) (see page 129)
 - [Define APPC/MVS TP Profiles](#) (see page 133) if using APPC/MVS command routing technique
 - [Allocate the CCM Options data set](#) (see page 134)
 - [Create dynamic allocation for the CCM Options data set](#) (see page 134)
 - (Optional) [Activate the CCM Store/Forward feature](#) (see page 134)
 - (Optional) [Activate the CCM IMS Message Log feature](#) (see page 135)
 - [Security considerations](#) (see page 135)
 - (Optional) [Define a DDname Table](#) (see page 136)
3. Define CCM Options in the CCMOPT data set.

Note: For information about how to define CCM options, see the *Command Control Manager User Guide*.

Command Routing Techniques Considerations

Command Control Manager provides the following routing techniques to pass commands to different IMS systems for execution:

IMS Operations Manager (OM)

If you currently use the IMS Operations Manager, CCM can take advantage of your environment to connect to IMS and issue the required IMS commands.

Note: This is the only command routing technique that supports IMS type 2 commands.

APPC/IMS

APPC/IMS connects directly from the requesting user or job to IMS, possibly from a different MVS system, to issue the required IMS commands.

APPC/MVS

APPC/MVS starts CCM executing on the same MVS system where the target IMS system runs. CCM running in the APPC initiator then connects to IMS as a BMP, and is able to issue IMS ICMD/RCMD DLI calls.

You can use different routing methods for different IMS systems. For example, you can choose APPC/IMS for DB/DC systems, and OM for DBCTL systems. However, remember that OM command routing technique must not be in the same CCM group as any other command routing technique.

We recommend that you choose command routing techniques as follows:

- If you already have OM in place for your IMS systems, and you need to issue commands only within a sysplex, use the OM command routing technique.
- If you currently use APPC/IMS, use the APPC/IMS routing technique. If you have both DB/DC and DBCTL systems, use APPC/IMS for the DB/DC systems, and APPC/MVS for the DBCTL systems.
- If you currently use neither, it may be easier to implement OM, unless you already have experience with APPC. If you have some APPC experience, implementing APPC/MVS requires no IMS changes, and may be easier to implement.

Operations Manager

Using OM to issue IMS commands requires that the following conditions are met:

- All the appropriate definitions are in place in all your IMS systems for the IMS SCI and OM.
- The IMS SCI- and OM-started tasks are active on all the appropriate MVS systems in your environment.

Note: You should have the SCI started task on every MVS system in your sysplex where a TSO user or CCM batch job might execute, not just the MVS systems where IMS executes.

- If one IMS in a CCM group uses the OM command routing technique, then all IMS systems in that CCM group must use the OM command routing technique.
- All IMS systems in a CCM group that use the OM command routing technique must be members of the same IMS plex (and therefore must all use the same IMSplex name).

Cross system support using OM is limited to a single sysplex. To access IMS systems across different sysplexes use a VTAM-based command routing technique (APPC/MVS or APPC/IMS).

APPC/IMS

Using APPC/IMS command routing technique requires that the following conditions are fulfilled:

- APPC/IMS is defined (APPC=Y in DFSPBxxx) and active (successful /START APPC) in the target IMS system.
- Based on your environment, there may be APPC/MVS definitions that need to be defined to use this interface.

APPC/IMS does not support the /LOCK, /UNLOCK, and /EXIT commands. To use these IMS commands, use a different command routing technique.

Note: This command routing technique cannot be used by CCM for a DBCTL system, because APPC/IMS is not available in a DBCTL environment.

APPC/MVS

The ICMD/RCMD DLI Call interface does not support the IMS /MODIFY command. CCM routes these commands to IMS via the MVS system console using the MGCRE service. This requires that IMS be enabled for CMDMCS commands by specifying CMDMCS=Y in the DFSPBxxx member of the IMS PROCLIB.

When using the ICMD/RCMD DLI Call interface, IMS does not return the DFS0488I database status messages that are returned using the APPC/IMS or IMS OM command routing techniques. CCM instead simulates the database status message (which follow commands that change database status such as /START DB or /DBR DB) by issuing a CCM0488I message.

When command routing technique APPC/MVS is requested, but a command request is originated from an IMS BMP connected to the target IMS system, CCM bypasses using APPC/MVS and issues the commands directly using the existing IMS BMP connection.

Note: An IMS system with APPC/IMS enabled (APPC=Y in DFSPBxxx) cannot use the APPC/MVS command routing technique.

Make Required IMS Changes

Modify the following:

- Add a program definition to the IMS sysgen to support CCM. This step is required only if you use the APPC/MVS routing technique OR if you use the Command Store and Forward feature of CCM. You can use member CCMSTG1 of the CIMTSAMP data set as an example of the definition that must be added to the IMS sysgen.
- Edit the IMS PROCLIB member DFSPBxxx as follows:
 - Specify the following to enable the IMS ICMD/RCMD DLI call interface:
`A0IS= A | C | R | S`
Note: You can specify any value but N.
 - Specify the following in the DFSPBxxx member for PROCLIB data set of each IMS system to enable IMS for MCS console commands:
`CMDMCS=Y`
Note: CCM uses the MVS EMCS console to issue commands that ICMD calls do not support.

- (APPC/MVS) Verify that APPC=N is specified. Verify that APPC/IMS is not automatically started by using the /DISPLAT ACT DC command, and check that APPC STATUS shows DISABLED. If it shows as ENABLED, consider using APPC/IMS instead, or remove any automated /START APPC commands that caused APPC/IMS to become enabled.
- (APPC/IMS) Verify that APPC=Y is specified. Verify that APPC/IMS is automatically started by using the /DISPLAT ACT DC command, and check that APPC STATUS shows ENABLED. If APPC STATUS shows as DISABLED, consider using APPC/MVS instead of APPC/IMS, or automate the startup of APPC/IMS by making a /START APPC command be issued each time IMS is restarted.

Update IMS Sysgen

If you plan to use either APPC/MVS as the command routing technique or if you want to activate the CCM command store/forward feature, you will need to define BMP programs in the IMS sysgen. The samplib data set (CIMTSAMP) has an example of the required definitions in ember name CCMSTG1. Add these definitions to the IMS sysgen source, perform an IMS sysgen, and implement the new sysgen.

How to Specify APPC/MVS Definitions

When using the APPC/MVS command routing technique and the Remote STC process for issuing IMS commands, you must define the following information to APPC/MVS and specify in the CCM Global options and IMS System Information.

Note: No definitions are required if you use only the APPC/IMS or IMS OM Routing Techniques.

The APPC/MVS definitions required for APPC/MVS Routing Technique and the Remote STC process include the following.

APPC/STC TPname

(global)

Specifies the transaction program name (TP name) defined to APPC/MVS that is used for the APPC/MVS command routing technique.

Limits: An APPC TP name must be defined for each IMS system for CCM to use. The TP names defined must all begin with the same 1- to 59-character prefix, followed by a period (.) and the IMSID. The prefix of the TP names must be specified in the CCM global options.

SYMDEST

Specifies the Partner LU (PLU) name and logmode table entry name (MODE) for a TP Name:

PLU

Specifies the APPC/MVS base LU on the MVS LPAR where an IMS system executes. This LU should already be defined.

MODE

Specifies a logmode entry that supports APPC, and should already be defined to VTAM. Your VTAM system programmer should be able to provide you with a mode table entry name that supports APPC communication.

Learn Your Current APPC/MVS Environment

To define the required entries to APPC/MVS and CCM, determine the following:

- APPC TP Profile data set name
- APPC Side Info data set name
- APPC/MVS base LU name
- APPC initiator name for each MVS LPAR where an IMS system executes

Follow these steps:

1. Issue MVS command D APPC,LU,ALL.
2. Find the LLUN (LU name) that has both SCHD=ASCH and BASE=YES on each MVS system where an IMS system runs.
3. Note the following:
 - LLUN and the TPDATA= data set name for each MVS system. The APPC/MVS base LU name and the TP Profile data set name are required to define the APPC/STC TPname in the CCM Global options.
 - The name of the APPC/MVS side info data set, which can be found in the line showing SIDEINFO= at the beginning of the display command output. This data set name is required to define APPC/MVS symbolic destinations.
4. Issue MVS command D ASCH,ALL.

The list of the APPC initiator classes defined on each MVS system appears. The initiator class must be able to concurrently schedule at least 1 more than the number of IMS subsystems on that MVS system. If an MVS system has three IMS subsystems executing, the APPC initiator class must be able to schedule at least four tasks concurrently (the MAX= value for the class must be at least 4).

Note: The name of the initiator class is required to define the APPC/MVS transaction program profile for CCM.

Define APPC/MVS Symbolic Destinations

The APPC/MVS Symbolic Destinations define the LU name and mode name that direct APPC sessions to the proper MVS LPAR for each IMS system. Defining the APPC/MVS symbolic destinations for each MVS LPAR where an IMS system may execute helps facilitate CCM customization. The APPC symbolic definitions do not require any product-specific information and may already be in place. If such definitions do not already exist, they can be defined using the APPC configuration utility.

Note: After you have defined the SYMDEST entries, use these names in the CCM IMS System Information in the SYMDEST field. Because you have defined these SYMDEST entries, you do not need to specify the PLU or MODE fields in the CCM IMS System Information.

Follow these steps:

1. Edit the CCMSIADD member in the samplib (CIMTSAMP) with the values from your system:

##SIDEINFO

If all MVS LPARs share the same Side Info data set, you can define each symbolic destination once. Otherwise, you specify the symbolic destinations in each Side Info data set found in the D APPC,LU,ALL command output.

##SYMDEST

Specifies the name of an MVS LPAR.

##MODE

Specifies a VTAM mode table entry name that supports APPC.

##LUNAME

Specifies the name of the APPC/MVS Base LU found in the D APPC,LU,ALL command output for the MVS LPAR.

2. Execute the job.

If you have three MVS LPARs, run the CCMSIADD job three times, once for each LPAR (changing the ##SYMDEST and ##LUNAME for each LPAR). If there are three different Side Info data sets, run the job nine times, three times for each Side Info data set name.

Example: Define Side Info

When you have three MVS LPARs (SYS1, SYS2, and SYS3) with IMS system executing on each LPAR, define three APPC/MVS Symbolic Destinations. You can create APPC/MVS symbolic destination names that match the MVS LPAR names (SYS1, SYS2, and SYS3).

Define APPC/MVS TP Profiles

The TP profile tells APPC/MVS how to start up the remote STC used to connect to IMS as a BMP to issue IMS commands. An APPC/MVS TP profile entry must be defined for each IMS system that CCM uses. Use the APPC configuration utility to define the TP profiles.

Define the TP profile for an IMS system only on the MVS LPAR where that IMS system executes. If there are different APPC/MVS TP Profile data sets on each LPAR, you need to define the IMS TP Profile name only once.

Follow these steps:

1. Edit the CCMTADD member in the samplib (CIMTSAMP) as follows:

##TPPROF

Specifies the TP Profile data set name found in the D APPC,LU,ALL command on the MVS LPAR where this IMS system executes.

##TPNAME

Specifies the name of the TP Profile. This name must be the APPC/STC TPname specified in the CCM Global options, with the ".imsid" added to the end of the name.

##MSGDSN

Specifies the data set name to be created that holds MVS SYSLOG messages for an execution of the CCM remote STC process. This data set is allocated as part of the CCMTADD job. Because you must run this job for each IMSID, include the IMSID as part of the MSGDSN data set name.

##SYSUDUMP

Specifies the data set name to be created that holds SYSUDUMP output in the event that an abend occurs in the CCM remote STC process. This data set is allocated as part of the CCMTADD job.

##VOLUME

Specifies the volume serial number of the DASD volume where the ##MSGDSN and ##SYSUDUMP data sets will be allocated.

##CLASS

Specifies the APPC/MVS initiator class found in the D ASCH,ALL command for the MVS LPAR where this IMS system executes.

##PSB

Specifies the name of the PSB that was added to the IMS stage 1 sysgen source. A sample is provided in CIMTSAMP member CCMSTG1.

##SDFSRESL

Specifies the data set name of the SDFSRESL data set for this IMS system.

##CCMLOAD

Specifies the data set name of the CCM load library (CIMTLOAD data set).

##IMSID

Specifies the IMSID specified in the ##TPNAME variable above.

2. Execute the job once for each IMS system that you define the TP profile for.

Allocate the Options Data Set

To allocate the CCM options data set, edit the sample job in the hlq.CIMTSAMP(CCMODINI) samplib member to specify required data set names, volsers, and space values, and execute the job.

Create Dynamic Allocation for the Options Data Set

To create dynamic allocation for the CCM Options data set, edit the sample job in the CCMASMOP samplib member as follows and execute:

- Customize the CCMOPTS data set name.
- Customize the loadlib data set name.

The member CCM#OPTS is created in the load library (CIMTLOAD).

Activate the CCM Store/Forward Feature

Follow these steps:

1. Edit the sample job in the CCMSFT samplib member to specify the required data set names, volser, and space values, and execute the job.

The CCM Store/Forward data set (CCMSTFWD) is allocated and initialized.

2. Edit the sample job in the CCMASMSF samplib member as follows to create a dynamic allocation member for CCMSFTWD and execute the job:

- Customize the CCMSTFWD data set name.
- Customize the CA Database Management Solutions for IMS for z/OS loadlib data set name.

The dynamic allocation member for CCMSFTWD is created in the CA Database Management Solutions for IMS for z/OS load library (CIMTLOAD).

3. Edit the sample job in the CCMBMPR samplib member to set up the CCM REDO BMPs JCL as follows:
 - Specify correct data set names, IMSID, and PSB name.

Note: DD statements CCMPRE and CCMPOST define IMS commands that are to be issued before (CCMPRE) and after (CCMPOST) any commands that are pending execution based on the contents of the Store/Forward data set contents.
4. Schedule the REDO BMP to execute immediately after every IMS restart completes, and before the system is opened up for processing. You can use automation or a facility like IMS Time Controlled Operations (TCO) to start up the BMP job.

Activate the CCM IMS Message Log

The CCM IMS Message Log lets you browse IMS master terminal (MTO) messages, IMS commands, and command responses from any IMS user. You can define the message log using z/OS System Logger log stream either with a single-system DASD log stream or using the Coupling Facility in a sysplex environment.

To define the CCM IMS Message Log, do *one* of the following:

- To create a DASD-only log stream that is not shared across IMS systems, customize and run the CCMLOGR1 sample job in the CA Database Management Solutions for IMS for z/OS sample library.
- To define the log stream for a sysplex environment, customize and run the CCMLOGR2 sample job in the <productgroup> sample library.

The job executes the IBM Utility, IXCMIAPU, to define the necessary structures and the log stream to the Coupling Facility.

Security Considerations

The following are recommended security settings for CCM:

Security verification for APPC/IMS and APPC/MVS

When CCM issues IMS commands, it passes the requesting user ID to IMS to verify that the user is authorized to issue that specific command. To enable this compatibility when using APPC/IMS or APPC/MVS, specify SECACPT=ALREADYV or AVPV on the VTAM LU definition (in VTAMLST). This tells APPC that it should trust that the partner in the conversation has a userid that is already verified.

Access levels for the CCM Options data set

Specify UACC of READ for the CCMOPTS data set, because all users of CCM will require read access to this data set. Administrators of CCM options should have CONTROL access to this VSAM data set, allowing them to use the ISPF application to change options stored in the CCMOPTS data set.

The following table lists profiles that are available for specifying user access to particular types of resources. To let user or group access a particular type of resources, specify READ access to the profile for the user or group.

Class	Profile	Option Type Protected	ISPF Option
FACILITY	CCM.OPTGBL	Global	1
FACILITY	CCM.OPTJOB	Job	2
FACILITY	CCM.OPTIMS	IMS	3
FACILITY	CCM.OPTGRP	Group	4
FACILITY	CCM.OPTSFV	View the Store/Forward DS	5
FACILITY	CCM.OPTSFE	Update the Store/Forward DS	5
FACILITY	CCM.OPTMSG	Message Disposition	6
FACILITY	CCM.OPTCMD	Command	C

Access to Store/Forward feature

If you activate the Store/Forward feature of CCM, grant CONTROL access to any users that could enter commands while a target IMS system is not available. The user ID that enters a command that must be stored for later use (TSO user or batch job) will require CONTROL access to the VSAM CCMSTFWD data set. The REDO BMP will also require CONTROL access to the CCMSTFWD data set to issue commands at IMS restart, and to remove the commands from the Store/Forward data set.

Access to Message Log

If you activate the CCM IMS Message Log, the security class LOGSTRM is used to protect log streams. Verify with your security administrator that appropriate security is in place for the log stream.

The MVS system logger and SMS will require ALTER access to any data sets you define for a DASD log stream.

Define a DDname Table

DDname table defines multiple sets of input and output ddnames that CCM uses. Using the DDname table lets you replace multiple user-written command processors without any changes to the batch job JCL.

In CCM Global options, you specify the ddnames for reading IMS commands for CCM to issue and to write output messages. To replace multiple user-written IMS command processors, specify multiple sets of input and output ddnames in the DDname table. CCM searches a batch job JCL until it finds a ddname in the table for input, and another ddname for output, and applies the first ddname it finds in the job JCL.

To define a DDname table, customize the *hlq.CIMTSAMP(CCMDDTBL)* member as described in the member and execute:

- Specify the input (TYPE=INPUT) and output (TYPE=OUTPUT) ddnames you want CCM to search for when executing a batch CCM job in CCMDD macros. You can add or remove these statements as needed.
- Verify that the last two statements in the SYSIN DD are CCMDD BUILD=YES and END.

The job creates the CCMDDTBL load module in your CCM load library. The module activates the CCM DDname table feature.

Customize the IMS Operations Manager

You can configure the IMS Operation Manager to send the messages to the CCM Combined Mesage Log.

Follow these steps:

1. Add the CCMLOAD data set to the IMS Operations Manager STEPLIB concatenation.
2. Add member CCMPARMS to the //PROCLIB data set for IMS Operations Manager and specify the name of the z/OS Combined Message logstream:

```
CCMPARMS
***** Top of Data ***
*
CCMLOGR=@CCM.LOGGER
***** Bottom of Data *
```

3. Add the following statement to the BPECONFIG Proclib member used by the IMS Operations Manager:

```
EXITMBR=(member, OM)
```

4. Add the following statement to the exit routine Proclib member:

```
EXITDEF (TYPE=INITTERM,EXITS=(CCMOINIO),ABLIM=0,COMP=OM)
```

```
EXITDEF (TYPE=OUTPUT,EXITS=(CCMOPSS0),ABLIM=0,COMP=OM)
```

Customize the Batch Processor

CCM Batch Processor replaces user-developed IMS AOI programs with no or minimal changes to JCL. The processor can run as an IMS BMP, DLI batch, or standard MVS batch job. The CCM sample library data set (CIMTSAMP) contains sample JCL for each type of job (CCMBMP,CCMDLI,CCMBATCH).

- When run as an IMS BMP, any PSB name can be used. CIMTSAMP(CCMSTG1) contains sample APPLCTN statements if you want to add new ones for CCM.
- When run as an IMS DLI batch job, the PSB you use must contain the CMPAT=YES parameter. CIMTSAMP(CCMPSTB) contains a sample PSB for IMS DLI batch.

- When run as an MVS batch job, there are no IMS considerations. (You may need SDFSRESL in the steplib concatenation if you are doing certain IMS database commands).
- In the CCM Global record, you can specify the ddnames of the input and output files used by CCM batch. These ddnames should be the names you use in your IMS AOI program. If you are using CCM to replace multiple IMS AOI programs, and you use different ddnames, there is a process where you can specify more than 1 set. CIMTSAMP(CCMDD/CCMDDTBL) contain more information about multiple ddname specification.

CCM provides a stub program that does a dynamic call to the CCM batch processor. This stub can be assembled/linked with any name. The stub is intended to replace your IMS AOI.

Once the ddname specification has taken place, and dynamic allocation and stub modules have been installed, you should be able to copy CIMTLOAD to a steplib data set in the old IMS AOI JCL.

Preparing to Start CA Database Management Solutions for IMS for z/OS

Verify the Installation

You can use the IVPIMS01job in the *hlq.CIMTSAMP*(IVPIMS01) member to verify the installation of the CA Database Management Solutions for IMS for z/OS. This job will finish with return code 0 only when you have installed all our products.

To verify the installation, edit IVPIMS01 in *hlq.CIMTSAMP* as described in the member, save your changes, and submit the job.

The job performs the following tasks:

- Assembles and links all DBDs and PSBs, and loads the database. The following libraries are created:
 - *hlq.IVP.DBDLIB* (all DBDs are placed here)
 - *hlq.IVP.PSBLIB* (all PSBs are placed here)
- Creates a secondary index with CA Secondary Index Builder, and runs CA Database Analyzer for IMS.
- Unloads and image copies the database. The unload file is used in a reload step, and the image copy is used in a database recovery.
- Deletes all data sets at the end of the job. All tasks should end with RC=0.

ITK STC Started Task Considerations

The ITK STC started task is used by Snapshot General Services support (FLASH=YES) in CA Database Copier, Full Function and HALDB online reorganization in CA Database Organizer, and Recovery Analyzer in CA High Performance Recovery.

The ITK STC is needed to issue IMS commands and to use BMP pause and resume functionality. It can also be used to enable option MMGRIO=YES (Media Manager) with an unauthorized CA Database Management Solutions for IMS for z/OS products load library.

ITK STC must be running on the same system as the target IMS system and on every LPAR containing a member of the IMSplex in a data sharing environment.

Note the following additional considerations:

- The ITK STC must run from an APF-authorized library.
- Only one ITK STC will execute per LPAR.

A sample ITK STC procedure is provided in the sample library, member STCITK.

STC Control Statements

You need to code the ITK STC (started task) control statements in a parmlib (*hlq.CIMTPARM*) member whose name matches the STC name. For example, if the STC name is FFOR, make the member name FFOR. A sample is provided in the PARMLIB (CIMTPARM) data set. Modify the variables in the sample to match your environment.

When you first execute the ITK STC, it will interactively request values for parameters that have not yet been coded. You respond through the operator console.

- Any values you supply are rewritten into the ITK STC parameter member.
- If you do not supply a value for a specific parameter, you can give a null reply.

The STC control statements are as follows:

- [ALLOC PARMS](#) (see page 140)
- [COMPANY NAME](#) (see page 141)
- [DIV_PFCOUNT](#) (see page 141)
- [DIV_PRIMARY](#) (see page 142)
- [DIV_SECONDARY](#) (see page 142)
- [DSN_PREFIX](#) (see page 143)
- [HPOALOG](#) (see page 144)
- [HPOCLOG](#) (see page 144)

- [MAP_MODULE](#) (see page 144)
- [PAUSE](#) (see page 144)
- [REL_MODULE](#) (see page 145)
- [SMS_DCLASS](#) (see page 145)
- [SMS_MCLASS](#) (see page 146)
- [SMS_SCLASS](#) (see page 146)
- [SMS_TRACE_DCLASS](#) (see page 147)
- [SMS_TRACE_MCLASS](#) (see page 147)
- [SMS_TRACE_SCLASS](#) (see page 148)
- [SYSPRINT](#) (see page 149)
- [TRACE_MAX_KB](#) (see page 149)
- [TRACE_PREFIX](#) (see page 149)
- [TRACE_UNIT](#) (see page 150)
- [TRACE_VOLUME](#) (see page 150)
- [TYPE](#) (see page 150)

More information:

How to Enable Online Reorg Processing in CA Database Organizer.....

ALLOC_PARMS—Create New VSAM Linear Data Sets

Valid for the Online Reorg component of CA Database Organizer.

The ALLOC_PARMS control statement sets other parameters to be used on the IDCAMS command to create new VSAM linear data sets.

This control statement has the following format:

```
ALLOC_PARMS=VOLUME (IDI007)
```

VOLUME (IDI007)

Indicates the parameter that will be passed as the volume list to IDCAMS. Any operand of this control statement is passed to IDCAMS when defining the ITK STC linear data sets.

COMPANY_NAME—Specify Company Name

Valid for the Online Reorg component of CA Database Organizer.

The COMPANY_NAME control statement specifies your company name. This information is used only in the creation of the repository trace files that online reorg creates when specific errors occur.

These files can be requested by Technical Support to help with problem diagnosis.

This control statement has the following format:

COMPANY_NAME=*companyname*

companyname

Defines the company name.

DIV_PFCOUNT—Determine FFOR Data Space Pages

Valid for the Online Reorg component of CA Database Organizer.

The DIV_PFCOUNT control statement determines the number of virtual data space pages to be paged when a page fault occurs. Online reorg stores data sequentially in its data spaces, and therefore, is helped if more than one virtual page is paged in when a page fault occurs.

Note: Paging in more than one page at a time does not increase the real-storage use for online reorg. Strike a balance between FFOR performance and real-storage that optimizes FFOR performance while not monopolizing real-storage.

This control statement has the following format:

DIV_PFCOUNT=*nnnnnnnn*

nnnnnnnn

Indicates 8-digit decimal number left-padded with zeros that represents the size in kilobytes (KB). The padding zeros are optional if the value is entered as an answer to a console message.

Limits: 00000008-00000255. We recommend that you initially set this value to 00000008.

DIV_PRIMARY—Set Primary VSAM Linear File FFOR Default Value

Valid for the Online Reorg component of CA Database Organizer.

The DIV_PRIMARY control statement sets the default value for the size (in kilobytes) of the primary VSAM linear file allocated by online reorg to back its data-in-virtual data space.

Note: The data-in-virtual data spaces house IMS database updates made to your online databases while online reorg runs. By using VSAM linear files to back the FFOR data spaces, online reorg protects your z/OS page data sets and paging subsystem from being impacted by online reorgs.

DIV_PRIMARY determines the size of the first linear data set allocated by online reorg, and consequently determines the size of the first FFOR data space.

- Tune this value as you run online reorg so that FFOR allocates as few data spaces as possible during your reorgs.
- One data space is the optimum number in terms of performance, so setting this value large enough to house all database updates made during a typical reorg is suggested.

Note: In addition to this control statement, which sets the FFOR default, you can set this value on a job-by-job basis by supplying an override value in your FFOR reorg jobs.

This control statement has the following format:

DIV_PRIMARY=nnnnnnnn

nnnnnnnn

Indicates 8-digit decimal number left-padded with zeros that represents the size in kilobytes (KB). The padding zeros are optional if the value is entered as an answer to a console message.

DIV_SECONDARY—Set FFOR Default Value for the Size of Secondary Extents

Valid for the Online Reorg component of CA Database Organizer.

The DIV_SECONDARY control statement sets the default value for the size (in kilobytes) of secondary extents for an FFOR data-in-virtual repository.

The first data space extent size is determined by the DIV_PRIMARY control statement and any subsequent data spaces in a repository are allocated using this parameter to determine the size (in kilobytes) of each additional extent.

Note: In addition to this control statement, which sets the FFOR default, you can set this value on a job-by-job basis by supplying an override value in your FFOR reorg jobs.

This control statement has the following format:

`DIV_SECONDARY=nnnnnnnn`

nnnnnnnn

Indicates 8-digit decimal number left-padded with zeros that represents the size in kilobytes (KB). The padding zeros are optional if the value is entered as an answer to a console message.

DSN_PREFIX—Add Data Set Name Prefix

Valid for the Online Reorg component of CA Database Organizer.

The DSN_PREFIX control statement is used during the online reorganization of a HALDB database when multiple partitions are to be reorganized in a single job step using PARTITION or NUMBEROFPARTS. The value specified is used to build the data set names for DD statements IEFRDER and FINALICx starting with the second partition.

Note: A valid DSN_PREFIX is required with COPYUNLOAD to enable dynamic allocation of the output image copy data sets. DELETEIC indicates whether to register or delete the copy.

This control statement has the following format:

`DSN_PREFIX=prefix`

prefix

Specifies a prefix for the data set name when multiple partitions are reorganized in a single job step.

- For the first partition, the data sets provided in the JCL is used.
- For the second and subsequent partitions, the required data sets are dynamically allocated using the value specified as a prefix for the data set name. The attributes of the dynamically allocated data sets are the same as those of the originally allocated JCL data sets.

Example: Add Data Set Name Prefix

In this example, the data set name is prefixed with CAI:

`PARTITION=MARKHI1,
DSN_PREFIX=HLQ.DSNPREF`

The following data set names will be generated when the previous values are specified.

`HLQ.DSNPREF.MARKHI1.FINALICA
HLQ.DSNPREF.MARKHI1.IEFRDER`

HPOALOG—Identify FFOR SYSOUT Class

Valid for the Online Reorg component of CA Database Organizer.

The HPOALOG control statement identifies the SYSOUT class for the FFOR activity log.

This control statement has the following format:

HPOALOG=A

A

Indicates a valid SYSOUT class.

HPOCLOG—Identify FFOR Command Log SYSOUT Class

Valid for the Online Reorg component of CA Database Organizer.

The HPOCLOG control statement identifies the SYSOUT class for the FFOR command log.

This control statement has the following format:

HPOCLOG=A

A

Indicates a valid SYSOUT class.

MAP_MODULE

Valid for the Online Reorg component of CA Database Organizer.

The MAP_MODULE control statement is used internally during FFOR processing. This control statement is required.

This control statement has the following format:

MAP_MODULE=HPOMAP

PAUSE—Identify the Normal BMP PAUSE Start-up Type

Valid for the Online Reorg component of CA Database Organizer.

The PAUSE control statement identifies the normal BMP PAUSE startup type. We strongly recommend that you set PAUSE to W (warm) and override it if necessary to C (cold).

This control statement has the following format:

PAUSE=W|C

W

Indicates that the normal BMP PAUSE startup type is warm. A warm start recovers all CSA areas and SSI capabilities from previous HPO sessions since the last IPL.

C

Indicates that the normal BMP PAUSE startup type is cold. A cold start builds new CSA areas and establishes a new SSI environment. A forced cold start (using this option) results in online reorg initialization attempting to free any CSA previously acquired by online reorg before initializing new CSA areas (a forced cold start does not recover the SSI areas).

Note: When the ITK STC is cold started (TYPE=C,PAUSE=any), it no longer communicates with PAUSE enabled IMS control regions until they are restarted. Because cold start (TYPE=C) refreshes the ITK STC modules and storage resident in CSA, the STC loses the ability to support PAUSE enabled IMS control regions that were started before the cold start of the ITK STC. These IMS regions must be restarted before an FFOR job can be executed.

REL_MODULE

Valid for the Online Reorg component of CA Database Organizer.

The REL_MODULE control statement is used internally during FFOR processing.

This control statement is required.

This control statement has the following format:

REL_MODULE=HPRELAT

SMS_DCLASS—Define VSAM Linear SMS Data Class

Valid for the STC component of CA Database Organizer.

The SMS_DCLASS control statement sets the default value for the VSAM linear Storage Management Subsystem (SMS) DATACLAS value. The value determines the SMS DATACLAS value to be used on the allocation request.

You must specify SMS_DCLASS, or one of the following: ALLOC_PARMS, SMS_SCLASS, or SMS_MCLASS.

This control statement has the following format:

`SMS_DCLASS=value`

value

Sets the default value for the VSAM linear Storage Management Subsystem (SMS) DATACLAS value.

Limits: It can be blank or 1 to 8 alphanumeric characters and is a valid SMS DATACLAS name, as defined by the system administrator.

Default: If left blank, the data set will be allocated without a DATACLAS specification. The default is SMS_DCLASS=blank.

SMS_MCLASS—Define VSAM Linear SMS Management Class

Valid for the STC component of CA Database Organizer.

The SMS_MCLASS control statement sets the default value for the VSAM linear SMS MGMTCLAS value. The value determines the SMS MGMTCLAS to be used on the allocation request.

You must specify SMS_MCLASS, or one of the following: ALLOC_PARMS, SMS_DCLASS, or SMS_SCLASS.

This control statement has the following format:

`SMS_MCLASS=value`

value

Sets the default value for the VSAM linear SMS MGMTCLAS value.

Limits: It can be blank or 1 to 8 alphanumeric characters and is a valid SMS MGMTCLAS, as defined by the system administrator.

Default: If left blank, the data set will be allocated without a STORCLAS specification. The default is SMS_MCLASS=blank.

SMS_SCLASS—Define VSAM Linear SMS Storage Class

Valid for the STC component of CA Database Organizer.

The SMS_SCLASS control statement sets the default value for the VSAM linear SMS STORCLAS value. The value determines the SMS STORCLAS to be used on the allocation request.

You must specify SMS_SCLASS, or one of the following: ALLOC_PARMS, SMS_DCLASS, or SMS_MCLASS.

This control statement has the following format:

`SMS_SCLASS=`*value*

value

Sets the default value for the VSAM linear SMS STORCLAS value.

Limits: It can be blank or 1 to 8 alphanumeric characters and is a valid SMS STORCLAS name, as defined by the system administrator.

Default: If left blank, the data set will be allocated without a STORCLAS specification. The default is SMS_SCLASS=blank.

SMS_TRACE_DCLASS—Define SMS Trace Default Data Class

Valid for the STC component of CA Database Organizer.

The SMS_TRACE_DCLASS control statement sets the default value for the trace file's SMS DATACLAS value. It determines the SMS DATACLAS value to be used on the allocation request.

You must specify SMS_TRACE_DCLASS, or one of the following to produce a trace file: TRACE_UNIT, TRACE_VOLUME, SMS_TRACE_SCLASS, or SMS_TRACE_MCLASS.

This control statement has the following format:

`SMS_TRACE_DCLASS=`*value*

value

Sets the default value for the trace file's SMS DATACLAS value.

Limits: It can be blank or 1 to 8 alphanumeric characters and is a valid SMS DATACLAS name, as defined by the system administrator.

Default: If left blank, the data set will be allocated without a DATACLAS specification. The default is SMS_TRACE_DCLASS=blank.

SMS_TRACE_MCLASS—Define SMS Trace Default Management Class

Valid for the STC component of CA Database Organizer.

The SMS_TRACE_MCLASS control statement sets the default value for the trace file's SMS MGMTCLAS value. It determines the SMS MGMTCLAS value to be used on the allocation request.

You must specify SMS_TRACE_MCLASS, or one of the following, to produce a trace file: TRACE_UNIT, TRACE_VOLUME, SMS_TRACE_DCLASS, or SMS_TRACE_SCLASS.

This control statement has the following format:

`SMS_TRACE_MCLASS=value`

value

Sets the default value for the trace file's SMS MGMTCLAS value.

Limits: It can be blank or 1 to 8 alphanumeric characters and is a valid SMS MGMTCLAS, as defined by the system administrator.

Default: If left blank, the data set will be allocated without a STORCLAS specification. The default is SMS_TRACE_MCLASS=blank.

SMS_TRACE_SCLASS—Define SMS Trace Default Storage Class

Valid for the STC component of CA Database Organizer.

Sets the default value for the trace file's SMS MGMTCLAS value.

The SMS_TRACE_SCLASS control statement sets the default value for the trace files SMS STORCLAS value. It determines the SMS STORCLAS value to be used on the allocation request.

You must specify SMS_TRACE_SCLASS, or one of the following, to produce a trace file: TRACE_UNIT, TRACE_VOLUME, SMS_TRACE_DCLASS, or SMS_TRACE_MCLASS.

This control statement has the following format:

`SMS_TRACE_SCLASS=value`

value

Sets the default value for the trace file's SMS STORCLAS value.

Limits: It can be blank or 1 to 8 alphanumeric characters and is a valid SMS STORCLAS name, as defined by the system administrator.

Default: If left blank, the data set will be allocated without a STORCLAS specification. The default is SMS_TRACE_SCLASS=blank.

SYSPRINT—Identify the SYSOUT Class for the SYSPRINT DDname

Valid for the STC component of CA Database Organizer.

The SYSPRINT control statement identifies the SYSOUT class for the SYSPRINT ddname (used for IDCAMS output).

This control statement has the following format:

SYSPRINT=*class*

class

Indicates a valid SYSOUT class.

TRACE_MAX_KB—Define Maximum Trace File Size

Valid for the Online Reorg component of CA Database Organizer.

The TRACE_MAX_KB control statement sets the maximum size for each individual trace file created by the FFOR started task. The online reorg does not exceed this size for any given trace file, but can allocate multiple files per trace if this maximum is not large enough to house the needed trace data.

This control statement has the following format:

TRACE_MAX_KB=*nnnnnnnn*

nnnnnnnn

Indicates 8-digit decimal number left-padded with zeros that represents the size of the trace file in kilobytes (KB). The padding zeros are optional if the value is entered as an answer to a console message.

TRACE_PREFIX—Add Trace Data Set Name Prefix

Valid for the Online Reorg component of CA Database Organizer.

The TRACE_PREFIX control statement sets the default value for the trace files data set name prefix used to dynamically allocate the online reorg trace files. The trace files are sequential data sets that CA Database Organizer creates when specific errors occur and can help Technical Support with problem diagnosis.

This control statement has the following format:

TRACE_PREFIX=*tprefix*

tprefix

Specifies a valid data set name prefix.

TRACE_UNIT—Define Trace Unit Name

Valid for the Online Reorg component of CA Database Organizer.

The TRACE_UNIT control statement defines a specific, generic, or esoteric unit name for dynamic allocation requests of an FFOR trace file.

Note: Do not set TRACE_UNIT if you have specified an SMS class value.

This control statement has the following format:

TRACE_UNIT=*unitname*

unitname

Specifies the device unit name. Enter a valid esoteric unit name defined to the operating system.

Limits: 1-8 alphanumeric characters

TRACE_VOLUME—Specify Trace Volume Name

Valid for the Online Reorg component of CA Database Organizer.

The TRACE_VOLUME control statement identifies a specific DASD volume for dynamic allocation requests of an FFOR trace file.

Note: Do not specify TRACE_VOLUME if you have provided an SMS class value.

This control statement has the following format:

TRACE_VOLUME=*tvolname*

tvolname

Indicates 1 to 8 alphanumeric characters of a valid DASD volume name.

TYPE—Identify FFOR Startup Type

Valid for the Online Reorg component of CA Database Organizer.

The TYPE control statement identifies the normal FFOR startup type. We strongly recommend that you set TYPE to W (warm) and override it if necessary to C (cold).

This control statement has the following format:

TYPE=W|C

W

Specifies warm start.

C

Specifies cold start.

Note: When the ITK STC is cold started (TYPE=C,PAUSE=any), it no longer communicates with PAUSE enabled IMS control regions until they are restarted. Because cold start (TYPE=C) refreshes the ITK STC modules and storage resident in CSA, the STC loses the ability to support PAUSE enabled IMS control regions that were started before the cold start of the ITK STC. These IMS regions must be restarted before an FFOR job can be executed.

ITK STC Communication

You can communicate with ITK STC (started tasks) using the following modify (/F) commands:

Note: The STC name must also be used with the modify command. For example: /F *stcname*,KILL.

- DISABLE
- DISPLAY ACTIVE|INTERNAL|LOCK|PAUSE|REP
- DUMP INTERNAL|REP
- ENABLE
- FREE LOCK
- KILL
- REFRESH
- RESUME
- SET TRACE

DISABLE Command—Prevent Start of New FFOR Jobs

The DISABLE command causes the ITK STC to enter a “draining” mode. In draining mode, no new FFOR reorg jobs are allowed to start. However, existing FFOR reorg jobs are allowed to complete normally.

The following syntax is valid:

```
/F DISABLE
```

Use the ENABLE command to resume processing after a DISABLE.

More information:

ENABLE Command—Resume New FFOR Job Processing

DISPLAY ACTIVE Command—List Active and Idle HPO Sessions

The DISPLAY ACTIVE command displays a list of active and idle HPO sessions. An IMS session is idle if it can support DL/I call data capture for an FFOR job, but no FFOR job is currently running.

Note: When the ITK STC is cold started (TYPE=C,PAUSE=any), it no longer communicates with PAUSE enabled IMS control regions until they are restarted. Because cold start (TYPE=C) refreshes the ITK STC modules and storage resident in CSA, the STC loses the ability to support PAUSE enabled IMS control regions that were started before the cold start of the ITK STC. These IMS regions must be restarted before an FFOR job can be executed.

This command has the following syntax:

```
/F DISPLAY ACTIVE  
/F DISPLAY A  
/F DIS ACTIVE  
/F DIS A  
/F D ACTIVE  
/F D A
```

DISPLAY INTERNAL Command—List HPCOM Control Blocks

The DISPLAY INTERNAL command produces a formatted display of the currently allocated HPCOM control blocks. The displays are written to the ITK STC command log (HPOCLOG DD dynamically allocated as a SYSOUT data set).

This command has the following syntax:

```
/F DISPLAY INTERNAL  
/F DISPLAY INT  
/F DIS INTERNAL  
/F DIS INT  
/F D INTERNAL  
/F D INT
```

DISPLAY LOCK Command—List Current Lock Value

The DISPLAY LOCK command displays the current value of the main HPCOM spin lock, the module name, and offset of the instruction that last obtained the spin lock.

This command has the following syntax:

```
/F DISPLAY LOCK
/F DISPLAY L
/F DIS LOCK
/F DIS L
/F D LOCK
/F D L
```

DISPLAY REP Command—List Allocated Repositories

The DISPLAY REP command produces a formatted display of the currently allocated repositories. The displays are written to the ITK STC command log (HPOCLOG DD dynamically allocated as a SYSOUT data set).

This command has the following syntax:

```
/F DISPLAY REP
/F DIS REP
/F D REP
```

DISPLAY PAUSE Command—List Paused BMPs

The DISPLAY PAUSE command lists all paused batch message programs (BMPs).

This command has the following syntax:

```
DISPLAY PAUSE
```

Use the RESUME command to resume paused BMPs.

More information:

RESUME Command—Resume STC ITK

DUMP INTERNAL Command—Create Dump of HPCOM Control Blocks

The DUMP INTERNAL command produces a formatted dump of the currently allocated HPCOM control blocks. The dump is written to the ITK STC command log (HPOCLOG DD dynamically allocated as a SYSOUT data set).

This command has the following syntax:

```
/F DUMP INTERNAL
/F DUMP INT
/F DU INTERNAL
/F DU INT
```

DUMP REP Command—Create Repository Dump

The DUMP REP command produces a formatted dump of the currently allocated repositories. This includes all in-memory control blocks that describe the repository and the actual contents of the repository.

Use caution when issuing this command. The output can be voluminous. The dump is written to the ITK STC command log (HPOCLOG DD dynamically allocated as a SYSOUT data set).

This command has the following syntax:

```
/F DUMP REP
/F DU REP
```

ENABLE Command—Resume New FFOR Job Processing

The ENABLE command resumes processing of new FFOR reorg jobs following a DISABLE command.

This command has the following syntax:

```
/F ENABLE
/F ENA
```

More information:

DISABLE Command—Prevent Start of New FFOR Jobs.....

FREE LOCK Command—Free Lock Unconditionally

The FREE LOCK command unconditionally frees the main HPCOM spin lock.

Note: Issue this command only as directed by Technical Support.

This command has the following syntax:

```
/F FREE LOCK
/F FREE L
/F F LOCK
/F F L
```

KILL Command—Destroy Existing FFOR Repository

The KILL command forces the destruction of an existing FFOR repository. If this command is used, all database updates stored in the repository are lost. Do not issue this command against an IMS ID or database name (dbdname) that is associated with a running FFOR reorg job.

This command has the following syntax:

```
/F KILL imsid dbdname  
/F K imsid dbdname
```

REFRESH Command—Refresh SYSOUT Data Sets

The REFRESH command causes the current SYSOUT data set for the FFOR activity log (ALOG) or command log (CLOG) to be closed and freed. This makes these SYSOUT data sets available for printing or purging without having to bring down the ITK STC. A new activity log or command log data set is dynamically allocated.

This command has the following syntax:

```
/F REFRESH ALOG|CLOG  
/F REF ALOG | CLOG
```

ALOG

Refreshes and closes the FFOR activity log.

CLOG

Refreshes and closes the command log.

RESUME Command—Resume STC ITK

The RESUME command causes the STC to resume any paused BMPs. This option requires that the target databases of the BMP be started in the IMS regions first. We recommend using this option only after a previous failure.

Use the DISPLAY PAUSE command to list paused BMPs.

This command has the following syntax:

```
/F RESUME
```

Example: Resume STCITK

```
/F STCITK,RESUME
```

More information:

DISPLAY PAUSE Command—List Paused BMPs

SECTRACE Command—Set Trace Flags

The SECTRACE command turns on and off the ITK STC trace flags.

This command has the following syntax:

```
/F SET TRACE ON|OFF trace flag
```

```
/F SET TR ON|OFF trace flag
```

ON

Turns on ITK STC trace flags.

OFF

Turns off ITK STC trace flags.

trace flag

Specifies the trace flag (TR1 or TR2). TR1 controls tracing of records as they are being written into the repositories. TR2 controls the requests made of the ITK STC by batch reorg jobs.

BMP Pause and Resume Functionality

BMP Pause and Resume functionality is handled on behalf of the caller by the ITK STC started task. In Full Function and HALDB online reorganization in CA Database Organizer, this functionality is defaulted to BMPPAUSE=YES. However, in CA Database Copier and CA High Performance Recovery, the default is BMPPAUSE=NO.

Note: DEDBs must be registered as preopen to DBRC. Otherwise, FH status codes can occur on resume of the BMPs. For more information about changing DEDBs to preopen, see the IBM IMS DBRC documentation.

Appendix A: Global Parameter Processing

This section contains the following topics:

Global Parameters	157
How Global Parameter Processing Works	157
How To Activate Global Parameter Processing	159

Global Parameters

Global parameters let you establish site-specific defaults and simplify the preparation of JCL for individual jobs. Once defined, you can use these definitions to supplement the keyword parameters coded in the JCL control statements. Parameters that are not provided in the JCL are found in the global parameter data set for the function being performed.

How Global Parameter Processing Works

After you have activated global parameter processing, the following processing occurs:

- An attempt is always made to allocate the global parameter data set, and to read the control statements for the function being performed.

The global parameters are not read until all keyword parameters in the coded JCL for a function have been processed. At that point, the global parameters are read, and any keywords that were *not* specified in the JCL are used to supplement the parameter set for the current execution. These keywords control the processing of the current function just as if they had been entered in the JCL.

Any keywords found that have already been specified in the JCL for the job step are ignored.

Note: For example, if the global parameter data set contains ABENDDUMP=NO, but the JCL contains ABENDDUMP=YES, the final setting is ABENDDUMP=YES. If the global parameter data set contains ABENDDUMP=YES and the JCL does not specify a value for ABENDDUMP, the final setting is ABENDDUMP=YES.

- After all control statements for a function have been processed, the global parameter processing proceeds as follows based on whether a DD statement is present for IDIPARM and the type of data set:
 - If a DD statement exists for IDIPARM and the data set is a sequential file (including "DD *" in-stream data), the data set is opened and the control statements within it are processed as global parameters. The requested function is performed with the parameter set including the JCL and global parameters.
 - If a DD statement exists for IDIPARM and the data set is fully qualified PDS with a member name, the data set is opened and the control statements within it are processed as global parameters. The requested function is performed with the parameter set including the JCL and global parameters.
 - If a DD statement exists for IDIPARM and the data set is a PDS with no member name, the data set is opened using a standard member name for the function being performed. The control statements within it are processed as global parameters, and the requested function is performed with the parameter set including the JCL and global parameters.
 - If there is no DD statement for IDIPARM, the utility looks in STEPLIB for a DFSMDA load module named IDIPARM. If this is not found, no global parameter processing is done.

If the load module is found, the data set name it defines is dynamically allocated. If the data set defined is a PDS, the utility opens it using a member name based on the requested function and the control statements within it are processed as global parameters. The requested function is performed with the parameters set including the JCL and global parameters. An informational message is printed when the data set is allocated, which shows the data set name and the member name that were used.

If the load module is not found, global parameter processing is not done.

Note: To prevent abends from occurring when you execute a product that invokes another product, do not include the member name with the IDIPARM DD. This causes the default members names to be selected for each product.

- In all cases, before attempting to open a partitioned data set, an internal check is performed to ensure that the required member is present in the library. If not, a message is issued. This helps prevent S013 abends. If the job step contained a DD statement for a fully qualified PDS with a member name, and that member is not found, the job step terminates. However, if the member name is determined based on the function being performed, global parameter processing is bypassed.
- All control statements found in the global parameter data set are clearly identified and printed on the output MSGS file, following the listing of the JCL control statements. This provides a list of the values that were used for a function in the job.

Any serious errors encountered during processing of the global parameters results in error messages and termination of the job step.

How To Activate Global Parameter Processing

Global parameter processing lets you specify installation standard keyword definitions in a PDS member (or sequential data set) for each utility. Global parameter processing is not activated during installation and is optional.

Note: No JCL changes are required to implement global parameter processing; however, you can add a DD statement to any JOBSTEP for IDIPARM to override the standard data set name. IDIPARM points to a data set containing global parameters. These parameters supplement the keyword definitions coded in the JCL only for that JOBSTEP.

To activate global parameter processing, follow these steps:

1. [Customize global parameter members](#) (see page 159).
2. [Modify, assemble, and link the DFSMDA dynamic allocation load module into the load library that contains the products](#) (see page 161).

Customize Global Parameter Members

Important! Use caution when setting up global parameter members because any serious errors found during processing cause the termination of all job steps that use them. Familiarize yourself completely with the affected function *before* changing its global parameter library member.

The *hlq.CIMTPARM* library contains sample global parameter members. We recommend that you create your production library because new versions of the products create a library that can overwrite your changes.

The sample members contain only some of the parameters for each function. You can modify these members so that selected keyword parameters are in effect for all executions of the products. If you do not change these members, the provided global parameters match the documented defaults. If a sample member is not provided for a particular function, create a member with the standard member name that is defined for the function.

Follow these steps:

1. Rename or copy the provided global parameter library (parmlib) data set. You can use any valid data set name; however, we recommend that the lowest-level qualifier be PARMLIB to clearly identify what the data set is used for.
2. Add any defined keyword parameter to the global parameter member for the desired function.

Note: Some keywords do not logically apply to all functions or executions and we recommend not adding them. For example, DBDNAME is typically different for each execution.

3. Move or copy the modified global parameter members from the sample library to the production library that the utilities use.

Syntax Rules

You can code global parameters in CA or AMS syntax, regardless of the format used in the JCL. The utility recognizes and correctly processes the global parameters. Continue using one syntax type for all control statements in the JCL and one syntax type for all control statements in the global parameter data set.

All other syntax rules remain the same, as for normal JCL control statements.

Sample Parameter Library Member Names

The following standard member names are used during global parameter processing. Each of the products reads these members after the function to be performed has been determined. If the standard member name is not found for the function being performed, the affected utility executes without global parameter processing, and an informational message appears. This lets you install and activate global parameter processing only for selected products as needed.

Note: If you define the global parameter data set as a sequential data set, this list of member names does not apply. Instead, define and create the named data set, and verify that any control statements the data set contains are valid for all of the performed functions.

- FUNCTION=CHACCUM reads the CHACCUM member
- FUNCTION=ANALYZE reads the DBAANALZ member
- FUNCTION=COPY, COPIC, and IICOPY reads the DBCCOPY member
- FUNCTION=EXTRACT reads the DBEEXTR member
- FUNCTION=UNLOAD reads the DBOUNLD member
- FUNCTION=RELOAD or FORMAT reads the DBORELD member
- FUNCTION=REORG reads the HPOS1, HPOS2, HPOS4, HPOS5, HPOS6, and HPOREORG members

- FUNCTION=BATCHREORG reads the HPOREORG member
- FUNCTION=RECOVER reads the HPRRECOV member
- FUNCTION=ANALYZE for the Randomizer Analysis Program reads the RAPANALZ member
- FUNCTION=ALLOCHECK or THRESHBUILD for the Database Space Analyzer reads the DSAPARMS member
- FUNCTION=INDEXBUILD reads the SIBIBLD member
- FUNCTION=INDEXCREATE reads the SIBICRE member
- FUNCTION=INDEXEXTRACT reads the SIBIEXTR member
- FUNCTION=SIXBUILD reads the SIXIBLD member
- FUNCTION=SIXEXTRACT reads the SIXIEXTR member

Assemble the DFSMDA for the Parmlib

After you have renamed the parmlib data set and modified the global parameter members, you must assemble and link a DFSMDA load module for the parmlib. This has the form of a standard IMS dynamic allocation control block (DFSMDA), and defines the data set name that is used to access the library during execution.

Follow these steps:

1. Edit the IDIPARM sample job in *hlq.CIMTSAMP* as follows:
 - a. Change the JOB statement to meet local requirements.
 - b. Rename the data set name for SYSLIB in STPASM to define IMS GENLIB.
Note: If you rename the data set name for the parmlib, you must also change it on the DFSMDA macro in the SYSIN for STPASM so that the utilities are able to access it. This name can point to a PDS or to a standard 80-byte sequential file.
 - c. Change the data set name for SYSLMOD in STPIEWL to define the load library that contains the utilities.
 - d. Change any required parameters of the work data sets (SYSUT1, SYSUT2, SYSPUNCH) to meet local requirements.

Save your changes.

2. Submit the job for execution.

The installation parmlib is defined and global parameter processing is activated.

Appendix B: Installing the IMS Information Repository

This section contains the following topics:

IMS Information Repository	163
How To Install IIR	164
How To Install the CA Datacom/AD Environment	164
How To Install the IIR Database	165
Set Up the IIR Historical Reporting Application	170
How To Establish a Data Sharing Environment	171

IMS Information Repository

The IMS Information Repository (IIR) is an optional feature that works with the reporting and utility functions of the following products:

- CA Database Analyzer for IMS
- CA Database Copier
- CA Database Organizer
- CA High Performance Recovery
- CA Secondary Index Builder

IIR improves a DBA's ability to recognize trends based on historical data collected by these solutions. It does not affect the overall performance of the monitored utility jobs. The information collected provides significant benefit to the IMS user in performance tuning, problem determination, and resource planning.

How To Install IIR

Before you can use IIR, you must install the "pre-packaged" version of the CA Datacom environment and the IIR database.

Note: If you skip installation of IIR during the product install process, you can activate it later by completing the process described in this section.

To install IIR, follow these steps:

1. Install the required CA Common Services for z/OS (CCS) components as listed on your cover letter.
Note: If these components are already installed, you do not have to reinstall them. For more detailed information about CCS, see the CA Common Services documentation.
2. Specify IIRRECORD=YES in the batch JCL of the utility you want to execute with (CA Database Analyzer for IMS, CA Database Copier, CA Database Organizer, CA High Performance Recovery, or CA Secondary Index Builder).
3. Install the CA Datacom/AD environment.

Important! If you already have CA Datacom/DB or CA Datacom/AD installed, you can use the previously defined environment to run IIR and skip these installation steps.

Note: Installation of the CA Datacom/AD environment can precede or follow the product install. However, both steps must be completed before attempting to install the IIR database.

4. Install the IIR database.

How To Install the CA Datacom/AD Environment

The CA Datacom/AD environment is installed separately from the CA Database Analyzer for IMS, CA Database Copier, CA Database Organizer, CA High Performance Recovery, and CA Secondary Index Builder product installation and post-installation steps described in this guide.

Note: For the detailed installation steps for the CA Datacom/AD, see the *CA Datacom/AD for z/OS Installation Guide*. IIR does not require any tailoring or maintenance tasks to be performed in the CA Datacom/AD environment.

To install the CA Datacom/AD environment, review the following information in the *CA Datacom/AD for z/OS Installation Guide*:

- The product installation and pre-installation information in the "Introduction" chapter.
Note: You can use IPOUPDTE or CCPUPDTE to perform the SAMPJCL mass editing process to reduce installation time and JCL editing requirements.
- The hardware and software requirements and an introduction to using SMP/E and CA Common Services in the "System Requirements" chapter.
- The installation worksheet before you install the CA Datacom/AD environment to reduce the time needed to edit and execute the installation jobs.
- The installation procedures for all and new installations:
 - We recommend that you install CA Dataquery for CA Datacom for use with IIR so that you can select it as one of your reporting options.
 - Use the sample member @AXIPOIN when using IPOUPDTE to edit the installation. The sample member provides the "update" parameters in the specific order needed for the installation JCL editing. Also, make sure that each line of the sample input member (@AXIPOIN) is reviewed and updated with the appropriate worksheet value according to the comments (at the right of each line).
 - The demonstration phase includes several jobs that you can execute to verify that the CA Datacom/AD installation is up and operational before continuing with the steps to install the IIR database tables into the environment. We recommend that you execute these verification steps.
 - Review the post-installation considerations.
 - To use the online portion of CA Dataquery for CA Datacom, perform the CICS modifications steps to add the necessary definitions to the various CICS tables.
 - To create site standard jobs for starting and stopping the CA Datacom/AD environment, follow the recommended steps to set up production jobs. Information is also provided to build jobs to spill the LXX (logging area) and the PXX (diagnostics and statistics area). These jobs should be made available, but are not used on a daily basis by normal IIR users.

How To Install the IIR Database

IIR uses a database (set of tables) that is installed into the CA Datacom/AD environment.

Important! The CA Datacom/AD environment must already be successfully installed before you can install the IIR database.

To install the IIR database, follow these steps:

1. Start the CA Datacom/AD environment.
2. Define the IIR database and tables.
3. Catalog the IIR database and tables.
4. Initialize the data areas and prepare the IIR tables.
5. Back up the CA Datacom/AD environment.
6. Stop the CA Datacom/AD environment.
7. (Optional) Add new tables to an existing IIR installation.

Start the CA Datacom/AD Environment

The CA Datacom/AD environment must be up and operational before executing any of the IIR installation jobs.

To start the CA Datacom/AD environment, ensure ADnnSTRT is submitted for execution (nn is the release designation. For example, 12 for CA Datacom/AD r12). This member starts the CA Datacom/AD environment. This job is a long running task that should be submitted to a job class without a time or CPU limit. This environment must be available for any access to the CA Datacom/AD databases.

Important! Once the IIR installation is complete, the CA Datacom/AD environment must be "up" before attempting to run any of the IMS Toolkit functions with the IIRRECORD=YES specification.

Define the IIR Database and Tables

The IIR database is defined to the CA Datacom/AD environment using a batch utility program that is provided with the environment. The batch utility defines the IIR database (known as ITKREPDDB) and the tables needed to support the IIR data collection facilities.

Note: For the definition of the database tables and columns, see the *IMS Information Repository User Guide*.

Important! After the database is successfully defined, it should never need to be defined to the environment again. You can redefine the database definition, if needed; however, this would normally only be done under instructions from CA Support.

Follow these steps:

1. Edit the IIRINS1 member in the ITK CIMTSAMP member and save your changes.

The IIRINS1 member is updated.

2. Submit the edited member for execution.

The job executes the CA Datacom/AD DDUPDATE batch utility. The expected return code is 0.

Catalog the IIR Database and Tables

After the IIR database is defined, you must catalog the database definition using the DDRTVCAT batch utility provided by the CA Datacom/AD environment. This utility validates the database definition to make sure it matches the current IIR database model and then catalogs it to the environment. Once cataloged, the database is available for processing under the CA Datacom/AD environment.

Important! Once the database is cataloged successfully, it should never need to be cataloged to the environment again. You should only recatalog the database definition under instructions from CA Support. Rerunning the catalog of an active database definition could cause existing data in that database's tables to be marked unusable and result in a loss of existing data.

Follow these steps:

1. Edit the IIRINS2 member in the ITK CIMTSAMP member and save your changes.

The IIRINS2 member is updated.

2. Submit the edited member for execution.

The job executes the CA Datacom/AD DDRTVCAT batch utility. The expected return code is 0.

Initialize the Data Areas and Prepare the IIR Tables

After you have defined and cataloged the database, you must allocate and format a set of data sets that are used to hold the data (and indexes) for the IIR tables in the CA Datacom/AD environment.

After the data sets have been initialized and loaded successfully, the tables are ready for use with CA Database Analyzer for IMS, CA Database Copier, CA Database Organizer, CA High Performance Recovery, and CA Secondary Index Builder. The INIT and LOAD can be re-executed as needed; however, remember that when this job is executed it removes all existing IIR data. You might want to rerun this step to “clean” the slate and begin the IIR collection from the beginning.

Note: For a list of these data sets and for more information about cleaning up or resetting the data in the IIR tables, see the *IMS Information Repository User Guide*.

Follow these steps:

1. Edit the IIRINS3 member in the ITK CIMTSAMP and save your changes.
The IIRINS3 member is updated.
2. Submit the edited member for execution.
The job executes the CA Datacom/AD DBUTLTY batch utility. This utility formats (INIT) each of the data sets and marks them “null” loaded (loaded with no rows). The expected return code is 0.

Back Up the CA Datacom/AD Environment

During the CA Datacom/AD installation, you are instructed to run the AXNEW07 job. This job creates a backup of the CA Datacom/AD environment, which includes everything except the data stored in the IIR database.

To back up the CA Datacom/AD environment, reexecute AXNEW07 following the successful implementation of the IIR database.

The IIR data is saved with the CA Datacom/AD environment information.

Note: This job should be standardized for your environment and added to the regularly scheduled system backups. These backups are only needed in the case of a system failure or accidental deletion of one of the CA Datacom/AD system data sets. If this occurs, contact CA Technical Support for assistance in restoring the required data sets.

Stop the CA Datacom/AD Environment

During the installation and post installation tasks, you were instructed to tailor and save the JCL member ADnnSTOP (*nn* is the release designation, 10 or 11). This member is used to stop the CA Datacom/AD environment.

When all active jobs end, the CA Datacom/AD environment begins a normal shutdown. During shutdown, various statistical reports are generated.

To stop the CA Datacom/AD environment, run ADnnSTOP.

This job executes DBUTLTY with a control statement that requests the CA Datacom/AD address space (ADnnSTRT) begin termination processing. After the termination request is passed to the ADnnSTRT job (CA Datacom/AD environment), active user jobs (queries or reports) using the environment finish, but no new user jobs are permitted to start.

You can use the following console modify command to shut down the environment:

```
/F ADnnSTRT,E0J
```

Note: The same shutdown sequence occurs whether the termination request is issued through a batch job (ADnnSTOP) or the console command.

Add New Tables to an Existing IIR Installation

You can update your current IIR installation to add new tables that may have been added since the initial installation.

Follow these steps:

1. Browse the IIRINS1 member to see what tables already exist from the install.
The IIRINS1 member lists the tables that already exist in the IIR installation.
2. Do *one* of the following:
 - If all tables are installed, exit the member. No additional changes are needed.
 - If a table does not exist, locate and edit the new table member in ITK CIMTSAMP and save your changes. For DBA00A, use IIRADD0A. For DBA00B and DBA00C, use IIRADDBC. For DBA00D, use IIRADD0D. For DSA001, use IIRADDSA.

The member is updated.

3. Submit the edited members for execution.

The members are executed. The expected return code is 0.

Set Up the IIR Historical Reporting Application

The IIR Historical Reporting application reads data from the IIR database and provides DBD job reports through the ISPF interface. This application uses the plan file (IIRPLNIN), which provides a description of the SQL query that particular load modules execute on the CA Datacom/AD database. To enable the IIR Historical Reporting option, import the plan definition to CA Datacom/AD.

Follow these steps:

1. Edit the following variables in the IIREMAIN member of the common CLIST (*hlq.CIMTCLS0*):

ITKHLQ

Specifies the toolkit high-level qualifier.

hlq.custom-loadlib

Specifies your CA Datacom/AD custom load library.

Example: CAI.DATACOM.CUSLIB

hlq.common-loadlib

Specifies your CA Datacom/AD common load library.

Example: CAI.DATACOM.CAILIB for CA Datacom 11

2. Edit the IIRPLNIN member of the sample library PDS (CIMTSAMP) to mirror the IIR configuration from the IIREMAIN member of CLIST. Set the following variables:

hlq.custom-loadlib

Specifies your CA Datacom/AD custom load library.

Example: CAI.DATACOM.CUSLIB

hlq.common-loadlib

Specifies your CA Datacom/AD common load library.

Example: CAI.DATACOM.CAILIB for CA Datacom 11

hlq.samplib(IIRPLN)

Specifies the plan file to import.

Example: CAI.IMS.TOOLKIT.CIMTSAMP(IIRPLN)

3. Run IIRPLNIN.

The plan file is imported to CA Datacom/AD.

How To Establish a Data Sharing Environment

You can use IIR in a data sharing environment, with more than one LPAR writing data to and accessing data from the CA Datacom Repository database. You can convert a single LPAR CA Datacom/AD system into a data sharing environment.

To establish a data sharing environment, follow these steps:

1. Specify the following parameters in the existing DBSIDPR module:

TOMUF=*mufname1*

Execution Multi User Facility (MUF) or CA Datacom control region name (accessing the CA Datacom database).

TOGROUP=*group_name*

Sharing group name (used with XCF).

2. Assemble and link the new DBSIDPR module (see install job AXINS05).
3. Specify the following MUF (Multi User Facility = Datacom control region) start options in CUSMAC member DBDATIN1:

MUF *mufname1*

Execution MUF name (accessing the CA Datacom database).

TASKS 20,mK,,,8

Number of tasks (20) allowed in MUF LPAR and number of tasks (8) allowed in remote LPAR. These numbers can be increased if necessary.

XCFFROM **,group_name*

Sharing group name (used with XCF).

4. APF authorize all MUF start job STEPLIB libraries in the execution MUF LPAR.
5. Ensure that XCF structure for inter-region communication exists.
6. Start the execution MUF job on LPAR1.

You can now write data to and execute data from the CA Datacom/AD database from all LPARs sharing this XCF group.

Appendix C: Using Snapshot General Services

This section contains the following topics:

Snapshot Overview	173
Initialize Snapshot General Services	174
Reinitialize Snapshot General Services	175
IBM Shark and Hitachi Data Systems Devices	175
Determine Whether a Device is FlashCopy II-Compatible	176
Initialization Parameters	176
Parameter Statements	178
Snapshot General Services Health Checks	187

Snapshot Overview

Snapshot General Services is a high-performance access method for the utility products. Snapshot General Services lets you exploit the point-in-time copy hardware features available on DASD subsystems from various vendors. This can greatly reduce the amount of time that tablespaces are unavailable to applications to make the copy.

After you initialize Snapshot General Services, you can use it to perform a point-in-time copy by specifying `SNAPSHOTACCESS YES` or `INSTANT` in your JCL.

Initialize Snapshot General Services

The Snapshot General Services subsystem is typically initialized by CAIRIM at IPL time. To make this happen, add a command to the CAIRIM startup parameters. The startup parameters are in the data set or member allocated to the PARMLIB DD statement in the CAIRIM started task procedure.

To initialize Snapshot General Services, add the following command to the CAIRIM started task procedure:

```
PRODUCT(SNAPSHOT GEN SERVICE) VERSION(TG10) INIT(IEFBR14) -  
  PARM(parameters)
```

The PRODUCT keyword begins in column 2 and specifies the service or solution description (up to 20 characters). This parameter is specified once for each product to be installed. The first line ends with a hyphen to show that the line is continued. The parameters in the PARM keyword can have a maximum length of 32 characters.

Note: If CAIRIM is used to initialize Snapshot General Services, ensure that all related maintenance has been applied to ensure correct parameter parsing. Otherwise, TGRPAR011E messages may be received on valid parameters. For more information about CA Common Services requirements, see the *CA Common Services Installation Guide*.

More information:

Initialization Parameters

Important! If the same Snapshot General Services subsystem is used when upgrading to a new maintenance level or migrating from release to release, an IPL is required.

Reinitialize Snapshot General Services

The following situations require that you reinitialize the Snapshot General Services subsystem:

- Snapshot General Services initialization parameters are changed after IPL.
- New versions of Snapshot General Services modules are installed after IPL.

Follow these steps:

1. Update the STARTTIG job supplied in the sample JCL library (*hlq.CIMTSAMP*) as follows:
 - Specify any necessary parameters in the PARM field of the EXEC statement.
 - Change the STEPLIB DD to point to the library where Snapshot General Services modules are installed, or comment it out if the modules are in a linklist library.
2. Run the TGRINIT job.

Snapshot General Services is reinitialized.

IBM Shark and Hitachi Data Systems Devices

Snapshot General Services supports the following storage devices:

- IBM 2105 and 2107 and DS8000 series Shark devices
- Hitachi Data Systems (HDS) devices (if the Hitachi Compatible Mirroring for IBM FlashCopy feature is installed)

Because HDS devices emulate IBM Shark devices, this section applies to both types.

Both IBM Shark devices and HDS devices use FlashCopy to perform instant copies from one volume to another. Both device types can use the older FlashCopy I mode. When you use FlashCopy I, each source volume must have a dedicated target volume with an identical track address. A target volume cannot be shared with other source volumes, because collisions and data corruption occur when two source volumes copy data to the same track on the target volume. Also, a target volume must be used *only* for temporary point-in-time copies. When Snapshot General Services processes its copies, it destroys any other data sets that have been written to the volume. The VOLGROUP statement is used to define your devices as FlashCopy I and map the source volumes to their dedicated target volumes.

Newer devices can also use FlashCopy II mode, which provides more flexibility. When you use FlashCopy II, no dedicated target volume is required. The copy data set is allocated in the same SMS storage class as the source data set. (You can also specify a different storage class, on a masked dsname basis, using the DSNGROUP statement.) The VOLGROUP statement is used to define your devices as FlashCopy II.

Determine Whether a Device is FlashCopy II-Compatible

All IBM Shark and HDS devices supported by Snapshot General Services are compatible with FlashCopy I, but only newer devices are FlashCopy II-compatible. In the VOLGROUP statement, the FCVER operand specifies whether to treat the devices as FlashCopy I or FlashCopy II. If you are unsure whether your devices are FlashCopy II-compatible, use this procedure to verify their compatibility.

Follow these steps:

1. Enter **FCQUERY DEVN(X'nnnn')** (in which 'nnnn' is the device's hexadecimal number) at a TSO READY prompt and press Enter.

Detailed information about the selected device appears, followed by another READY prompt.
2. View the information. If an ACT column is present, the device is FlashCopy II-compatible. If a STATUS column is present, the device is FlashCopy I only.

Initialization Parameters

The following initialization parameters are valid for Snapshot General Services:

INITMSG

Displays extra initialization messages on the console. These messages provide additional information such as the version of the initialization program and the location of important control blocks. This information is not needed during normal operation, and tends to clutter the consoles, but it can be useful during troubleshooting.

PARMDSN(*dsname*)*

Defines the name of the Snapshot General Services parameter data set, where *dsname* is the name of a sequential data set; or if a member name is specified, a member of a partitioned data set.

Note: You can also preallocate the parameter data set to TGRPARM in the CAIRIM or TG10INIT initialization JCL. This overrides the PARMDSN value.

PARMVOL(*volume*)*

Defines the volume serial number where the Snapshot General Services parameter data set resides, where *volume* is the one- to six-character volume serial number of the volume. This parameter is not required if the data set is cataloged.

Note: You can also preallocate the parameter data set to TGRPARAM in the CAIRIM or TG10INIT initialization JCL. This overrides the PARMVOL value.

Because CAIRIM limits the PARM field to 32 characters, it is not practical to specify PARMDSN and PARMVOL as parameters. Instead, put a //TGRPARAM DD statement in the CAIRIM procedure that points to the Snapshot General Services parameter file. Optionally, you can do this in the TG10INIT reinitialization job (instead of specifying PARMDSN and PARMVOL in the JCL parameter).

SUBSYS(*name*)

Defines the one- to four-character name of a poly-Snapshot General Services subsystem. You cannot use the name CATG because it is reserved for the master Snapshot General Services subsystem.

If specified on initial startup, TG10INIT initializes the master Snapshot General Services subsystem, and then initializes the specified Snapshot General Services subsystem. If TG10INIT is run after initial startup and SUBSYS is specified, only the specified Snapshot General Services subsystem is initialized or reinitialized.

The default or master subsystem is generally used for production processing. The SUBSYS parameter is not required for the master subsystem. Typically, additional subsystems would be defined only for testing, or at the request of Technical Support.

To make a job use a subsystem other than the master, add a special DD statement to its JCL as follows:

```
//TGRSUBSY DD SUBSYS=name
```

name

Defines the name of the subsystem, as defined in the SUBSYS(*name*) initialization parameter.

XMANID(*xmanid*) or XMANID(NULL)

Defines the Xmanager ID of the Xmanager address space to associate with this Snapshot General Services subsystem. Typically, you do not need to specify this; when an Xmanager address space starts, the Snapshot General Services subsystem it uses is automatically associated with it.

If you specify XMANID, then any Xmanager address space that uses this subsystem must have the specified XMANID. XMANID(NULL) removes the association between the subsystem and the XMANID.

Parameter Statements

The parameter statements in the Snapshot General Services parameter file are used to map IBM 2105 (Shark) source volumes to target volumes and to specify global options. When multiple statements apply, such as two VOLGROUP statements that apply to a volume serial number, the first statement defined in the parameter file is used.

A sample parameter library definition is provided in the TGRPARM member of *high-level.PARMLIB*.

Note: You can enter comments in the Snapshot General Services parameter file by putting an asterisk in column 1. You can continue non-comment lines by ending them with a hyphen.

BCVGROUP Statement

The BCVGROUP statement gives a name to a group of business continuation volumes (BCVs) so that they can be conveniently referred to in DSNGROUP statements. These BCVs have been split from the volumes they mirror, re-clipped with a different volume serial number, and brought online. The BCVs determine where copies are put when copying data sets on EMC devices. The following operands can be used with this statement:

NAME(*group-name*)

Defines the name associated with this BCVGROUP. The name is used to refer to the group in DSNGROUP statements. This is a required operand.

Limits: 1 to 8 characters

VOLUMES(*vol-list*)

Defines a list of one or more volume serial numbers or masks, separated by commas or blanks, to which the BCVGROUP applies. This is a required operand.

Limits: 1 to 6 characters (per serial number or mask)

When using a mask to specify a list of volume serial numbers, the following rules apply:

- An underscore (_) represents a single character.
- A percent sign (%) represents a string of zero or more characters.
- Any other character represents itself.

We recommend that you pad a mask that ends in a percent sign to the proper length with percent signs. Otherwise, the system pads the mask with blanks. For example, a mask of ABC% is padded with blanks to six characters, and matches volume serial numbers beginning with ABC and ending with two blanks, such as ABC, ABCD, ABC1, and so on, but does not match ABCDE or ABC001. To match all volumes that begin with ABC, specify this mask as ABC%%.

DSNGROUP Statement

The DSNGROUP statement defines the allocation characteristics for copies of particular groups of data set on EMC storage devices. By default, Snapshot General Services copies the SMS data class, SMS management class, and SMS storage class from the source data set. Use the DSNGROUP statement to specify different allocation characteristics for the flash image copy data sets.

The following operands can be used with this statement:

NAME(*group-name*)
DSNMASK(*dsn-mask*)
[BCVGROUP(*b-group*)]
[DATACLAS(*d-class*)]
[MGMTCLAS(*m-class*)]
[STORCLAS(*s-class*)]

NAME(*group-name*)

Specifies the name associated with a DSNGROUP. The name is used in messages to identify the DSNGROUP in use.

Limits: 1 to 8 characters

DSNMASK(*dsn-mask*)

Specifies the names of source data sets. The DSNGROUP statement defines the allocation characteristics for the copies of the data sets whose data set name matches the *dsn-mask*. You can specify a single mask for each DSNGROUP.

Limits: 1 to 44 characters. The mask must specify at least as many qualifiers as the tablespace name to be matched.

When specifying *dsn-mask*, the following rules apply:

- An underscore (_) represents a single character.
- A percent sign (%) represents a string of zero or more characters.
- Any other character represents itself.

Examples: A typical DB2 tablespace name (source) might look like the following:

D81A.DSNDBC.LG6DB.PAYROLL.I0001.A001

- To match all tablespaces in the D81A subsystem, specify the *dsn-mask* as follows:

D81A.%.%.%.%.%

- To match tablespaces for the LG6DB database in the D81A subsystem, the LG7DB database, the LG8DB database, and any other database with a name beginning with LG, followed by a single character, followed by DB, specify the *dsn-mask* as follows:

D81A.%.LG_DB.%.%.%

- To match the same tablespaces as the previous mask, but would also match the LGDB database, the LG95DB database, the LG1024DB database, and so on, specify the *dsn-mask* as follows:

D81A.%.LG%DB.%.%.%

Note: When a masked data set name is passed to Snapshot General Services (for example, D81A.DSNDBC.LG6DB.PAYROLL.I0001.A%), only the DSNGROUP information that matches the first data set is used.

BCVGROUP(*b-group*)

(Optional) Defines the name of a BCV group defined with a BCVGROUP statement. If you specify a BCVGROUP when the data set to be copied is on an EMC storage device, the copy is allocated on one or more of the volumes in the BCV group.

DATACLAS(*d-class*)

(Optional) Defines the SMS data class to use for copies of this data set.

Note: DATACLAS is ignored when you specify BCVGROUP.

MGMTCLAS(*m-class*)

(Optional) Defines the SMS management class to use for copies of this data set.

Note: MGMTCLAS is ignored when you specify BCVGROUP.

STORCLAS(*s-class*)

(Optional) Defines the SMS storage class to use for copies of this data set.

Note: STORCLAS is ignored when you specify BCVGROUP.

VOLGROUP Statement

The VOLGROUP statement is used to define IBM Shark or HDS source volumes as FlashCopy I or FlashCopy II devices and, for FlashCopy I devices, to map source volumes to target volumes.

Note: If you omit the VOLGROUP statement, FlashCopy I mode is used. However, you will receive an error message because Snapshot General Services requires the TGTMAP operand from the VOLGROUP statement to map the volumes.

The following operands can be used with this statement:

NAME(*group-name*)

Specifies a name for this VOLGROUP. This operand is required.

Limits: 1–8 characters

VOLUMES(*vol-list*)

Specifies the volume serial numbers to which this VOLGROUP statement applies. You can also specify masks. Separate the numbers or masks with commas or blanks. This operand is required.

Limits: 1–6 characters per item

The following rules apply to volume serial number masks:

- An underscore (_) represents a single character.
- A percent sign (%) represents a string of zero or more characters.
- Any other character represents itself.

A mask that ends in a percent sign should be padded to the proper length with percent signs. For example, a mask of ABC% will be padded with blanks to six characters, and will match volume serial numbers beginning with ABC and ending with two blanks. Thus, it would match volsers of ABC, ABCD, ABC1, and so on, but would not match ABCDE or ABC001. To match all volsers that begin with ABC, you must specify this mask as ABC%%%.

If multiple VOLGROUP statements apply to the same volume, the first statement encountered in the initialization parameters is used. For example, consider the following VOLGROUP statements:

```
VOLGROUP NAME(GROUP1) VOLUMES(PRD%%%) FCVER(2)
```

```
VOLGROUP NAME(GROUP2) VOLUMES(PRD123) FCVER(1)
```

The PRD123 volume belongs to GROUP1 because that was the first VOLGROUP statement that matched it.

FCVER(1|2)

Specifies whether to treat the devices for this VOLGROUP statement as FlashCopy I or FlashCopy II. FlashCopy I devices must be defined as FCVER(1). FlashCopy II-compatible devices can be defined as FCVER(1) or FCVER(2). If you specify FCVER(1), you must use the TGTMAP operand to map your source volumes to your target volumes.

Note: If you omit FCVER from the VOLGROUP statement, the devices will be treated as FlashCopy I.

TGTMAP(*tgt-map*)

Defines a mask that maps the source volumes to the target volumes. This operand applies only to FlashCopy I devices (devices specified or defaulted as FCVER(1)), and is required for those devices. For devices defined as FCVER(2), it is ignored.

Important! The target volumes specified here must be dedicated to Snapshot General Services. *They must not be used by any other jobs or systems.* Snapshot General Services manages the space on the volumes and will destroy any data put on the volumes by other jobs or systems.

The target volser map is specified like a volser, but with the following special characters to specify mapping:

- A percent sign (%) copies the character in that position from the source volser.
- An asterisk (*) at the end of a map copies all remaining characters from the source volser. Inserting an asterisk at the end is equivalent to replacing the asterisk and following blanks with percent signs.
- Any other characters in the map are copied to the target volser, replacing the characters in the equivalent positions of the source volser.

For example, the following VOLGROUP statement will allocate the copy data set on the BKP050 volume:

```
VOLGROUP NAME(GROUP2) VOLUMES(SYS050) TGTMAP(BKP%%%) FCVER(1)
```

Both the source and target volume serial numbers can be masked. For example, consider the following VOLGROUP statement:

```
VOLGROUP NAME(GROUP3) VOLUMES(PRD%%%) TGTMAP(SGS***) FCVER(1)
```

In the previous statement, any volume whose volser begins with PRD has a corresponding target volser that is the same, except that the characters PRD are replaced by SGS. Thus, source volumes PRD123, PRD001, and PRD975 have target volumes SGS123, SGS001, and SGS975, respectively.

There must be a one-to-one correspondence between source and target volumes. The easiest way to do this is to set up a naming convention for source volumes and their corresponding target volumes. For example, a VOLGROUP statement that specified VOLUMES(SRC%%%) and TGTMAP(CPY%%%) would map SRC001 to CPY001, SRC002 to CPY002, and so on.

IXVTOC(YES|NO)

Specifies whether to use an indexed VTOC on the target volume.

Important! Do not use this keyword unless requested by CA Support.

Default: YES

Note: You cannot copy Extended Format data sets (for example, striped data sets) on a volume in a VOLGROUP with IXVTOC(NO) specified.

OPTIONS Statement

The OPTIONS statement specifies global options that apply to all Snapshot General Services executions.

The following operands can be used in this statement:

MESSAGES(ALL|STD)

Specifies one of the following options for displaying messages:

ALL

Returns all messages to the caller.

You can specify MESSAGES(ALL) on a job-by-job basis by including a DD DUMMY statement in the JCL, with a ddname of TGRDEBUEG, as follows:

```
//TGRDEBUEG DD DUMMY
```

STD

Suppresses unimportant messages.

EMCPARAL(YES|NO)

Specifies whether to use parallel processing when copying data sets on EMC devices when available (EMC version 5.4.0 or later):

YES

Uses parallel processing if available.

NO

Does not use parallel processing, even if it is available.

Important! Specify EMCPARAL(NO) only at the direction of CA Support.

MAXATASK(*num-tasks*)

Specifies the number of parallel allocation tasks to be used for FlashCopy II copies.

Limits: 1–99

Default: 1

The optimum value for this option varies from site to site, therefore some experimentation is necessary. When you increase *num-tasks*, performance improves up to a point, and then it decreases.

To see how long the allocation tasks take, specify MESSAGES(ALL) or include a //TGRDEBUG DD DUMMY statement in the JCL, and then review the TGRIBY007I and TGRIBY008I messages:

```
TGRIBY007I All FlashCopy II allocation tasks have completed
TGRIBY008I (1) ARC: 0 TRC: 0 Duration: 00:00:09.505232 Count: 4
TGRIBY008I (2) ARC: 0 TRC: 0 Duration: 00:00:05.409171 Count: 2
```

MAXCTASK(*num-tasks*)

Specifies the number of parallel copy tasks to be used for FlashCopy II copies.

Limits: 1–99

Default: 1

The optimum value for this option varies from site to site, therefore some experimentation is necessary. When you increase *num-tasks*, performance improves up to a point, and then it decreases.

To see how long the copy tasks take, specify MESSAGES(ALL) or include a //TGRDEBUG DD DUMMY statement in the JCL, and then review the TGRIBY007I and TGRIBY008I messages:

```
TGRIBY007I All FlashCopy II copy tasks have completed
TGRIBY008I (1) ARC: 0 TRC: 0 Duration: 00:00:00.118480 Count: 6
TGRIBY008I (2) ARC: 0 TRC: 0 Duration: 00:00:00.115612 Count: 8
```

STATINTV(*status-interval*)

Specifies how often in seconds checks for completion of the copy operation are performed on the flash DASD device. When SNAPSHOTACCESS INSTANT or FLASHIC=YES is specified, Snapshot General Services waits for the physical copy to complete before registering the copy and continuing processing.

Default: 15

Limits: 1–3600

Note: The STATINTV value should not exceed the JWT value specified in the SMFPRMxx member of SYS1.PARMLIB. (JWT has a default value of 600 seconds). If STATINTV has a larger value, the job abends.

If you specify MESSAGES(ALL), or if you include a //TGRDEBUG DD DUMMY statement in the JCL, STATINV also controls how often the TGRF2K003I status messages are issued. See the following sample messages:

```
TGRF2K003I FC2 Copy Status at 18:11:35.04: 0% done
TGRF2K003I FC2 Copy Status at 18:11:55.09: 26% done
TGRF2K003I FC2 Copy Status at 18:12:15.18: 52% done
TGRF2K003I FC2 Copy Status at 18:12:35.24: 79% done
TGRF2K003I FC2 Copy Status at 18:12:55.29: 92% done
TGRF2K003I FC2 Copy Status at 18:13:15.34: 100% done
```


Appendix D: Snapshot General Services Health Checks

This appendix describes health checks for Snapshot General Services. The product owner for all Snapshot General Services health checks is CA_DB2.

DB2_TGR_CHECK_FCII_DEVS@xmanxxxx

Description

This Snapshot General Services check looks for FlashCopy II-capable devices that are defined to Snapshot General Services as FlashCopy I devices. Redefining them as FlashCopy II devices can greatly reduce the number of needed disk volumes.

This check runs when Xmanager is initialized, and every time a Snapshot General Services subsystem is initialized or reinitialized.

Best Practice

Defining a device as FlashCopy II can significantly reduce storage requirements and operational complexity. Unlike FlashCopy I devices, FlashCopy II devices do not require a dedicated target volume for each source volume, and permit multiple jobs to be copied to or from the same device concurrently.

You can define the device type by using the VOLGROUP statement in the Snapshot General Services initialization parameters.

Parameters Accepted

The following parameter can be set in the VOLGROUP statement:

FCVER(1|2)

Defines whether a device is FlashCopy I or FlashCopy II.

Debug Support

No.

Verbose Support

No.

Reference

For instructions on defining device types, see [VOLGROUP Statement](#) (see page 181).

Messages

See the *Message Reference Guide*.

Appendix E: Snapshot General Services Health Checks

This appendix describes health checks for Snapshot General Services. The product owner for all Snapshot General Services health checks is CA_DB2.

DB2_TGR_CHECK_FCII_DEVS@xmanxxxx

Description

This Snapshot General Services check looks for FlashCopy II-capable devices that are defined to Snapshot General Services as FlashCopy I devices. Redefining them as FlashCopy II devices can greatly reduce the number of needed disk volumes.

This check runs when Xmanager is initialized, and every time a Snapshot General Services subsystem is initialized or reinitialized.

Best Practice

Defining a device as FlashCopy II can significantly reduce storage requirements and operational complexity. Unlike FlashCopy I devices, FlashCopy II devices do not require a dedicated target volume for each source volume, and permit multiple jobs to be copied to or from the same device concurrently.

You can define the device type by using the VOLGROUP statement in the Snapshot General Services initialization parameters.

Parameters Accepted

The following parameter can be set in the VOLGROUP statement:

FCVER(1|2)

Defines whether a device is FlashCopy I or FlashCopy II.

Debug Support

No.

Verbose Support

No.

Reference

For instructions on defining device types, see [VOLGROUP Statement](#) (see page 181).

Messages

See the *Message Reference Guide*.

Appendix F: CA Database Organizer Health Checks

This appendix describes health checks for CA Database Organizer. The product owner for all CA Database Organizer health checks is CA IMSTOOLS.

IMST_ITK_STC_ABEND@jobname

Description

The ITK started task attaches many tasks that work can be dispatched on. It is critical that all tasks are available and running normally. This health check verifies that each subtask is running normally and that there are no abending tasks. When all subtasks are operating normally, the health check generates a message that indicates the ITK STC is operating normally and that there are no abending tasks.

Best Practice

Review the messages generated from this health check to verify that all of the required subtasks are executing. Early notification on the potential need to fix the ITK STC helps avoid unscheduled downtime and assists you in pro-actively maintaining your software.

Parameters Accepted

No.

Debug Support

When one or more subtasks contain errors, the health check generates an exception error that assigns a severity level to the exception and lists the abending tasks. Additional messages are also generated to help diagnose and correct the condition. Notify the systems programmer of this condition.

We recommend that the systems programmer performs the following steps:

1. Issue the following command from a z/OS console:

```
DUMP COMM=(jjj)
```

The system issues the following command:

```
*id IEE094D SPECIFY OPERAND(S) FOR DUMP COMMAND
```

2. Reply as follows:

```
Rid, JOBNAME=jjj, SDATA=(SQA, CSA, PSA, TRT, LSQA, RGN, SUM, SWA)
```

The SVC dump completes.

3. Issue the following command:

P jjj

The ITK started task is terminated.

4. Enter the following command:

S jjj

The ITK started task is started.

Verbose Support

No.

Reference

For more information about the ITK started task, see the *CA Database Management Solutions for IMS for z/OS Installation Guide*.

For more information about the DUMP command, see the *IBM z/OS System Commands*.

Messages

For more information about messages related to this health check, see the *CA Database Management Solutions for IMS for z/OS Message Reference Guide*.

More information:

ITK STC Started Task Considerations

Index

A

allocate and mount • 39

C

CAI.SAMPJCL

library • 58

sample jobs • 58

contacting technical support • 5

copy files to USS directory • 42, 43, 46

customer support, contacting • 5

D

download

files using ESD • 35

options • 42

overview • 33

to mainframe through a PC • 46

using batch JCL • 43

E

external HOLDDATA • 54

F

free space • 38

G

GIMUNZIP utility • 48

H

hash setting • 48

high-level qualifier • 48

HOLDDATA • 54

I

IEBCOPY • 58

installing

from Pax-Enhanced ESD • 33

from tape • 57

Integrated Cryptographic Services Facility (ICSF) • 48

internal HOLDDATA • 54

J

Java version support • 48

M

maintenance • 53

P

pax ESD procedure

copy product files • 42

create product directory • 47

download files • 35

set up USS directory • 38

pax file

copy files to USS directory • 42, 43, 46

process overview • 33

product download window • 35

product-level directory • 47

R

read me • 33, 48

S

sample JCL • 58

sample jobs • 43, 47

CAtoMainframe.txt • 43

Unpackage.txt • 47

SMP/E

GIMUNZIP utility • 48

support, contacting • 5

T

tape, installing from • 57

technical support, contacting • 5

U

UNIX System Services (USS)

access requirements • 33, 38

directory cleanup • 52

directory structure • 38

UNZIPJCL • 48