

CA Librarian®

Installation Guide

r4.4



Second 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 © 2010 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 ACF2™ for z/OS (CA ACF2)
- CA Culprit™ (CA Culprit)
- CA Datadictionary™ (CA Datadictionary)
- CA Earl™ (CA Earl)
- CA Endeavor® (CA Endeavor)
- CA Librarian® (CA Librarian)
- CA Mainframe Software Manager (CA MSM)
- CA Netman™ (CA Netman)
- CA Roscoe® (CA Roscoe)
- CA Scheduler® (CA Scheduler)
- CA Top Secret® for z/OS (CA Top Secret)
- CA 7® Workload Automation (CA 7)

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 in the second edition of this documentation:

- [Install the ISPF Options](#) (see page 206)—Updated JCL content to reflect correct PANELS information.

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

- All pre-installation, installation, and configuration steps now reside in the *Installation Guide*. This guide includes the steps to install your product using the follow methods:
 - CA MSM—CA MSM simplifies and unifies the management of CA mainframe products on z/OS systems. The services provided by CA MSM acquire, install, deploy, and maintain products in a common way.
 - Pax-Enhanced Electronic Software Delivery (ESD)—This utility helps download and install CA's mainframe software and maintenance electronically to your own disk.
 - Tape

Contents

Chapter 1: Overview 13

Audience	13
How the Installation Process Works.....	13

Chapter 2: Preparing for Installation 15

Hardware Requirements	15
DASD Devices	15
Software Requirements	15
Compatibility with IBM Software	16
Compatibility with Compilers.....	16
Compatibility with CA Software	16
CA Common Services for z/OS and OS/390 Components	16
Optional Components	17
CA Common Services for z/OS and OS/390.....	17
CAIRIM	18
CAISSF.....	18
CA-C Runtime	19
CA Earl Reporting Service.....	19
CA SRAM Service	19
Storage Requirements.....	20
Target Libraries	20
Distribution Libraries.....	21
Product Libraries	22
Pre-Installation Considerations	22
GRS Considerations	24
GRS Considerations for Wide Record Master Files	25
Concurrent Releases	25

Chapter 3: Installing Your Product Using CA MSM 27

CA MSM Documentation.....	27
Getting Started Using CA MSM	28
How to Use CA MSM: Scenarios.....	28
Access CA MSM Using the Web-Based Interface	37
Acquiring Products	38
Update Software Catalog	38
Download Product Installation Package	39

Migrate Installation Packages Downloaded External to CA MSM	40
Add a Product.....	41
Installing Products.....	43
Install a Product	43
Create a CSI	46
Download LMP Keys.....	49
Maintaining Products	50
How to Apply Maintenance Packages	50
Download Product Maintenance Packages.....	51
Download Maintenance Packages for Old Product Releases and Service Packs	52
Manage Maintenance Downloaded External to CA MSM	53
Manage Maintenance	55
GROUPEXTEND Mode	59
Back Out Maintenance.....	63
Setting System Registry	64
View a System Registry	64
Create a Non-sysplex System	65
Create a Sysplex or Monoplex.....	66
Create a Shared DASD Cluster.....	67
Create a Staging System.....	68
Authorization	69
Change a System Registry	70
Maintain a System Registry using the List Option.....	76
Delete a System Registry.....	77
FTP Locations	77
Data Destinations.....	81
Remote Credentials.....	87
Deploying Products	89
Deployment Status.....	90
Creating Deployments.....	91
View a Deployment.....	96
Change Deployments	97
Delete a Deployment	103
Confirm a Deployment	104
Products	106
Custom Data Sets	108
Methodologies	115
Systems	132
Deployment Summary	134

Chapter 4: Installing Your Product from Pax-Enhanced ESD **137**

How to Install a Product Using Pax-Enhanced ESD	137
How the Pax-Enhanced ESD Download Works	139
ESD Product Download Window	139
USS Environment Setup	142
Allocate and Mount a File System	143
Copy the Product Pax Files into Your USS Directory	146
Download Using Batch JCL	147
Download Files to Mainframe through a PC	150
Create a Product Directory from the Pax File	151
Sample Job to Execute the Pax Command (Unpackage.txt)	152
Copy Installation Files to z/OS Data Sets	152
Receiving the SMP/E Package	153
How to Install Products Using Native SMP/E JCL	154
Prepare the SMP/E Environment for Pax Installation	154
Run the Installation Jobs for a Pax Installation	156
Clean Up the USS Directory	156
Apply Maintenance	157
Maintenance	158
HOLDDATA	159

Chapter 5: Installing Your Product from Tape **161**

Chapter 6: Installation Tape **163**

Contents of the Installation Tape	163
Unload the Sample JCL from Tape	164
How to Install Products Using Native SMP/E JCL	165
Prepare the SMP/E Environment for Tape Installation	166
Run the Installation Jobs for a Tape Installation	167
Apply Maintenance	168
HOLDDATA	169

Chapter 7: Deploying Your Product **171**

Chapter 8: Configuring Your Product **173**

LIB/CCF System Master File Conversion	173
Upgrading from LIB/CCF r3.7 or Earlier	175
CCFCNV37	175
Execution of CCFCNV37	176

Reformatting the System Master File Under CA Roscoe	178
Suggested Conversion Procedures (CA Roscoe and TSO)	178
Suggested Conversion Procedures (VM/ESA and z/VM).....	180
CCFCNV37 Error and Informational Messages.....	181
Allocate Optional VSAM Control File.....	187
Initialize VSAM Control File	188
Receive/Apply Customer ID USERMOD.....	188
Receive/Apply Module Rename USERMOD	189
Install External Security Interface, Activate LAM Subsystem.....	190
ECSA Requirement	190
Activate LAM Subsystem.....	190
How to Run Two Versions of the LAM Subsystem	191
Modifying CAIRIM	192
RIM Rules	192
Optional External Security USERMOD.....	193
Execute LAMSERV (Optional)	194
Install ELIPS (Optional)	194
Assemble and Link the ELIPSGEN Macro.....	194
Customize Panels	204
Install the CA Roscoe Interface (Optional)	205
Install the ISPF Options	206
Copy LIB/CCF Model System	207
Install LIB/TSO	207
The \$LIBTSO Macro	208
Create the TLICD File	215
Install the LIB/TSO HELP Commands.....	216
Install LIB/CCF-CA Roscoe.....	219
Install the LIB/CCF RPF Members.....	220
Assemble and Link the \$CCFGEN Macro	222
Apply Optional LIB/CCF USERMODS	222
Update the Eligible Program List.....	223
Review the JCL Skeletons	224
Modify the LIB/CCF System Tables.....	226
Install LIB/CCF-ISPF(TSO).....	226
Assemble and Link the \$CCFGEN Macro	227
Apply Optional LIB/CCF USERMODS	229
Update the TSO Table (Optional)	229
Review the JCL Skeletons	230
Modify the LIB/CCF System Tables.....	231
Install LIB/DD.....	231
Verify the Product	232
Install UCRs (Optional)	232

Appendix A: Upgrading from LIB/CCF Release 3.7 or Earlier	233
CCFCNV37.....	233
Execution of CCFCNV37.....	235
Reformatting the System Master File Under CA Roscoe.....	236
Suggested Conversion Procedures (CA Roscoe and TSO)	237
Suggested Conversion Procedures (VM/ESA and z/VM).....	238
CCFCNV37 Error and Informational Messages	239
Appendix B: LIB/CCF System Master File Conversion	247
Index	249

Chapter 1: Overview

This guide describes how to acquire, install, and implement CA Librarian to make it available to the staff who customize and use the product.

Audience

This guide details <lib> installation procedures for general mainframe users. We strongly recommend that you read this entire document before starting an installation.

Readers of this book should have knowledge in the following areas:

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

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 untailed.
- 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 15).
2. Acquire the product using one of the following methods:
 - CA MSM
 - Pax-Enhanced Electronic Software Delivery (ESD)
 - Order a DVD.
3. Install the product based on your acquisition method.
4. Install the CA Common Services using the pax files that contain the CA Common Services you need at your site.

All sites should install all CA Common Services contained in the Required CA Common Service bundle.
5. Apply maintenance, if applicable.
6. Deploy your target libraries.
7. Configure your product.

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](#) (see page 15)

[Software Requirements](#) (see page 15)

[CA Common Services for z/OS and OS/390](#) (see page 17)

[Storage Requirements](#) (see page 20)

[Pre-Installation Considerations](#) (see page 22)

[Concurrent Releases](#) (see page 25)

Hardware Requirements

CA Librarian runs on any IBM System/370, 30xx, 4300, z/900 Series or compatible processor.

DASD Devices

CA Librarian supports the following DASD devices for initializing master files:

- 2311
- 2314
- 3330
- 3340
- 3350
- 3375
- 3380
- 3390
- 3410
- 9345

Software Requirements

This section describes software requirements.

Compatibility with IBM Software

CA Librarian supports the following IBM MVS, z/OS and OS/390, and ISPF releases:

- MVS/ESA SP3.1.0 or above
- OS/390 and z/OS SP1.3.0 or above
- z/OS SP1.1.0 or above
- ISPF/PDF 2.2 or above (for ELIPS)
- ISPF 2.2 or above (for LIB/CCF-ISPF and the
- LIB/CCF-CA Roscoe batch login program (\$CCFB109))

Compatibility with Compilers

The CA Librarian subsystem now supports IBM's VisualAge PLI for z/OS and OS/390 and C/C++ for z/OS and OS/390.

Compatibility with CA Software

CA Librarian supports the following CA software products:

- CA Culprit r14.1 or above
- CA Datadictionary r2.4 or above
- CA Earl r6.0 or above
- CA Roscoe IE r6.0 or above (VSAM master files are not supported until r6.0 of CA Roscoe; wide record master files require CA Roscoe 6.0)
- CA ACF2 r5.2 genlevel 9010 or above
- CA Top Secret r4.2 genlevel 9006 or above
- CA 7 Workload Automation r3.0 or above
- CA Netman r4.8 or above
- CA Scheduler Job Management r7.1 or above

CA Common Services for z/OS and OS/390 Components

The following are CA Common Services components:

- CAIRIM
- CAISSF
- CA-C Runtime

Optional Components

CA Librarian contains the following optional components. You must decide which ones you want to install.

- CA Roscoe interface
- ISPF interface (ELIPS)
- LIB/AM (CA Librarian Access Method)
- LIB/CCF—CA Roscoe (Change Control Facility)
- LIB/CCF—ISPF (Change Control Facility)
- LIB/DD (CA Datadictionary interface)
- LIB/TSO (TSO command processor interface)

CA Common Services for z/OS and OS/390

This section presents an overview of the CA Common Services for z/OS and OS/390 that CA Librarian uses. See your CA Common Services documentation more information. If there are other CA products installed at your site, some of these Services might already be installed. The following CA Common Services for z/OS and OS/390 are required to install and use CA Librarian:

- CAIRIM
- CAISSF
- CA C Runtime

The following CA Common Services for z/OS and OS/390 are *not* required to install or use CA Librarian:

- CA Earl
- CA SRAM

CAIRIM

CAIRIM, the CAI Resource Initialization Manager, is the common driver for a collection of dynamic initialization routines that eliminate the need for user SVCs, SMF exits, subsystems, and other installation requirements commonly encountered when installing systems software.

These routines are grouped under the CA dynamic service code S910. Some of CAIRIM's features are:

- Obtaining SMF data
- Verification of proper software installation
- Installation of z/OS and OS/390 interfaces
- Automatic startup of CA and other vendor products
- Proper timing and order of initialization.

CA Librarian uses CAIRIM to install the CA Librarian subsystem and SVC.

CAISSF

CAISSF, the CAI Standard Security Facility, allows CA software to offer standardized security interfaces regardless of the underlying access control software. CAISSF offers user authentication and resource access validation facilities. It can interface with CA security products (such as CA ACF2 or CA Top Secret) or compatible non-CA security products. CAISSF is a subservice contained in the CA service code S910 (CAIRIM). For CA security products, some of CAISSF's features include:

- A single security mechanism
- Isolation of CA enterprise solutions from CA or vendor mechanisms.

For non-CA security products, some of CAISSF's features include:

- Resource class translation
- Access level translation
- Selective logging of requests
- Request type control
- Message support for failed access.

CA Librarian uses CAISSF to provide security for CA Librarian libraries and members.

CA-C Runtime

CA-C Runtime is a runtime facility with re-entrancy capabilities. Its modular architecture insulates C Runtime programs from system and release dependencies. There is little, if any, system-dependent code linked with the user program. This allows for smaller user programs and easier maintenance. CA-C Runtime uses a memory manager to handle dynamic allocation requests for small pieces of storage. This enables fewer calls to be made on the operating system, resulting in faster allocation and de-allocation. Specifications for the use of CA-C Runtime are presented in solution-specific documentation as is necessary.

CA Earl Reporting Service

The CA Earl (Easy Access Report Language) Reporting component is a user-friendly report definition facility with the power of a comprehensive programming system. CA Earl lets you modify and print the contents and layout of a predefined CA product report using English-like statements. The routines that provide this service are grouped under the CA service code XE60. Some of the CA Earl Reporting Service's features are:

- Page, user, and field headings
- Automatic subtotalling and totaling capabilities
- Automatic data editing
- Full arithmetic computational facilities
- High-level capabilities
- Enhanced printed output control.

The CA Librarian Change Control Facility (LIB/CCF) optionally uses CA Earl to generate LIB/CCF reports.

CA SRAM Service

The CA SRAM (Sort Reentrant Access Method) Service is a complete replacement for conventional methods of invoking a sort system from high-level languages. CA SRAM allows the activation of several sorts concurrently, thereby simplifying the data and logic flow. The user program can manipulate the incoming data to the sort in a high-level language without the need for special exit routines.

The service routines that accomplish this are grouped under the Computer Associates service code SR66. Some of CA SRAM's features are:

- All loaded modules are coded to be completely reentrant
- Sorts in ascending or descending sequence
- Accepts fixed and variable length records

- Allows key definitions to spread out over the record
- Low overhead
- Operating system independence.

The CA Librarian Change Control Facility (LIB/CCF) optionally uses CA SRAM with CA Earl.

Storage Requirements

The following tables estimate disk space required for CA Librarian data sets. A default block size that fits on most DASD storage devices was used.

Target Libraries

The following table estimates disk space for the target libraries required to install CA Librarian. These estimates include common components, therefore, less space can be required if some of these components are already installed.

Library Name	Description	Blk Size	LRECL	Space (Blks)	Dir Blks
CAI.CALJLINK	Load library	6144	N/A	1000	41
CAI.CALJPARM	Procedure library	3120	80	3	5
CAI.CALJSAMP	Source library	3120	80	725	5
CAI.CALJMAC	Macro library	3120	80	89	5
CAI.CALJRPf	LIB/CCF CA Roscoe RPFs	3120	80	89	25
CAI.CALJSAMP	User contributed routines	3120	80	725	10
CAI.CALJMENU	LIB/CCF ISPF message library	3120	80	28	5
CAI.CALJSENU	LIB/CCF ISPF skeleton library	3120	80	40	10
CAI.CALJPENU	LIB/CCF ISPF panel library	3120	80	760	35
CAI.CALJTENU	LIB/CCF ISPF table library	3120	80	1	1
CAI.CALUMENU	ELIPS message library	3120	80	29	5
CAI.CALUPENU	ELIPS panel library	3120	80	290	20
CAI.CALUSENU	ELIPS skeleton library	3120	80	20	5
CAI.CALUMJPN	ELIPS Panel Library (JPN)	3120	80	290	205
CAI.CALUTENU	ELIPS table library	3120	80	1	1

Library Name	Description	Blk Size	LRECL	Space (Blks)	Dir Blks
CAI.CALUHENU	LIB/TSO HELP COMMANDS	3120	80	35	5
CAI.CALUPJPN	ELIPS Panel Library (JPN)	3120	80	290	20
CAI.CALJJCL	Sample JCL streams	3120	80	310	35
CAI.CALUEXEC	ELIPS REXX/CLIST library	3120	80	3	5
CAI.CALJXML	MSM 3.0 Deployment	32760	512	16	2

* CAI.CALJLINK should be allocated with full-track blocking performance.

Distribution Libraries

The following table estimates disk space for the distribution libraries needed to install CA Librarian.

Library Name	Description	Blk Size	LRECL	Space (Blks)	Dir Blks
CAI.AALJLINK	CA Librarian load	6144	N/A	50	100
CAI.AALJPARM	CA Librarian procedure library	3120	80	3	
CAI.AALJRPF	CA Librarian LIB/CCF Roscoe RPFs	3120	80	20	25
CAI.AALJMENU	CA Librarian CCF messages	3120	80	30	5
CAI.AALJSENU	CA Librarian CCF skeletons	3120	80	10	10
CAI.AALJMAC	CA Librarian macro library	3120	89	5	
CAI.AAJPENU	CA Librarian CCF panels	3120	80	20	5
CAI.AALUMENU	CA Librarian Elips messages	3120	80	30	5
CAI.AALUSENU	CA Librarian Elips skeleton library	3120	80	20	5
CAI.AALUTENU	CA Librarian Elips table library	3120	80	15	1
CAI.AALUPENU	CA Librarian Elips panel library	3120	80	10	15
CAI.AALUEXEC	CA Librarian REXX/CLIST library	3120	80	3	5
CAI.AALUPJPN	CA Librarian Elips panel library (Japan)	3120	80	10	10
CAI.AALUMJPN	CA Librarian Elips message Library (Japan)	3120	80	5	10
CAI.AALJJCL	CA Librarian Sample JCL streams	3120	80	10	15

Library Name	Description	Blk Size	LRECL	Space (Blks)	Dir Blks
CAI.AALJXML	CA Librarian XML library	32760	512	16	16

Product Libraries

The following table estimates disk space for the various data sets allocated during the CA Librarian installation.

Library Name	Description	Blk Size	LRECL	Space (Blks)	Dir Blks
LIBR.LIBCCF.PRODLOAD	LIB/CCF production load	6144	N/A	100	50
LIBR.LIBCCF.BKUPLOAD	LIB/CCF backup load	6144	N/A	100	50
LIBR.LIBCCF.POBJECT	LIB/CCF production object	1120	80	100	50
LIBR.LIBCCF.TESTMAST	LIB/CCF test master	2004	2004	100	N/A
LIBR.LIBCCF.PRODMAST	LIB/CCF production master	2004	2004	100	N/A
LIBR.LIBCCF.HISTMAST	LIB/CCF history master	2004	2004	100	N/A
LIBR.LIBCCF.SYSMAST	LIB/CCF system master	2004	2004	100	N/A
CAI.LIBR.TLICD	LIB/TSO TLICD file	750	750	50	3
CAI.LIBR.VSAM	CA Librarian control file (VSAM)	1024	56	250	N/A

Pre-Installation Considerations

The following presents important information you should note and precautionary measures we recommend:

- When upgrading from a previous release of CA Librarian, take backups of those libraries where you are installing CA Librarian *before* beginning the installation.
- Before executing any installation jobs, review the supplied member and modify the JCL to include site-specific information and to meet your site's JCL standards.
- All of the JCL supplied with CA Librarian allocates library space in blocks.
- The CA Librarian installation tape is in SMP/E "relfile" format, with the files created by the IBM IEBCOPY utility. The function modification identifiers (FMIDs) are loaded into relative files (source, macro, and load). CA Librarian consists of eight FMIDs, seven for CA Librarian and one for CA Profile.

Each FMID has its own set of relative files, which are listed following:

- CALJ440—5 (macro, source, load, JCL, and XML)
- CALJ441—3 (macro and 2 load)
- CALJ442—2 (macro and load)
- CALJ441—2 (macro and load)
- CALR440—1 (load)
- CALU440—2 (macro and load)
- CALU441—2 (macro, source, and load)
- CALU442—3(macro, source, and load)
- CALU443—1 (Japanese macro and load)
- Install CA Librarian in its own SMP/E target and distribution zones, for example, CAIT0 and CAID0.
- Accept CA Librarian so that you can run an SMP/E RESTORE for product maintenance.
- SMP/E USERMODs are used for customizing such CA Librarian facilities as the LIBRID defaults module and the LIB/CCF DB2 interface.

Important! Never accept these USERMODs into your SMP/E system.

- CA Librarian takes advantage of various facilities that CA Common Services for z/OS and OS/390 provide. Specifically, you must install the S910 component, comprised of CAIRIM, CA-C Runtime, and CAISSF, before installing CA Librarian. CAIRIM, the Resource Initialization Manager, eliminates the need to IPL when installing the CA Librarian Access Method (LIB/AM). CAISSF, the Standard Security Interface, lets CA Librarian offer a standardized security interface. See the *CA Common Services for z/OS and OS/390 Getting Started* for installation procedures of the S910 component.
- CA Librarian uses SVC168 to implement the external security interface.
- In addition to the CSA requirements of CAIRIM, the CA Librarian Subsystem (LAM) acquires ECSA storage. The amount of ECSA storage is computed using the following formula: ECSA bytes equals ((MAXUSER plus 1) times 4) + 876 + ((number of wide record master files - 10) * 98)

The MAXUSER parameter is defined in the IEASYSxx member of SYS1.PARMLIB. See the *CA Common Services for z/OS and OS/390 Getting Started* for CSA requirements for CAIRIM.

You can reduce the CSA storage requirements of CAIRIM by placing member LAMMVS in the LPA.

GRS Considerations

If your site uses GRS, include a CONVERSION RNL for each master file, as follows:

```
RNLDEF RNL(CON) TYPE(GENERIC) QNAME(ADRPRDCT)
RNAME(master.file.dsn)
```

A GENERIC type RNAME of the data set name is defined to cover all of the resource names listed in the following table.

Alternatively, you can define multiple master files under one RNLDEF by specifying the high-level data set name qualifiers, as follows:

```
RNLDEF RNL(CON) TYPE(GENERIC) QNAME(ADRPRDCT)
RNAME(master.file.qualifier)
```

A CONVERSION RNL is *optional* but recommended for BDAM or single-volume VSAM master files. A CONVERSION RNL is *required* for multi-volume VSAM master files.

For update processing (both batch and online), CA Librarian employs resource serialization to minimize the duration of enqueues and reserves issued on the master file.

The resources used are listed below in the order in which they are always claimed:

Resource	QNAME	RNAME
Master file	ADRPRDCT	Data set name
Block zero	ADRPRDCT	Data set name plus .0
Module	ADRPRDCT	Data set name plus member name
Index	ADRPRDCT	Data set name plus .2
bit map	ADRPRDCT	Data set name plus .4

Important! In the VM/ESA and z/VM environment where LIB/CMS is installed, including ADRPRDCT in the GRS conversion RNL corrupts the master file. VM/ESA and z/VM users of CA Librarian share master files with z/OS and OS/390 users through the use of real and virtual RESERVE/RELEASE. If GRS intercepts and converts the CA Librarian-issued RESERVE commands, VM/ESA and z/VM users might not recognize simultaneous accesses from the z/OS and OS/390 system.

GRS Considerations for Wide Record Master Files

The CA Librarian VSAM control file is reserved by the LAMSERV regions using the QNAME, LIBRLAM. This reserve is eligible to be converted using a CONVERSION RNL as follows:

```
RNLDEF RNL(CON) TYPE(SPECIFIC) QNAME(LIBRLAM)
RNAME(VSAM.CNTL.DSN)
```

The wide record master files use the standard ISPF enqueue method for PDS files; QNAME, SPFEDIT, RNAME dsname. A sample CONVERSION RNL follows:

```
RNLDEF RNL(CON) TYPE(GENERIC) QNAME(SPFEDIT)
RNAME(dsn.qualifier)
```

Concurrent Releases

You can install this release of CA Librarian and continue to use an older release for your production 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.
- 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

Use the procedures in this section to manage your product using CA MSM. Managing includes acquiring, installing, maintaining, and deploying products, setting system registries, and managing your CSIs. These procedures assume that you have already installed and configured CA MSM.

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.

When you have completed the procedures in this section, go to [Configuring Your Product](#).

This section contains the following topics:

[CA MSM Documentation](#) (see page 27)

[Getting Started Using CA MSM](#) (see page 28)

[Acquiring Products](#) (see page 38)

[Installing Products](#) (see page 43)

[Maintaining Products](#) (see page 50)

[Setting System Registry](#) (see page 64)

[Deploying Products](#) (see page 89)

Note: The following procedures are for CA MSM r3. If you are using CA MSM r2, see the *CA Mainframe Software Manager r2 Product Guide*.

CA MSM Documentation

This chapter includes the required procedures to install your product using CA MSM. If you want to learn more about the full functionality of CA MSM, see the CA Mainframe Software Manager bookshelf on the CA MSM product page on <https://support.ca.com/>.

Note: To ensure you have the latest version of these procedures, go to the CA Mainframe Software Manager product page on [the CA Support Online website](#), click the Bookshelves link, and select the bookshelf that corresponds to the version of CA MSM that you are using.

Getting Started Using CA MSM

This section includes information about how to get started using CA MSM.

How to Use CA MSM: Scenarios

In the scenarios that follow, imagine that your organization recently deployed 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 products.

- The first scenario shows how you can use CA MSM to acquire the product.
- The second scenario shows how you can use CA MSM to install the product.
- The third scenario shows how you can use CA MSM to maintain products already installed in your environment.
- The fourth scenario shows how you can use CA MSM to deploy the product to your target systems.

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 37), 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](#) (see page 38). 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](#) (see page 39).

After you find your product in the catalog, you can [download the product installation packages](#) (see page 39).

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 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](#) (see page 87) for those systems.
 - c. Set up the target systems ([Non-Sysplex](#) (see page 65), [Sysplex or Monoplex](#) (see page 66), [Shared DASD Cluster](#) (see page 67), and [Staging](#) (see page 68)), and validate them.
 - d. [Add FTP](#) (see page 77) information, including data destination information, to each system registry entry.
2. Set up [methodologies](#) (see page 115).

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](#) (see page 132), [products](#) (see page 106), [custom data sets](#) (see page 108), and [methodologies](#) (see page 115), 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.

System Registration

You must add and then validate each system in the enterprise that you are deploying to the CA MSM system registry. You can only send a deployment to a validated system. This process is called registering your system and applies to each system in your enterprise. For example, if you have five systems at your enterprise, you must perform this procedure five times.

Note: After a system is registered, you do not need to register it again, but you can update the data in the different registration fields and re-register your system.

The system registration process contains the following high-level steps:

1. Set up your remote credentials.

This is where you provide a user ID and password to the remote target system where the deployment will copy the installed software to. Remote credentials are validated during the deployment process. You will need the following information:

- Remote user ID
- Remote system name
- Password
- Authenticated authorization before creating a remote credential.

Your system administrator can help you with setting up your remote credentials.

2. Set up your system registry.

The CA MSM system registry is a CA MSM database, where CA MSM records information about your systems that you want to participate in the deployment process. There is one entry for each system that you register. Each entry consists of three categories of information: general, FTP locations, and data destinations.

Each system registry entry is one of four different system types. Two reflect real systems, and two are CA MSM-defined constructs used to facilitate the deployment process. The two real system types are Non-Sysplex System and Sysplex Systems. The two CA MSM-defined system types are Shared DASD Clusters and Staging Systems.

Non-Sysplex Systems

Specifies a stand-alone z/OS system that is not part of a sysplex system.

Note: During system validation, if it is found to be part of a sysplex, you will be notified and then given the opportunity to have that system automatically be added to the sysplex that it is a member of. This may cause the creation of a new sysplex system. If you do not select the automatic movement to the proper sysplex, this system will be validated and cannot be deployed.

Sysplex or Monoplex Systems

Specifies a *Sysplex* (SYStem comPLEX), which is the IBM mainframe system complex that is a single logic system running on one or more physical systems. Each of the physical systems that make up a Sysplex is often referred to as a *member* system.

A *Monoplex system* is a sysplex system with only one system assigned.

Note: Monoplexes are stored in the Sysplex registry tree but with the name of the Monoplex System and not the Monoplex Sysplex name. For example, a system XX16 defined as a Monoplex, with a Sysplex name of LOCAL. It will be depicted in the System Registry as a Sysplex with the name of XX16. This sysplex will contain one system: XX16.

This system type can help you if you have Monoplexes with the same Sysplex name (for example: LOCAL). Instead of showing multiple LOCAL Sysplex entries that would need to be expanded to select the correct Monoplex system, the CA MSM System Registry shows the actual Monoplex System name at the top-level Sysplex Name.

Shared DASD Clusters

Specifies a *Shared DASD Clusters* system, which defines a set of systems that share DASD and it can be composed of Sysplex systems, Non-Sysplex systems, or both. A Staging system cannot be part of a Shared DASD Cluster.

Staging Systems

Specifies a *Staging system*, which is an SDS term that defines a virtual system. A Staging system deploys the deployment to the computer where the CA MSM driving system is located. To use a Staging system, the CA MSM driving system must be registered in the CA MSM System Registry.

Note: A Staging system can be useful in testing your deployments and learning deployment in general. It can also be used if your target systems are outside a firewall. For example, deploy to a Staging system and then manually copy the deployment to tape.

3. Define the FTP location information for every system.

FTP locations are used to retrieve the results of the deployment on the target system (regardless if the deployment was transmitted through FTP or using Shared DASD). They are also used if you are moving your deployments through FTP.

To define the FTP location, provide the following:

URI

Specifies the host system name.

Port Number

Specifies the port number.

Default: 21.

Directory Path

Specifies the landing directory, which is the location that the data is temporarily placed in during a deployment.

4. Define a data destination for every system.

The data destination is how you tell CA MSM which technique to use to transport the deployment data to the remote system. The following choices are available:

FTP

When FTP is selected as the transport mechanism, the deployment data is shipped to the target system through FTP. It is temporarily placed on the target system at the landing directory specified in the FTP Location information section of the System Registry.

Shared DASD

When you specify shared DASD, CA MSM uses a virtual transport technique. That is, it does not actually copy the data from one system to the other. Because the two systems share DASD, there is no need to do this. All of the deployment data is kept in USS file systems managed by CA MSM.

Even though the DASD is shared, the remote system may not be able to find the deployment data in the USS file system. Therefore, CA MSM temporarily unmounts the file system from the CA MSM driving system and mounts it in read-only mode on the remote system.

For CA MSM to determine where to mount the file system on the remote system, you must specify a mount point location in the data destination. In addition, you can provide allocation information for the creation of the deployment file system, so that when the file system is created on the CA MSM driving system, it will be on the DASD that is shared.

Data destinations are assigned to Non-Sysplex and Sysplex systems, and Shared DASD Clusters. Data destinations are named objects, and may be assigned to multiple entities in the system registry and have their own independent maintenance dialogs.

The remote allocation information is used by the deployment process on the remote system, letting you control where the deployed software is placed. By specifying the GIMUNZIP volser, CA MSM adds a volume= parameter to the GIMUNZIP instructions on the remote system. The list of zFS VOLSERS is needed only if both of the following occur:

- The software you are deploying contains USS parts.
- You select a container copy option during the deployment process.

Note: After you have created your systems, you will need to validate them.

5. Register each system by validating that it exists.

Note: You should validate your Non-Sysplex Systems first, and then your Sysplex or Shared Cluster Systems.

You start the validation process when you select the Validate button in the Actions drop-down list for a Sysplex System, Non-Sysplex System, and Shared DASD Cluster on that system's System Registry Page. This starts a background process using the CCI validation services to validate this system.

Note: Staging Systems are not validated. However, you will need to create and validate a system registry entry for the CA MSM driving system if you are going to utilize Staging systems.

Note: If the validation is in error, review the message log, update your system registry-entered information, and validate again.

You are now ready to deploy your products.

Deploying Products

After you install software using CA MSM, you still need to deploy it. You can use the deployment wizard to guide you through the deployment process. In the wizard, you can deploy one product at a time. You can also save a deployment at any step in the wizard, and then manually edit and deploy later.

Note: You must have at least one product, one system, and one methodology defined and selected to deploy.

You must complete the following steps in the Deployment wizard before you deploy:

Deployment Name and Description

Enter the deployment name and description using the wizard. The name must be a meaningful deployment name.

Note: Each deployment name must be unique. Deployment names are not case-sensitive. For example DEPL1 and depl1 are the same deployment name.

We recommend that you enter an accurate and brief description of this deployment.

CSI Selection

Select a CSI. A CSI is created for the installed product as part of the installation process.

Product Selection

Displays the products that are installed in the CSI you selected.

Custom Data Set

Custom data sets let you add other data sets along with the deployment. They contain either a z/OS data set or USS paths.

- For a z/OS data set, you need to provide a data set name that is the actual existing z/OS data set and a mask that names the data set on the target system. This mask may be set up using [symbolic qualifiers](#) (see page 119) and must be available to CA MSM. During the deployment process, the custom data set is accessed and copied to the target system the same way a target library is accessed and copied.
- For USS paths, you need to provide a local path, a remote path which may be set up using [symbolic qualifiers](#) (see page 119) and type of copy. Type of copy can be either a container copy or a file-by-file copy.

You can [add a custom data set](#) (see page 109).

Methodology

Methodology is the process by which data sets are named on the target system. A methodology provides the *how* of a deployment, that is, what you want to call your data sets. It is the named objects with a description that are assigned to an individual deployment.

To [create a methodology](#) (see page 116), specify the following:

Data set name mask

Lets you choose symbolic variables that get resolved during deployment.

Disposition of the target data sets

If you select Create, ensure that the target data sets do not exist, otherwise, the deployment fails.

If you select *Create or Replace* and the target data sets do not exist, they will be created. If the target data sets exist, *Create or Replace* indicates that data in the existing data set, file, or directory will be replaced, as follows:

Partitioned data set

Create or Replace indicates that existing members in a partitioned data set will be replaced by members with the same name from the source file. Any currently existing member that is not in the source file will remain in the PDS. Any member from the source that does not already exist in the target PDS will be added to the target PDS.

The amount of free space in the PDS should be sufficient to hold the additional content, because no automatic compress is performed.

Directory in a UNIX file system

Create or Replace indicates files in a directory will be replaced by files with same name from the source. Any currently existing directory in a UNIX file system that is not in the source will remain in the UNIX file system.

Sequential data set or a file in the UNIX file system

Create or Replace indicates the existing data set or file and its attributes will be replaced with the data from the source file.

For a VSAM data set (cluster)

Create or Replace indicates that an existing VSAM cluster should be populated with the data from the source file. The existing VSAM cluster must be of the same type as the source cluster (ESDS, KSDS, LDS, or RRDS). In addition, the existing VSAM cluster must have characteristics that are compatible with the source cluster (such as, record size, key size, and key offset). Replace does not verify the compatibility of these characteristics!

Note: You can replace the contents of an existing cluster using the IDCAMS ALTER command to alter the cluster to a reusable state. You must do this before the data from the VSAM source is copied into the cluster using an IDCAMS REPRO command. The REPRO command will use both the REPLACE and REUSE operands, and after you use it, the cluster is altered back to a non-reusable state if that was its state to begin with.

System Selection

Select the system for this deployment.

Preview

Preview identifies the deployment by name and briefly states the products, systems, means of transport, target libraries including source, target and resolution, as well as SMP/E environment and snapshot information. It shows the translated symbolic qualifiers.

Use this option to review your deployment before deploying.

Deploy

Deploy combines the snapshot, transmit, and deploy action into one action. Deploy enables you to copy your CA MSM-installed software onto systems across your enterprise. For example, you can send one or many products to one or many systems. Deploy can send the software by copying it to a shared DASD or through FTP.

Summary

After your products have successfully deployed, you can review your deployment summary and then confirm your deployment. You can also delete a completed deployment.

Confirm

Confirms that the deployment is complete. A deployment is not completed until it is confirmed. After it is confirmed, the deployment moves to the Confirmed deployment list.

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](#) (see page 51) 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](#) (see page 52).
3. [Apply the maintenance](#) (see page 55).

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.

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.

Acquiring Products

This section includes information about how to use CA MSM to acquire products.

Update Software Catalog

Initially, the CA MSM software catalog is empty. To see available products at your site, update the catalog. As new releases become available, update the catalog again to refresh the information. The available products are updated using the site ID associated with your credentials on [the CA Support Online website](#).

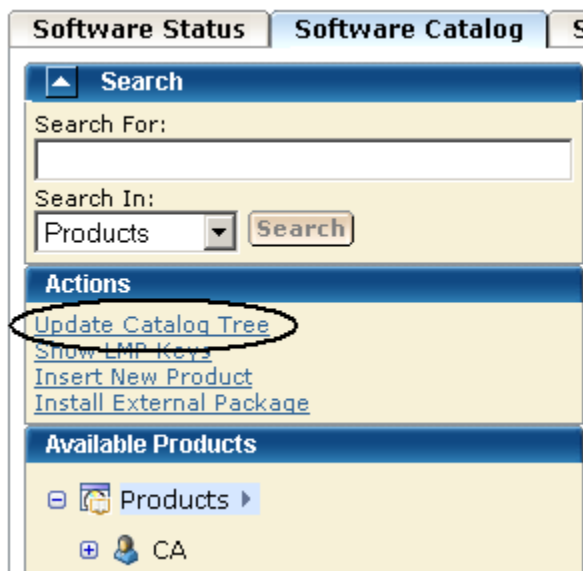
If you update the catalog tree and some changes are missing, check your user settings on [the CA Support Online website](#).

Follow these steps:

1. Click the Software Catalog tab.

Note: The information on the Software Status tab for HIPERs and new maintenance is based on the current information in your software catalog. We recommend that you update the catalog on a daily or weekly basis to keep it current.

- Click the Update Catalog Tree link in the Actions section at the left.



You are prompted to confirm the update.

- Click OK.

A dialog that shows the progress of the task opens. When the task completes, you can click Show Results on the Progress tab to close this dialog. The task output browser opens and you can view the action details. Click Close to close the task output browser.

Note: While a task is in progress, you can perform other work. You can click Hide to exit the dialog and view the task status later on the Tasks tab.

Download Product Installation Package

You can download product packages through the Software Catalog tab. The Update Catalog action retrieves information about the products for your site.

Follow these steps:

- Verify that your CA MSM login user name is associated with a registered user of [the CA Support Online website](#) on the Software Acquisition Settings page.
CA MSM uses the credentials to access [the CA Support Online website](#).

2. Locate and select the product you want to download by using the Search For field or expanding the Available Products tree at the left.

The product releases are listed.

Note: If the product does not appear on the product tree, click the Update Catalog Tree link in the Actions section at the left. The available products are updated using the site ID associated with your credentials for [the CA Support Online website](#). If you update the catalog tree and some changes are missing, check your user settings on [the CA Support Online website](#).

3. Click Update Catalog Release in the Actions column in the right pane for the product release you want to download.

A dialog that shows the progress of the task opens. When the task completes, you can click Show Results on the Progress tab to close this dialog. The task output browser opens and you can view the action details. Click Close to close the task output browser.

Note: While a task is in progress, you can perform other work. You can click Hide to exit the dialog and view the task status later on the Tasks tab.

The product packages are downloaded.

Note: You can expand the tree in the right panel by selecting the Products link from the catalog tree. Then, click the vendor link in the right panel. If you select and download multiple products using this method and one of the products cannot be downloaded, the remaining products are not downloaded either. Remove the checks from the products that were processed and repeat the update catalog request.

Migrate Installation Packages Downloaded External to CA MSM

If you have acquired product pax files by means other than through CA MSM, you can add information about these product installation packages to CA MSM from the Software Catalog tab.

Migrating these packages to CA MSM provides a complete view of all your product releases. After a package is migrated, you can use CA MSM to [install the product](#) (see page 43).

Follow these steps:

1. Click the Software Catalog tab, and click Insert New Product.

Note: A product not acquired from [the CA Support Online website](#) does not appear in Software Catalog until you perform this step.

An entry is added for the product.

2. Select the product gen level (for example, SP0 or 0110) for which the package applies.

The packages for the gen level are listed.

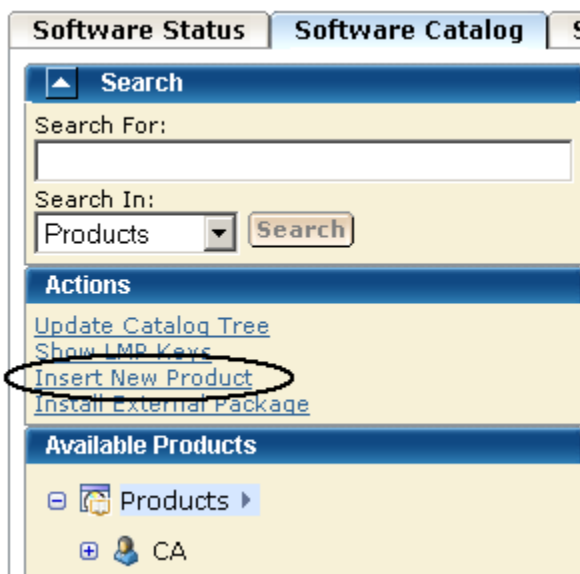
3. Click the Add External Package button.
You are prompted to enter a path for the package.
 4. Specify the USS path to the package you want to migrate, and click OK.
Information about the package is saved in the CA MSM database.
- Note:** To see the added package, refresh the page.

Add a Product

Sometimes, a product is not currently available from [the CA Support Online website](#). For example, if you are testing a beta version of a product, the version is delivered to you by other means. You can add these types of product packages to CA MSM using the Insert New Product action.

Follow these steps:

1. Click the Software Catalog tab, and click the Insert New Product link in the Actions section at the left.



- You are prompted to supply information about the product.
2. Specify the name, release, and gen level of the product, and click OK.
The product is added to the software catalog.
 3. Click the gen level of the product you want to install on the product tree at the left.
The Base Install Packages section appears at the right.
 4. Click the Add External Package button.
You are prompted to identify the package.

5. Specify the USS path to the package you want to add, and click OK.

Note: To add several packages from the same location, use [masking](#) (see page 42).

Information about the package is saved in the CA MSM database.

Note: To see the added package, refresh the page.

Masking for External Packages

Masking lets you add more than one [package](#) (see page 41) (or set of [maintenance files](#) (see page 53)) from the same location using a pattern (mask). You can use masking for components, maintenance in USS, and maintenance in data sets. You can use masking for files only, not for directories.

Masking: Use the asterisk symbol (*).

- For PDS and PDSE, you can mask members using asterisks.

- For sequential data sets, use the following characters:

?

Match on a single character.

*

Match on any number of characters within a data set name qualifier or any number of characters within a member name or file system name.

**

Match on any number of characters including any number of qualifiers within a data set name.

You can use as many asterisks as you need in one mask. After you enter the mask, a list of files corresponding to the mask pattern appears.

Note: By default, all files in the list are selected. Verify what files you want to add.

Example 1

The following example displays all PDF files that are located in the `/a/update/packages` directory:

```
/a/update/packages/*.pdf
```

Example 2

The following example displays all files located in the `/a/update/packages` directory whose names contain `p0`:

```
/a/update/packages/*p0*
```

Example 3

The following example displays all sequential data sets whose name starts with *PUBLIC.DATA.PTFS.:*

```
PUBLIC.DATA.PTFS.**
```

Example 4

The following example displays all members in the PDS/PDSE data set *PUBLIC.DATA.PTFLIB* whose name starts with *RO:*

```
PUBLIC.DATA.PTFLIB(RO*)
```

Installing Products

This section includes information about how to use CA MSM to install products.

Install a Product

You can install a downloaded product through the Software Catalog, Base Install Packages section. The process starts a wizard that guides you through the installation. At the end of the wizard, a task dynamically invokes the SMP/E and other utilities required to install the product.

Note: If your site uses only one file system (for example, only zFS or only HFS), you can configure CA MSM to use this file system for all installed products regardless of the file system that the product metadata specifies. The settings are available on the System Settings, Software Installation page. The file system type that you specify will override the file system type that the product uses.

Any USS file system created and mounted by CA MSM during a product installation is added in CA MSM as a managed product USS file system. CA MSM lets you enable and configure verification policy that should be applied to these file systems when starting CA MSM. For verification results, review CA MSM output.

These settings are available on the System Settings, Mount Point Management page.

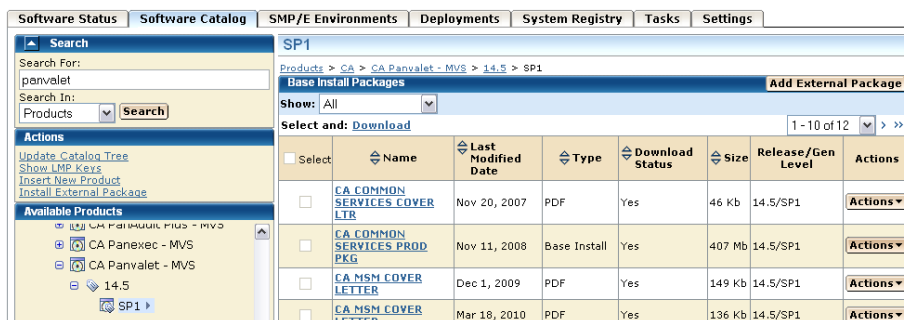
During installation, you select the CSI where the product is to be installed, and specify its zones. You can either specify target and distribution zones to be in the existing CSI data sets, or create new data sets for each zone.

Note: While you are working with a particular SMP/E environment, the SMP/E environment is locked and other CA MSM users cannot perform any action against it. When the task finishes, or when you log out from CA MSM, or when your CA MSM session is inactive for more than 10 minutes, the lock releases.

Follow these steps:

1. Click the Software Catalog tab, and select the product gen level (for example, SP0 or 0110) you want to install on the product tree at the left.

Information about the product appears in the Base Install Packages section at the right, for example:



Note: If a product is acquired external to CA MSM, you can install the product using the Install External Package link. The process starts the wizard.

2. Do one of the following:
 - If the package was acquired using CA MSM, locate the product package that you want to install, click the Actions drop-down list to the right of the package, and select Install.
 - or
 - If the package was acquired external to CA MSM, click the Install External Packages link under the Actions section in the left pane, enter the location of the package, and click OK.

The Introduction tab of the wizard appears.

Note: An information text area can appear at the bottom of the wizard. The area provides information that helps you progress through the wizard. For example, if a field is highlighted (indicating an error), the information text area identifies the error.

3. Review the information about the installation, and click Next.

Note: If the license agreement appears for the product that you are installing, scroll down to review it, and accept it.

You are prompted to select the type of installation.

4. Click the type of installation, and then click Next.

(Optional) If you select Custom Installation, you are prompted to select the features to install. Select the features, and click Next.

A summary of the features to install appears, with any prerequisites.

5. Review the summary to check that any prerequisites are satisfied.

- If no prerequisites exist, click Next.

You are prompted for the CSI to use for this installation.

- If prerequisites exist, and they are all satisfied, click Next.

You are prompted to locate the installed prerequisites. If an installed prerequisite is in more than one CSI or zone, the CSI and Zone drop-down lists let you select the specific instance. After you make the selections, click Next.

You are prompted for the CSI to use for this installation.

- If prerequisites are not satisfied, click Cancel to exit the wizard. Install the prerequisites, and then install this product.

Note: You can click Custom Installation to select only those features that have the required prerequisites. You can click Back to return to previous dialogs.

6. Select an existing CSI, or click the Create a New SMP/E CSI option button, and click Next.

If you select Create a New SMP/E CSI, you are prompted to [specify the CSI parameters](#) (see page 46).

If you select an existing CSI, the wizard guides you through the same steps. Allocation parameters that you specify for work DDDEFs are applied only to new DDDEFs that might be created during the installation. The existing DDDEFs if any remain intact.

Note: Only CSIs for the SMP/E environments in your working set are listed. You can configure your working set from the SMP/E Environments tab.

- If you select a CSI that has incomplete information, the wizard prompts you for extra parameters.
- If you select an SMP/E environment being used in CA MSM by another user, a notification message appears. You are prevented from performing any actions on the SMP/E environment. You can either wait until the notification message disappears and the SMP/E environment becomes available, or click Cancel to select another SMP/E environment.

After you select a CSI or specify a new CSI, you are prompted for the target zone to use.

7. Select an existing zone, or click the Create a New SMP/E Target Zone option button. Click Next.

Note: If you select Create a New SMP/E Target Zone, you perform additional steps similar to the steps for the Create a New SMP/E CSI option. The target zone parameters are pre-populated with the values that are entered for the CSI. You can change them.

If you want the target zone to be created in a new data set, select the Create New CSI Data Set check box and fill in the appropriate fields.

After you select or specify a target zone, you are prompted for the distribution zone to use.

8. Select an existing zone, or click the Create a New SMP/E Distribution Zone option button. Click Next.

Note: If you selected to use an existing target zone, the related distribution zone is automatically selected, and you cannot select other distribution zone. If you selected to create a new target zone, you create a new distribution zone, and you cannot select existing distribution zone.

After a distribution zone is selected or specified, a summary of the installation task appears.

Note: If you select Create a New SMP/E Distribution Zone, you perform additional steps similar to the steps for the Create a New SMP/E CSI option. The distribution zone parameters are prepopulated with the values that are entered for the target zone. You can change them.

- If you want the distribution zone to be created in a new data set, select the Create New CSI Data Set check box and fill in the appropriate fields.
- If you want to use the same data set that you have already specified to be created for the target zone, the data set will be allocated using the parameters you have defined when specifying the target zone.

9. Review the summary, and click Install.

A dialog that shows the progress of the task opens. When the task completes, you can click Show Results on the Progress tab to close this dialog. The task output browser opens and you can view the action details. Click Close to close the task output browser.

Note: While a task is in progress, you can perform other work. You can click Hide to exit the dialog and view the task status later on the Tasks tab.

Create a CSI

You can create a CSI while you are [installing a product](#) (see page 43). During the process, you are asked to specify the following:

- Data set allocation parameters, which you can then customize for each data set
- Parameters for DDDEF allocation

You can specify data set allocation parameters collectively for all SMP/E data sets, target libraries, and distribution libraries that will be allocated during product installation. You can allocate data sets using one of the following methods:

- Allocate data sets using SMS parameters.
- Allocate cataloged data sets using UNIT and optionally VOLSER.
- Allocate uncataloged data sets using UNIT and VOLSER.

If you allocate uncataloged data sets, you must specify a VOLSER. Based on the value that you enter, CA MSM performs the following validations to help ensure integrity of the installation:

- The value of VOLSER must specify a mounted volume.
- You must have ALTER permissions for the data sets with the entered high-level qualifier (HLQ) on the volume defined by VOLSER.
- To test allocation, CA MSM temporarily allocates one of the uncataloged data sets that should be allocated during the installation.
 1. The data set is allocated with one track for both primary and secondary space.
 2. CA MSM verifies that the data set has been allocated on the specified volume.
 3. The data set is deleted.

If the data set allocation fails or the data set cannot be found on the specified volume, you cannot proceed with the product installation wizard.

Follow these steps:

1. Click Create a New SMP/E CSI from the product installation wizard.

You are prompted to define a CSI.

2. Specify the following, and click Next:

Name

Defines the name for the environment represented by the CSI.

Data Set Name Prefix

Defines the prefix for the name of the CSI VSAM data set.

Catalog

Defines the name of the SMP/E CSI catalog.

Cross-Region

Identifies the cross-region sharing option for SMP/E data sets.

Cross-System

Identifies the cross-system sharing option for SMP/E data sets.

High-Level Qualifier

Specifies the high-level qualifier (HLQ) for all SMP/E data sets that will be allocated during installation. The low-level qualifier (LLQ) is implied by the metadata and cannot be changed.

DSN Type

Specifies the DSN type for allocating SMP/E data sets.

SMS Parameters / Data Set Parameters

Specify if this CSI should use SMS or data set parameters, and complete the applicable fields.

Storage Class (SMS Parameters only)

Defines the SMS storage class for SMP/E data sets.

Management Class (SMS Parameters only)

Defines the management class for SMP/E data sets.

Data Class (SMS Parameters only)

Defines the data class for SMP/E data sets.

VOLSER (Data Set Parameters only)

Defines the volume serial number on which to place data sets.

Note: This field is mandatory if you set Catalog to No.

Unit (Data Set Parameters only)

Defines the type of the DASD on which to place data sets.

Catalog (Data Set Parameters only)

Specifies if you want SMP/E data set to be cataloged.

Note: An information text area can appear at the bottom of the wizard. The area provides information that helps you progress through the wizard. For example, if a field is highlighted (indicating an error), the information text area identifies the error.

Work DDDEF allocation parameters and a list of the data sets to be created for the CSI appear.

3. Specify whether to use SMS or Unit parameters for allocating work DDDEFs for the CSI, and complete the appropriate fields.

Note: The settings for allocating work DDDEFs are globally defined on the System Settings, Software Installation tab. You must have the appropriate access rights to be able to modify these settings.

4. Review the data set names. Click the Override link to change the high-level qualifier of the data set name and the allocation parameters, and then click Next.

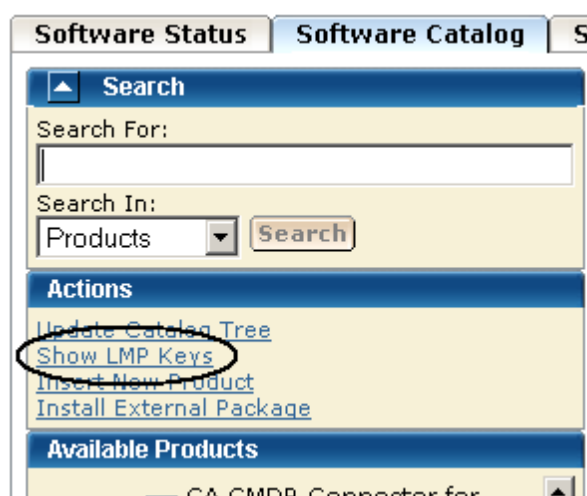
You are prompted to specify any additional parameters. A new CSI is specified.

Download LMP Keys

When you install a CA Technologies product on z/OS systems, you must license the product on each system that uses the product. You do this by entering CA Common Services for z/OS CA License Management Program (LMP) statements. You can download LMP keys through the Software Catalog tab so that the keys are available for you to enter manually. The Show LMP Keys action retrieves the keys for the products to which your site is entitled.

Follow these steps:

1. Click the Software Catalog tab, and click the Show LMP Keys link in the Actions section at the left.



A list of LMP keys retrieved for the indicated site ID appears.

2. Select the site ID for which you want to list the LMP keys from the Site IDs drop-down list.

The list is refreshed for the selected site ID.

If the list is empty or if you want to update the lists, proceed to the next step.

3. Click Update Keys.

You are prompted to confirm the update.

4. Click OK.

The LMP keys are retrieved. On completion of the retrieval process, the LMP keys are listed for the selected site.

Note: You can use the Refresh Site IDs button to refresh the information on the page.

Maintaining Products

This section includes information about how to use CA MSM to download and apply product maintenance packages.

How to Apply Maintenance Packages

Use this process to download and apply product maintenance packages.

1. Identify your download method. This section details the steps to use the following download methods:
 - [Download Product Maintenance Packages](#) (see page 51)
 - [Download Product Maintenance Packages for Old Product Releases and Service Packs](#) (see page 52)
 - [Manage Maintenance Downloaded External to CA MSM](#) (see page 53)

Contact your system administrator, if necessary.

2. Apply the product maintenance package. This section also details the role of USERMODs.

Note: This section also describes how to back out maintenance that has been applied but not yet accepted.

Download Product Maintenance Packages

You can download maintenance packages for installed products through the Software Catalog tab.

Follow these steps:

1. Verify that your CA MSM login user name is associated with a registered user of [the CA Support Online website](#) on the Software Acquisition Settings page.

CA MSM uses the credentials to access [the CA Support Online website](#).

2. Click the name of the product for which you want to download maintenance on the product tree at the left.

Maintenance information about the product appears in the Releases section at the right.

3. Click the Update Catalog Release button for the product release for which you want to download maintenance.

A dialog that shows the progress of the task opens. When the task completes, you can click Show Results on the Progress tab to close this dialog. The task output browser opens and you can view the action details. Click Close to close the task output browser.

Note: While a task is in progress, you can perform other work. You can click Hide to exit the dialog and view the task status later on the Tasks tab.

The maintenance packages are downloaded.

More information:

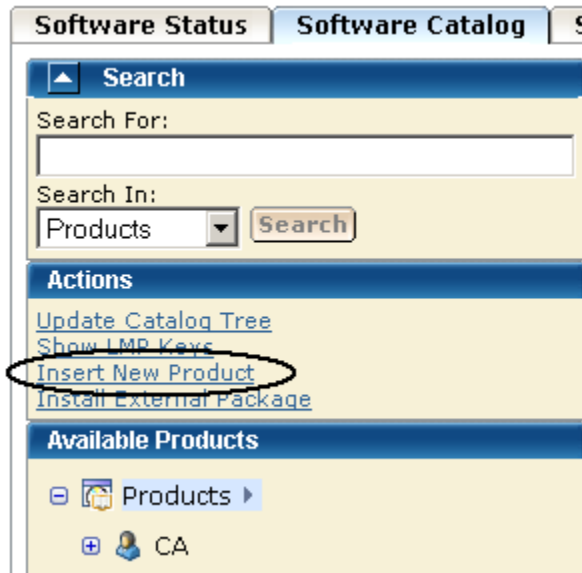
[Download Maintenance Packages for Old Product Releases and Service Packs](#) (see page 52)

Download Maintenance Packages for Old Product Releases and Service Packs

CA MSM does not retrieve information about old product releases and service packs. If you need maintenance from those releases and service packs, you must add them to the software catalog before you can download the maintenance.

Follow these steps:

1. Click the Software Catalog tab, and click the Insert New Product link in the Actions section at the left.



You are prompted to supply information about the product release.

2. Specify the name, release, and gen level of the product, and click OK.

Note: Use the same product name that appears on the product tree, and use the release and gen level values as they appear for Published Solutions on [the CA Support Online website](#).

The product release is added to the software catalog.

3. From the product tree at the left, click the name of the product for which you want to download maintenance.

Maintenance information about the product appears in the Releases section at the right.

4. Click Update Catalog Release for the added product release.

Maintenance packages are downloaded. A dialog that shows the progress of the task opens. When the task completes, you can click Show Results on the Progress tab to close this dialog. The task output browser opens and you can view the action details. Click Close to close the task output browser.

Note: While a task is in progress, you can perform other work. You can click Hide to exit the dialog and view the task status later on the Tasks tab.

Manage Maintenance Downloaded External to CA MSM

Some maintenance packages, such as unpublished maintenance, APARs, and USERMODs, may be acquired externally to CA MSM. You can add information about these maintenance packages to CA MSM from the Software Catalog tab. The process starts a wizard that guides you through the migration.

Adding these maintenance packages to CA MSM provides you with a complete view of all the maintenance for a product release. After a package is migrated, you can use CA MSM to [apply the maintenance](#) (see page 55).

The maintenance package must be located in a z/OS data set or a USS directory. If you use a z/OS data set, it must have an LRECL of 80. If you place the maintenance in a USS directory, copy it in binary mode.

The maintenance is placed as either a single package or an aggregated package that is a single file comprised of multiple maintenance packages. An *aggregated package* is a file that comprises several single maintenance packages (nested packages). When you add an aggregated package, CA MSM inserts all nested packages that the aggregated package includes and the aggregated package itself. In the list of maintenance packages, the aggregated package is identified by the CUMULATIVE type.

When you insert an aggregated package, CA MSM assigns a fix number to it. The fix number is unique and contains eight characters, starting with AM (for Aggregated Maintenance) followed by a unique 6-digit number whose value increases by 1 with each added aggregated package.

Note: If the aggregated maintenance package has the same fix number as one of its nested packages, only the nested packages are added. The aggregated package itself will not be available in the list of maintenance packages.

Follow these steps:

1. Click the Software Catalog tab, and select the product release for which the maintenance applies.

The maintenance packages for the release are listed.

2. Click the Add External Maintenance button.

You are prompted to specify the package type and location.

3. Specify the package type and either the data set name or the USS path.

Note: To add several packages from the same location, use [masking](#) (see page 42).

4. Click OK.

The maintenance package with the related information is saved in the CA MSM database.

Note: To see the added package, refresh the page.

More information:

[Manage Maintenance](#) (see page 55)

View Aggregated Package Details

You can view which nested packages are included in the aggregated package. The information includes the fix number, package type, and package description.

Follow these steps:

1. Click the Software Catalog tab, and select the product release that has the aggregated package whose details you want to view.

The maintenance packages for the release are listed.

2. Click the Fix # link for the aggregated package.

The Maintenance Package Details dialog opens.

3. Click the Nested Packages tab.

A list of nested packages contained in the aggregated package appears.

Manage Maintenance

After maintenance has been downloaded for a product, you can manage the maintenance in an existing SMP/E product installation environment.

Note: While you are working with a particular SMP/E environment, the SMP/E environment is locked and other CA MSM users cannot perform any action against it. When the task finishes, or when you log out from CA MSM, or when your CA MSM session is inactive for more than 10 minutes, the lock releases.

The following installation modes are available:

Receive and Apply

Receives the maintenance and applies it to the selected SMP/E environment.

Receive and Apply Check

Receives the maintenance and checks if the maintenance can be applied to the selected SMP/E environment.

Receive, Apply Check, and Apply

Receives the maintenance, checks if the maintenance can be applied to the selected SMP/E environment, and applies it if it can be applied.

Receive Only

Receives the maintenance.

The process starts a wizard that guides you through the maintenance steps. At the end of the wizard, a task dynamically invokes the SMP/E and other utilities required to apply the maintenance.

Note: You can also manage maintenance to an SMP/E environment using the SMP/E Environments, Maintenance tab.

Follow these steps:

1. Click the Software Catalog tab, and select the product from the tree at the left. Maintenance information appears at the right for the releases you have.
2. Click Update Catalog Release for the release on which you want to apply maintenance.

The maintenance information is updated.

- If the information indicates that maintenance is available, click the Release Name link.

The maintenance packages are listed, for example:

Software Status		Software Catalog	SMP/E Environments	Deployments	System Registry	Tasks	Settings																																																																													
<p>Search</p> <p>Search For:</p> <p>Search In: Products</p> <p>Actions</p> <p>Update Catalog Tree</p> <p>Show LMP Keys</p> <p>Insert New Product</p> <p>Install External Package</p> <p>Available Products</p> <ul style="list-style-type: none"> CA Panvalet - MVS <ul style="list-style-type: none"> 14.4 14.5 <ul style="list-style-type: none"> SP1 CA Panvalet Option for ISPF - MVS CA Panvalet Option for TSO - MVS CA Partition Expert for DB2 for z/OS - MVS CA PDSMAN PDS Library Management ALL 5 COMPONENTS - MVS CA PDSMAN PDS Library Management All Extensions and Performance - MVS 		<p>14.5</p> <p>Products > CA > CA Panvalet - MVS > 14.5</p> <p>Maintenance Packages Add External Maintenance Refresh</p> <p>Show: All All for current release All source IDs</p> <p>Select and: Install 1 - 10 of 70</p> <table border="1"> <thead> <tr> <th>Select</th> <th>Fix #</th> <th>Description</th> <th>Confirmed Date</th> <th>Type</th> <th>Installed</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>0185668</td> <td>* PRODUCT DOCUMENTATION CHANGE</td> <td>Jan 29, 2007</td> <td>PEA/PDC</td> <td>Not installable</td> <td>Actions</td> </tr> <tr> <td><input type="checkbox"/></td> <td>0089243</td> <td>* PRODUCT ERROR ALERT *</td> <td>Jun 20, 2007</td> <td>PEA/PDC</td> <td>Not installable</td> <td>Actions</td> </tr> <tr> <td><input type="checkbox"/></td> <td>R012055</td> <td>0607: MSM INST. ADD SUPPORT FOR SAMPJCL UNDER SMP/E</td> <td>Oct 7, 2009</td> <td>PTF</td> <td>No (0/1)</td> <td>Actions</td> </tr> <tr> <td><input type="checkbox"/></td> <td>0088258</td> <td>14.5-SP00 : PANO/PAN#1 INPUT STREAM INVALID COMMAND</td> <td>May 11, 2007</td> <td>PTF</td> <td>No (0/1)</td> <td>Actions</td> </tr> <tr> <td><input type="checkbox"/></td> <td>0088259</td> <td>14.5-SP01 : PANO/PAN#1 INPUT STREAM INVALID COMMAND</td> <td>May 11, 2007</td> <td>PTF</td> <td>No (0/1)</td> <td>Actions</td> </tr> <tr> <td><input type="checkbox"/></td> <td>0086490</td> <td>14.5-SP00 : DOING ++WRITE, LNG FMT CHANGED AFTER</td> <td>Mar 6, 2007</td> <td>PTF</td> <td>No (0/1)</td> <td>Actions</td> </tr> <tr> <td><input type="checkbox"/></td> <td>0090975</td> <td>14.5-SP00/SP01: PAM DIRECTORY AVERAGE BYTES</td> <td>Sep 4, 2007</td> <td>PTF</td> <td>No (0/1)</td> <td>Actions</td> </tr> <tr> <td><input type="checkbox"/></td> <td>0081764</td> <td>14.5-SP00: PAN#1 ++CONTROL WITH NO CODE GIVES ERROR</td> <td>Aug 25, 2006</td> <td>PTF</td> <td>No (0/1)</td> <td>Actions</td> </tr> <tr> <td><input type="checkbox"/></td> <td>0081763</td> <td>14.5-SP00: PV071 DOING ++SCANS OF ZTYPE1-8 MEMBERS</td> <td>Aug 25, 2006</td> <td>PTF</td> <td>No (0/1)</td> <td>Actions</td> </tr> <tr> <td><input type="checkbox"/></td> <td>0086868</td> <td>14.5-SP00: ZTYPE7 NOT FORMATTED CORRECTLY ON TSO</td> <td>Mar 19, 2007</td> <td>PTF</td> <td>No (0/1)</td> <td>Actions</td> </tr> </tbody> </table>						Select	Fix #	Description	Confirmed Date	Type	Installed	Actions	<input type="checkbox"/>	0185668	* PRODUCT DOCUMENTATION CHANGE	Jan 29, 2007	PEA/PDC	Not installable	Actions	<input type="checkbox"/>	0089243	* PRODUCT ERROR ALERT *	Jun 20, 2007	PEA/PDC	Not installable	Actions	<input type="checkbox"/>	R012055	0607: MSM INST. ADD SUPPORT FOR SAMPJCL UNDER SMP/E	Oct 7, 2009	PTF	No (0/1)	Actions	<input type="checkbox"/>	0088258	14.5-SP00 : PANO/PAN#1 INPUT STREAM INVALID COMMAND	May 11, 2007	PTF	No (0/1)	Actions	<input type="checkbox"/>	0088259	14.5-SP01 : PANO/PAN#1 INPUT STREAM INVALID COMMAND	May 11, 2007	PTF	No (0/1)	Actions	<input type="checkbox"/>	0086490	14.5-SP00 : DOING ++WRITE, LNG FMT CHANGED AFTER	Mar 6, 2007	PTF	No (0/1)	Actions	<input type="checkbox"/>	0090975	14.5-SP00/SP01: PAM DIRECTORY AVERAGE BYTES	Sep 4, 2007	PTF	No (0/1)	Actions	<input type="checkbox"/>	0081764	14.5-SP00: PAN#1 ++CONTROL WITH NO CODE GIVES ERROR	Aug 25, 2006	PTF	No (0/1)	Actions	<input type="checkbox"/>	0081763	14.5-SP00: PV071 DOING ++SCANS OF ZTYPE1-8 MEMBERS	Aug 25, 2006	PTF	No (0/1)	Actions	<input type="checkbox"/>	0086868	14.5-SP00: ZTYPE7 NOT FORMATTED CORRECTLY ON TSO	Mar 19, 2007	PTF	No (0/1)	Actions
Select	Fix #	Description	Confirmed Date	Type	Installed	Actions																																																																														
<input type="checkbox"/>	0185668	* PRODUCT DOCUMENTATION CHANGE	Jan 29, 2007	PEA/PDC	Not installable	Actions																																																																														
<input type="checkbox"/>	0089243	* PRODUCT ERROR ALERT *	Jun 20, 2007	PEA/PDC	Not installable	Actions																																																																														
<input type="checkbox"/>	R012055	0607: MSM INST. ADD SUPPORT FOR SAMPJCL UNDER SMP/E	Oct 7, 2009	PTF	No (0/1)	Actions																																																																														
<input type="checkbox"/>	0088258	14.5-SP00 : PANO/PAN#1 INPUT STREAM INVALID COMMAND	May 11, 2007	PTF	No (0/1)	Actions																																																																														
<input type="checkbox"/>	0088259	14.5-SP01 : PANO/PAN#1 INPUT STREAM INVALID COMMAND	May 11, 2007	PTF	No (0/1)	Actions																																																																														
<input type="checkbox"/>	0086490	14.5-SP00 : DOING ++WRITE, LNG FMT CHANGED AFTER	Mar 6, 2007	PTF	No (0/1)	Actions																																																																														
<input type="checkbox"/>	0090975	14.5-SP00/SP01: PAM DIRECTORY AVERAGE BYTES	Sep 4, 2007	PTF	No (0/1)	Actions																																																																														
<input type="checkbox"/>	0081764	14.5-SP00: PAN#1 ++CONTROL WITH NO CODE GIVES ERROR	Aug 25, 2006	PTF	No (0/1)	Actions																																																																														
<input type="checkbox"/>	0081763	14.5-SP00: PV071 DOING ++SCANS OF ZTYPE1-8 MEMBERS	Aug 25, 2006	PTF	No (0/1)	Actions																																																																														
<input type="checkbox"/>	0086868	14.5-SP00: ZTYPE7 NOT FORMATTED CORRECTLY ON TSO	Mar 19, 2007	PTF	No (0/1)	Actions																																																																														

Red asterisks identify HIPER maintenance packages.

- Click the Fix # link for each maintenance package you want to install.

The Maintenance Package Details dialog appears, identifying any prerequisites.
- Review the information on this dialog, and click Close to return to the Maintenance Packages section.
- Select the maintenance packages you want to install, and click the Install link.

Note: The Installed column indicates whether a package is installed.

The Introduction tab of the wizard appears.
- Review the information about the maintenance, and click Next.

The packages to install are listed.
- Review and adjust the list selections as required, and click Next.

The SMP/E environments that contain the product to maintain are listed. Only environments in your working set are listed.
- Select the environments in which you want to install the packages.
- Click Select Zones to review and adjust the zones where the maintenance will be installed, click OK to confirm the selection and return to the wizard, and click Next.

Note: If you select an SMP/E environment being used in CA MSM by another user, a notification message appears. You are prevented from performing any actions on the SMP/E environment. You can either wait until the notification message disappears and the SMP/E environment becomes available, or click Cancel to select another SMP/E environment.

11. Select the installation mode for the selected maintenance, and click Next.
 - If prerequisites exist and are available, review them and click Next. CA MSM installs these prerequisites as part of the process. If a prerequisite is *not* available, the wizard cannot continue. You must acquire the prerequisite and restart the process.
 - If [HOLDDATA](#) (see page 159) entries exist, review and select them, and click Next.

SMP/E work DDDEFs of SMPWRKx and SYSUTx, with their allocation parameters, are listed.

Note: For more information about SMPWRKx and SYSUTx data sets, see the *IBM SMP/E for z/OS Reference*.

12. Review the allocation parameters of work DDDEFs, and edit them if necessary to verify, that sufficient space is allocated for them during the maintenance installation:

Note: Changes in the allocation parameters apply to the current maintenance installation only.

- a. Click Override for a DDDEF to edit its allocation parameters.

A pop-up window opens.

- b. Make the necessary changes, and click OK to confirm.

The pop-up window closes, and the DDDEF entry is selected in the list indicating that the allocation parameters have been overridden.

Note: To update allocation parameters for all DDDEFs automatically, click Retrieve DDDEF. CA MSM provides values for all DDDEFs based on the total size of the selected maintenance packages that you want to install. All DDDEF entries are selected in the list indicating that the allocation parameters have been overridden.

- If you want to cancel a parameter update for any DDDEF, clear its check box.
- If you want to edit the allocation parameters for a particular DDDEF after you automatically updated them using the Retrieve DDDEF button, click Override. Make the necessary changes and click OK to confirm, and return to the wizard.

13. (Optional) Review SMP/E work DDDEF and their allocation parameters for the selected SMP/E zones, and click Close to return to the wizard.

Note: The allocation parameters can differ from the allocation parameters that you obtained using the Retrieve DDDEF button.

14. Click Next.

A summary of the task appears.

15. Review the summary, and click Install.

A dialog that shows the progress of the task opens. When the task completes, you can click Show Results on the Progress tab to close this dialog. The task output browser opens and you can view the action details. Click Close to close the task output browser.

Note: While a task is in progress, you can perform other work. You can click Hide to exit the dialog and view the task status later on the Tasks tab.

The task applies the maintenance. You can accept the maintenance (except USERMODs) using the SMP/E Environments, Maintenance tab. As a best practice, CA MSM prevents you from accepting USERMODs.

More information:

[Download Product Maintenance Packages](#) (see page 51)

[Download Maintenance Packages for Old Product Releases and Service Packs](#) (see page 52)

View Installation Status of Maintenance Package

You can view installation status details of each maintenance package, including a list of SMP/E environments where the package is installed. You can also see the SMP/E environment data sets, and the installation status of the package for each SMP/E environment zone. For example, a maintenance package can be received in the global zone, but applied in a target zone, and accepted in a distribution zone.

Note: The installation status is not available for aggregated maintenance packages, for packages that are uninstallable, and for packages that do not have available SMP/E environments for installation.

Depending on the package status for each zone, you can see available actions for the package. For example, if the package is not received in an SMP/E environment zone, the Install action is available.

Follow these steps:

1. Click the Software Catalog tab, and select the product release that has the maintenance package whose installation status you want to view.

The maintenance packages for the release are listed.

2. Click the status link in the Installed column for the maintenance package.

The Maintenance Package Details dialog opens to the Installation Status tab. A list of SMP/E environments with package status per zone appears.

Note: Click the Actions drop-down list to start the installation wizard for packages that are not yet installed in at least one SMP/E environment zone, or the accept wizard for packages that are not accepted in at least one SMP/E environment zone. Click Install to More Environments to install the maintenance package in one or more SMP/E environments available for the package.

USERMODs

A product USERMOD can be provided as a published maintenance package downloaded during the Update Catalog process. When CA MSM downloads a package including a ++USERMOD statement, it is loaded under the product with a USERMOD type. You can install these packages using CA MSM but cannot accept them because they are not intended to be permanent.

You can create a USERMOD manually, or we can provide an unpublished maintenance package as a USERMOD. In this case, the USERMOD file, which contains the ++USERMOD statement and the body of the USERMOD, must be [managed as an externally downloaded package](#) (see page 53).

GROUPEXTEND Mode

CA MSM lets you invoke the SMP/E utility with the GROUPEXTEND option enabled for managing (applying and accepting) maintenance.

Sometimes before you install a maintenance package, you install other maintenance packages first (SYSMODs).

If a SYSMOD - prerequisite for the required maintenance package, has not been applied or cannot be processed, you can install the maintenance package in GROUPEXTEND mode. (For example, the SYSMOD is held for an error, a system, or a user reason ID; it is applied in error; it is not available.) The SMP/E environment where the product is installed automatically includes a superseding SYSMOD.

Note: When applying maintenance in GROUPEXTEND mode, the SMP/E environment *must* receive all SYSMODs that are included in the GROUPEXTEND option.

When you apply maintenance in GROUPEXTEND mode, the following installation modes are available:

Apply Check

Checks if the maintenance can be applied to the selected SMP/E environment in GROUPEXTEND mode.

Apply

Applies the maintenance to the selected SMP/E environment in GROUPEXTEND mode.

Apply Check and Apply

Checks if the maintenance can be applied to the selected SMP/E environment in GROUPEXTEND mode. Then applies it if possible.

For the GROUPEXTEND option, CA MSM does not automatically receive and display maintenance or HOLDDATA prerequisites that must be bypassed when applying the maintenance. Apply check mode lets you check if any prerequisites or HOLDDATA exist and report them in the task output.

You can also use the following similar installation modes to accept maintenance in GROUPEXTEND mode:

- Accept Check
- Accept
- Accept Check and Accept

How Maintenance in GROUPEXTEND Mode Works

We recommend that you apply maintenance in GROUPEXTEND mode in the following sequence:

1. Receive all SYSMODs that you want to include by the GROUPEXTEND option.
2. Run the maintenance in Apply check mode.
 - If the task fails, review SMPOUT in the task output. Review if there are missing (not received) SYSMODs or HOLDDATA that must be resolved or bypassed.
 - If the task succeeds, review SMPRPT in the task output. Review what SYSMODs were found and applied.
3. Run the maintenance in Apply mode, and specify SYSMODs that you want to exclude and HOLDDATA that you want to bypass, if any exist.

The followings options are available for bypassing HOLDDATA:

- HOLDSYSTEM
- HOLDCLASS
- HOLDERERROR
- HOLDUSER

Note: For more information about the BYPASS options, see the *IBM SMP/E V3Rx.0 Commands*. *x* is the SMP/E release and corresponds to the SMP/E version that you use.

You can run the maintenance in Apply mode in the same CA MSM session after Apply check mode is completed. The values that you entered for Apply check mode are then prepopulated on the wizard dialogs.

Manage Maintenance in GROUPEXTEND Mode

CA MSM lets you invoke the SMP/E utility with the GROUPEXTEND option enabled for managing (applying and accepting) maintenance.

Note: While you are working with a particular SMP/E environment, the SMP/E environment is locked and other CA MSM users cannot perform any action against it. When the task finishes, or when you log out from CA MSM, or when your CA MSM session is inactive for more than 10 minutes, the lock releases.

Follow these steps:

1. Click the SMP/E Environments tab, and select the SMP/E environment from the tree on the left side.

A list of products installed in the SMP/E environment appears.

Note: If you select an SMP/E environment being used in CA MSM by another user, a notification message appears. You are prevented from performing any actions on the SMP/E environment. You can either wait until the notification message disappears and the SMP/E environment becomes available, or click Cancel to select another SMP/E environment.

2. Click the Maintenance link.

A list of maintenance packages for the products installed in the SMP/E environment appears.

3. Select the maintenance packages that you want to apply in GROUPEXTEND mode, and click the Apply GROUPEXTEND link.

The Introduction tab of the wizard appears.

4. Review the information about the maintenance, and click Next.

The packages that you want to apply are listed.

Note: Click a link in the Status column for a maintenance package, if available, to review a list of zones. The zones indicate, where the maintenance package is already received, applied, or accepted. Click Close to return to the wizard.

5. Review the packages, and click Next.

The Prerequisites tab of the wizard appears.

Important! For the GROUPEXTEND option, CA MSM does not automatically receive and display maintenance or HOLDDATA prerequisites that must be bypassed when applying the maintenance. Apply check mode lets you review if any prerequisites or HOLDDATA exist and report them in the task output. We recommend that you run the maintenance in Apply check mode first.

6. Read the information that is displayed on this tab, and click Next.

Installation options appear.

7. Specify installation options as follows, and click Next:
 - a. Select the installation mode for the selected maintenance.
 - b. Review the GROUPEXTEND options and select the ones that you want to apply to the maintenance:

NOAPARS

Excludes APARs that resolve error reason ID.

NOUSERMODS

Exclude USERMODs that resolve error user ID.

- c. (Optional) Enter SYSMODs that you want to exclude in the Excluded SYSMODs field. You can enter several SYSMODs, separate them by a comma.

The Bypass HOLDDATA tab of the wizard appears.

8. (Optional) Enter the BYPASS options for the HOLDDATA that you want to bypass during the maintenance installation. You can enter several BYPASS options, separate them by a comma.

9. Click Next.

A summary of the task appears.

10. Review the summary, and click Apply GROUPEXTEND.

A dialog that shows the progress of the task opens. When the task completes, you can click Show Results on the Progress tab to close this dialog. The task output browser opens and you can view the action details. Click Close to close the task output browser.

Note: While a task is in progress, you can perform other work. You can click Hide to exit the dialog and view the task status later on the Tasks tab.

- If you run the maintenance installation in Apply check mode and the task succeeds, review SMPRPT in the task output. Review what SYSMODs were found and applied.
- If you run the maintenance installation in Apply check mode and the task fails, review SMPOUT in the task output. Review if there are missing (not received) SYSMODs or HOLDDATA that must be resolved or bypassed.

You can accept the maintenance (except USERMODs) in the GROUPEXTEND mode using the SMP/E Environments, Maintenance tab. As a best practice, CA MSM prevents you from accepting USERMODs.

Note: You cannot accept USERMODs in GROUPEXTEND mode. Providing you have not enabled NOUSERMODS option, you can install USERMODs that are prerequisites for the maintenance package being installed.

Back Out Maintenance

You can back out an applied maintenance package (but not an accepted maintenance package) through the SMP/E Environments tab. The process starts a wizard that guides you through the backout.

Note: While you are working with a particular SMP/E environment, the SMP/E environment is locked and other CA MSM users cannot perform any action against it. When the task finishes, or when you log out from CA MSM, or when your CA MSM session is inactive for more than 10 minutes, the lock releases.

Follow these steps:

1. Click the SMP/E Environments tab, and select the SMP/E environment from which you want to back out maintenance on the tree on the left side.

Products installed in the environment are listed.

2. Select the product component from which you want to back out maintenance.

The features in the component are listed.

Note: You can back out maintenance from all the products in the environment. Click the Maintenance tab to list all the maintenance packages for the environment.

3. Select the function from which you want to back out maintenance.

The maintenance packages for the feature are listed.

Note: You can use the Show drop-down list to show only applied packages.

4. Select the packages that you want to back out, and click the Restore link.

The maintenance wizard opens to the Introduction step.

Note: If you select an SMP/E environment being used in CA MSM by another user, a notification message appears. You are prevented from performing any actions on the SMP/E environment. You can either wait until the notification message disappears and the SMP/E environment becomes available, or click Cancel to select another SMP/E environment.

5. Review the information about the backout, and click Next.

The packages to back out are listed.

6. Review and adjust the list selections as required, and click Next.

Note: To review and adjust a list of zones from where you want to restore the maintenance, click Select Zones. Click OK to confirm the selection and return to the wizard.

The Prerequisite tab of the wizard appears.

7. Review the prerequisites if they exist, and click Next. CA MSM restores these prerequisites as part of the maintenance backout process.

A summary of the task appears.

- Review the summary, and click Restore.

A dialog that shows the progress of the task opens. When the task completes, you can click Show Results on the Progress tab to close this dialog. The task output browser opens and you can view the action details. Click Close to close the task output browser.

Note: While a task is in progress, you can perform other work. You can click Hide to exit the dialog and view the task status later on the Tasks tab.

Setting System Registry

This section includes information about how to use CA MSM to set the system registry. The *system registry* contains information about the systems that have been defined to CA MSM and can be selected as a target for deployments. You can create Non-Sysplex, Sysplex, Shared DASD Cluster, and Staging systems as well as maintain, validate, view, and delete a registered system, and investigate a failed validation.

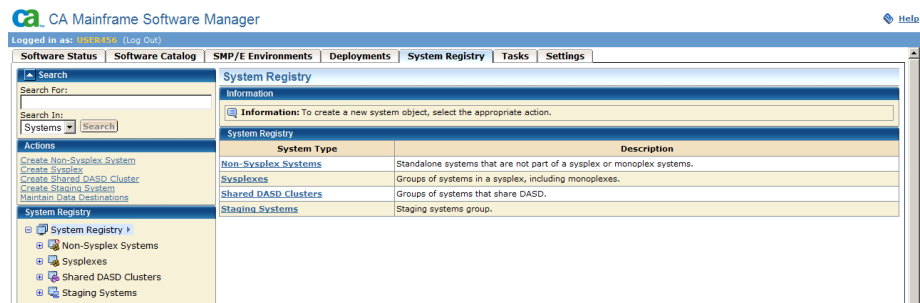
View a System Registry

You can view a system registry by using the CA MSM.

Follow these steps:

- Click the System Registry tab, and select Non-Sysplex Systems, Sysplexes, Shared DASD Clusters, or Staging Systems from the tree on the left side.

Information about the systems that you selected appears on the right side.

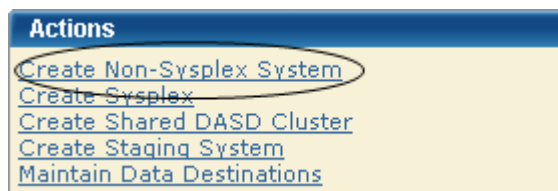


Create a Non-sysplex System

You can create a non-sysplex system registry.

Follow these steps:

1. Click the System Registry tab, and in the Actions section click the Create Non-Sysplex System link.



The New Non-Sysplex System dialog appears.

Note: The asterisk indicates that the field is mandatory.

2. Enter the following information, and click Save:

Name

Enter the non-sysplex system name.

Limits: Eight characters

Note: Sysplex and non-sysplex systems can have the same name. Use the Description field to differentiate between these systems.

Description

Enter the description.

Limits: 255 characters

CCI System ID

(Optional) Enter the CAICCI system ID.

Limits: Eight characters

Note: The *CAICCI system ID* is a unique name for a system that is part of a CAICCI network. If you do not specify one, CA MSM obtains it using a validate action.

The non-sysplex system is saved, and its name appears in the non-sysplex system list on the left.

Note: To withdraw this create request, click Cancel.

3. Detail the nonstaging system.

Important! z/OS systems running under VM are treated as being in BASIC mode and not LPAR mode. As a result, the LPAR number is null in the z/OS control block. When the LPAR number is null, the system validation output shows the following message:

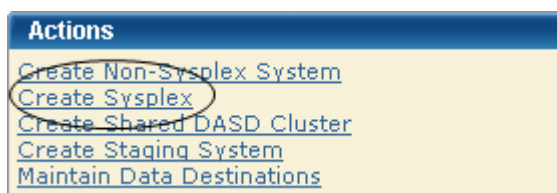
Property Name: z/OS LPAR Name, Value: ** Not Applicable **.

Create a Sysplex or Monoplex

If you have monoplexes with the same sysplex name, you can create a sysplex or monoplex system registry. Monoplexes are stored in the sysplex registry tree but with the name of the sysplex system and not the monoplex sysplex name. For example, you have a system XX16 defined as a monoplex, with a sysplex name of LOCAL. The system registry displays the system as a sysplex, with the name LOCAL. This sysplex contains one system: XX16.

Follow these steps:

1. Click the System Registry tab, and in the Actions section click the Create Sysplex link.



The New Sysplex dialog appears.

Note: The asterisk indicates that the field is mandatory.

2. Enter the following and click Save.

Name

Enter the sysplex system name.

Limits: Eight characters

Description

Enter the description.

Limits: 255 characters

Sysplex and non-sysplex system can have the same name. Use the Description field to differentiate these systems.

The sysplex system is saved, and its name appears in the sysplex list on the right.

Note: Click Cancel to withdraw this create request.

Important! z/OS systems running under VM are treated as being in BASIC mode and not LPAR mode. As a result, the LPAR number is null in the z/OS control block. In this case, the system validation output includes the following message:

Property Name: z/OS LPAR Name, Value: ** Not Applicable **.

3. Right-click the newly added sysplex and select Create Sysplex System to add a system to a sysplex. Repeat this process for each system belonging to this sysplex.

4. Enter the following data items for each system:

Name

Enter the sysplex system name.

Limits: Eight characters

Note: Sysplex and non-sysplex systems can have the same name. Use the Description field to differentiate between these systems.

Description

Enter the description.

Limits: 255 characters

CCI System ID

(Optional) Enter the CAICCI system ID.

Limits: Eight characters

Note: The *CAICCI system ID* is a unique name for a system that is part of a CAICCI network. If you do not specify one, CA MSM obtains it using a validate action.

The non-sysplex system is saved, and its name appears in the non-sysplex system list on the left.

Note: To withdraw this create request, click Cancel.

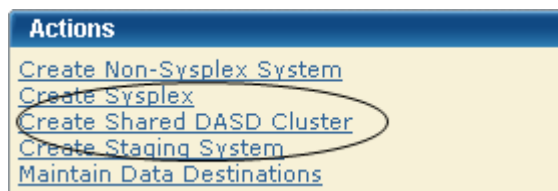
5. Detail the nonstaging system.

Create a Shared DASD Cluster

You can create a shared DASD cluster.

Follow these steps:

1. Click the System Registry tab, and in the Actions section click the Shared DASD Cluster link.



The New Shared DASD Cluster dialog appears.

Note: The asterisk indicates that the field is mandatory.

2. Enter the following information, and click Save:

Name

Enter the shared DASD cluster name.

Limits: Eight characters

Note: Each shared DASD cluster name must be unique and it is not case-sensitive. For example, DASD1 and dasd1 are the same shared DASD cluster name. A shared DASD cluster can have the same name as a non-sysplex, sysplex, or staging system.

Description

Enter the description.

Limits: 255 characters

The shared DASD cluster is saved, and its name appears in the Shared DASD Clusters section on the right.

Note: Click Cancel to withdraw this create request.

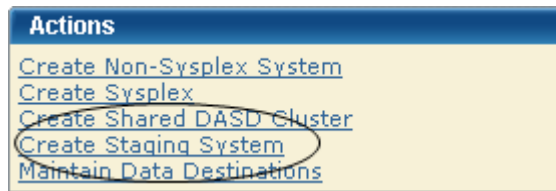
3. Right-click the newly added DASD cluster name and select Add System or Sysplex to this Shared DASD Cluster. Select the systems or sysplexes that you want to add to the DASD cluster.

Create a Staging System

You can create a staging system.

Follow these steps:

1. Click the System Registry tab, and in the Actions section click the Create Staging System link.



The New Staging System dialog appears.

Note: The asterisk indicates that the field is mandatory.

2. Enter the following information, and click Save:

Name

Enter the staging system name.

Limits: Eight characters

Note: Each staging system name must be unique and is not case-sensitive. For example, STAGE1 and stage1 are the same staging system name. A staging system can have the same name as a non-sysplex, sysplex, or a shared DASD cluster.

Description

Enter the description.

Limits: 255 characters

The staging system is saved, and it appears in the Staging System Registry on the right.

Note: Click Cancel to withdraw this create request.

Authorization

CA MSM supports the following authorization modes for the system registry.

Edit Mode

Lets you update and change system registry information.

Note: After the information is changed, you must click Save to save the information or Cancel to cancel the changed information.

View Mode

Lets you view system registry information.

Note: You cannot edit information in this mode.

Change a System Registry

You can change the system registry if you have Monoplexes with the same sysplex name (for example: LOCAL). Instead of showing multiple LOCAL sysplex entries which would need to be expanded to select the correct Monoplex system, the CA MSM System Registry shows the actual Monoplex System name at the top level Sysplex Name.

Follow these steps:

1. Click the System Registry tab, and select Non-Sysplex Systems, Sysplexes, Shared DASD Clusters, or Staging Systems from the tree on the left side.

Information about the systems that you selected appears on the right side.

2. Select the system to change.

Detailed information about the system appears on the right side.

3. Update the following information as needed. The information that you update is dependent on whether you are changing a [Non-Sysplex System](#) (see page 65), [Sysplex](#) (see page 66), [Shared DASD Cluster](#) (see page 67), or [Staging System](#) (see page 68).

4. Depending on the type of system, do one of the following:

- For Shared DASD or sysplex system only, select the [contact system](#) (see page 75), which is the system where the Shared DASD or FTP is located. The FTP location should be set to the contact system URI. The contact system is used for remote credentials.

For example, if the contact system is set to CO11, FTP location URI is set to XX61 and the remote credentials are set up for CO11, the deployment could fail because your remote credentials might not be the same on both systems (CO11 and XX61) and, because you set the Contact System to CO11 but you are contacting to XX61, a spawn will be started on CO11 but CA MSM will look for the output on XX61 because that is where the FTP location was set.

Note: Monoplexes are stored in the Sysplex registry tree but with the name of the Monoplex System and not the Monoplex Sysplex name. For example, a system XX16 defined as a Monoplex, with a sysplex name of LOCAL. It will be depicted in the System Registry as a Sysplex with the name of XX16. This sysplex will contain one system: XX16.

The FTP and DATA Destinations at the system level are not used when the Sysplex is a Monoplex. The only FTP Location and Data Destinations that are referenced are those defined at the Sysplex Level.

- For Staging systems, enter the GIMUNZIP volume and/or [zFS candidate volumes](#) (see page 76).

The zFS candidate volumes let you specify an optional list of VOLSERs used during the allocation of zFS container data sets for USS parts.

5. Select one of the following actions from the Actions drop-down list in the General bar:

Cancel

Cancel this maintenance.

Save

Save the changes to this maintenance.

Validate

Validate authenticates this entry.

Note: The validation process is done in steps; each system in this request is validated with the last step summarizing, verifying, and confirming the validation. If the validation fails this step shows how the validation failed. You can [investigate the failed validation](#) (see page 73).

Validation Rules

- For a Non-Sysplex system, that single system is validated and the last step summarizes, verifies, and confirms the validation.
- For a Sysplex system, each system within the Sysplex is validated as an individual step and the last step summarizes, verifies, and confirms the validation.
- For Shared DASD Cluster each Non-Sysplex system is validated, each Sysplex system is validated as described in the Sysplex Rule and the last step summarizes, verifies, and confirms the validation.

Note: A Staging system is not validated.

When a system is validated, the status appears in the Status field.

The following are the system validation results:

Validated

Indicates that the system is available, status is updated as valid, and system registry is updated with results from validation.

Validation in Progress

Indicates that the system status is updated to in progress.

Validation Error

Indicates that the system status is updated to error, and you can [investigate the failed validation](#) (see page 73).

Not Validated

Indicates that this system has not been validated yet.

Not Accessible

Indicates that the system has not been validated because it is no longer available or was not found in the CCI Network.

Validation Conflict

Indicates that the system has been contacted but the information entered then different then the information retrieved.

Error Details

When there is a validation conflict, the Error details button appears. Click this button to find the reason for this conflict. You can [investigate the failed validation](#) (see page 73).

Note: The error reason resides in local memory. If the message *Please validate the system again* appears, the local memory has been refreshed and the error has been lost. To find the conflict again, validate this system again.

Conflict Details

When a validation is in conflict, the Error details button appears. Click this button to find the reason for this conflict. You can [investigate the failed validation](#) (see page 73).

Note: The conflict reason is kept in local memory. If the "Please validate the system again." message appears, the local memory has been refreshed and the conflict has been lost. To find the conflict again, validate this system again.

Failed Validations

Use the following procedures in this section to investigate a failed validation, make corrections, and revalidate:

- [Investigate a Failed Validation using the Tasks Page](#) (see page 73)
- [Investigate a Failed Validation Immediately After a Validation](#) (see page 74)
- [Download a Message Log](#) (see page 74)
- [Save a Message Log as a Data Set](#) (see page 75)
- [View Complete Message Log](#) (see page 75)

Note: The CA MSM screen samples in these topics use a non-sysplex system as an example. The method also works for a sysplex or a shared DASD cluster.

Investigate a Failed Validation Using Task Output Browser

You can investigate a failed validation, make corrections, and validate it again.

Follow these steps:

1. On the System Registry tab, in the column on the left, find the system with a validation status error and make a note of it.
 2. Click the Tasks tab and then click Task History.
 3. At the Show bar, select All task, or My task to list the tasks by Owner.
- Note:** You can refine the task list by entering USER ID, types, and status.
4. Find the failed validation and click the link in the Name column.

The screenshot shows the 'Task History' window with a table of tasks. The 'Name' column contains a link to 'Validating System: XX60' which is circled in red. The 'Status' column shows a red 'X' and the word 'Failed'. The 'Start Time' is 1/12/2010 02:26:01PM and the 'Stop Time' is 1/12/2010 02:26:09PM. The 'Task ID' is 432.

Owner	Name	Type	Status	Start Time	Stop Time	Task ID
USER456	Validating System: XX60	System Registry	Failed	1/12/2010 02:26:01PM	1/12/2010 02:26:09PM	432

The Validate System Task Output Browser appears.

The screenshot shows the 'Validate System: XX60' window. It has a 'General' tab and a 'Steps' tab. The 'General' tab shows details: Name: Validate System: XX60, Task ID: 447, User ID: USER456, Status: Failed, Status Message: Failed to undo command. The 'Steps' tab shows a table with two steps: 'Validating System: XX60' (Succeeded) and 'Validation Results' (Failed).

#	Name	Description	Status
1	Validating System: XX60	Validating system and retrieving values.	Succeeded
2	Validation Results	Validation results for all the systems that were validated.	Failed

5. Click the Validation Results link to view the results.

6. Click the messages log to review the details for each error.

Note: You can analyze the error results and can determine the steps that are required to troubleshoot them.

7. Correct the issue and validate again.

Investigate a Failed Validation After Validation

You can investigate a failed validation, make corrections, and validate it again.

Follow these steps:

1. On the System Registry tab, in the column on the left, find the system with a validation status error, and make a note of it.
2. Click Details to see the error details.
3. If the error message prompts you to revalidate the system, click Validate.
4. Click the Progress tab.
5. Click Show Results to view the results.

The validation results appear.

6. Click the messages logs to review the details for each error.

Note: You can analyze the error results and can determine the steps that are required to troubleshoot them.

7. Correct the issue and validate again.

Download a Message Log

You can save the message log in the following ways:

- To download a zipped file of all the text messages for this validation, click the Deployment Name on the top left tree. Click the Download Zipped Output button on the General menu bar. Save this file.
- To download as TXT, click the Deployment Name or the Deployment Results on the left tree. Click the Action button on the Message Log bar and click the Download as TXT. Save this file.
- To download as ZIP, click the Deployment Name or the Deployment Results on the left tree. Click the Action button on the Message Log bar and click the Download as ZIP. Save this file.

Save a Message Log as a Data Set

You can save a message log as a data set.

Follow these steps:

1. Click the Deployment Name or the Deployment Results on the left tree. Click the Action button on the Message Log bar, and click the Save as Data Set.

The Save Output as Data Set dialog appears.

Note: This information is sent to CA Support to analyze the failed deployment.

Note: The asterisk indicates that the field is mandatory.

2. Enter the following information and click OK:

Data Set Name

Enter a data set name. CA MSM generates a value.

VOLSER

For non-SMS data, enter the Volser.

Example:

Volser: SYSP01 and SYSP02

Storage Class

For SMS Allocation data, enter the Storage Class.

The message log is saved as a data set.

View Complete Message Log

To view the complete message log for a failed validation, click Show All.

Note: To close the message log, click Close.

Contact System

The *contact system* defines which system the deployment is unpackaged on. That is, which system CAICCI is spawned to run the unpackaging.

When deploying to a shared DASD cluster, sysplex, or both, the deployment is sent to only one system in that configuration, where it is unpackaged. The expectation is that all other systems within that configuration have access to the unpackaged deployment.

For a shared DASD cluster or sysplex, the URI must be the URI of the Contact System. Also, set up Remote Credentials for the contact system, because they are used to retrieve the deployment results.

zFS Candidate Volumes

You can use a *zFS candidate volume* when your environmental setup dictates that zFS container data sets are directed to the specified volume.

When your environmental setup dictates that zFS container data sets are directed to specified zFS candidate volumes, use one or more of the candidate volumes. CA MSM uses the candidate volumes in the IDCAMS statement to create the zFS container VSAM data set.

The zFS candidate volumes are only required if the following statements are true:

- Your deployment has USS parts.
- You are doing a container copy.
- You selected zFS as the container type.
- The remote system requires it.

Note: Remote system requirement is customer defined.

To allocate and maintain your disk, the following products are recommended:

CA Allocate

CA Allocate is a powerful and flexible allocation management system that lets the Storage Administrator control the allocation of all z/OS data sets.

CA Disk Backup and Restore

CA Disk is a flexible, full-featured hierarchal storage management system.

You can also use the following standard IBM techniques:

- Allocation exits
- ACS routines

If you do not implement any of these options, z/OS needs a candidate list of volumes for placing the zFS archive.

Maintain a System Registry using the List Option

Follow these steps:

1. Click the System Registry tab.
The System Registry window appears.
2. In the System Registry panel on the right, click the System Type link, and then click the system name.
The detailed system entry information appears.

Delete a System Registry

Follow these steps:

1. Click the System Registry tab and on the right, in the System Registry panel, select Non-Sysplex Systems, Sysplexes, Shared DASD Clusters, or Staging Systems.

The system list appears.

2. Select each system registry that you want to delete, click Delete, and then click OK to confirm.

The system is deleted.

FTP Locations

The [FTP](#) (see page 77) Locations lists the current FTP locations for this system. You can [add](#) (see page 77), [edit](#) (see page 79), [set default](#) (see page 80), or [remove](#) (see page 80) [FTP](#) (see page 77) locations.

An FTP location must be defined for every system. They are used to retrieve the results of the deployment on the target system regardless if the deployment was transmitted through FTP or using Shared DASD. They are also used if you are moving your deployments through FTP. You will need the URI (host system name), port number (default is 21), and the directory path, which is the landing directory. The landing directory is where the data is temporarily placed during a deployment.

Deployment FTP Locations

File Transfer Protocol (FTP) is a protocol for transfer of files from one computer to another over the network.

Define an FTP location for every system if you deploy to specified systems within a sysplex. They are used to retrieve the deployment results on the target system regardless of whether the deployment was transmitted through FTP or using shared DASD. They are also used when you are moving your deployments through FTP. You need the URI (host system name), port number (default is 21), and the directory path, which is the landing directory. The landing directory is where the data is temporarily placed during a deployment.

Add FTP Locations

You can add [FTP](#) (see page 77) locations.

Follow these steps:

1. Click the System Registry tab, and select Non-Sysplex Systems, Sysplexes, or Shared DASD Clusters from the tree on the left side.

Information about the systems that you selected appears on the right side.

2. Select the system you want to create FTP locations for.

Detailed information about the system appears on the right side.

3. Click the FTP Locations tab.

The FTP Locations window appears.

4. Click Add.

The New FTP Location dialog appears.

Note: The asterisk indicates that the field is mandatory.

5. Enter the following information, and click Save:

URI

Enter the URI.

Limits: Maximum length is 255.

Port

Enter the Port.

Limits: Maximum Port number is 65535 and must be numeric.

Default: 21

Directory Path

Enter the Directory Path.

Limits: Must start with a root directory, that is /.

The new FTP location appears on the list.

Note: Click Cancel to withdraw this create request.

More information:

[Edit FTP Locations](#) (see page 79)

[Delete FTP Locations](#) (see page 80)

[Set FTP Location Default](#) (see page 80)

Edit FTP Locations

You can edit [FTP](#) (see page 77) locations.

Note: The asterisk indicates that the field is mandatory.

Follow these steps:

1. Click the System Registry tab, and select Non-Sysplex Systems, Sysplexes, or Shared DASD Clusters from the tree on the left side.

Information about the systems that you selected appears on the right side.

2. Select the system you want to change FTP locations for.

Detailed information about the system appears on the right side.

3. Click the FTP Location tab.

The FTP Locations window appears.

4. Select the FTP location, click the Actions drop-down list, and select Edit.

The Edit FTP Location dialog appears.

5. Update the following and click Save:

URI

Enter the URI.

Limits: Maximum length is 255.

Port

Enter the Port.

Limits: Maximum Port number is 65535 and must be numeric.

Default: 21

Directory Path

Enter the Directory Path.

Limits: Most start with a root directory, that is, /.

Your changes are saved.

Note: Click Cancel to close this dialog without saving your changes.

Set FTP Location Default

You can set an [FTP](#) (see page 77) location default.

Follow these steps:

1. Click the System Registry tab, and select Non-Sysplex Systems, Sysplexes, or Shared DASD Clusters from the tree on the left side.

Information about the systems that you selected appears on the right side.

2. Select the system you want to set the FTP location default to.

Detailed information about the system appears on the right side.

3. Click the FTP Locations tab.

The FTP Locations window appears.

4. Select the FTP location you want to set as the default, and then select Default from the Actions drop-down list.

Default appears in the Default column, and this location becomes the default FTP location.

Note: The Default action is not available if only one FTP location is defined.

Delete FTP Locations

You can delete [FTP](#) (see page 77) locations.

Follow these steps:

1. Click the System Registry tab, and select Non-Sysplex Systems, Sysplexes, or Shared DASD Clusters from the tree on the left side.

Information about the systems that you selected appears on the right side.

2. Select the system you want to delete FTP locations from.

Detailed information about the system appears on the right side.

3. Click the FTP Locations tab.

The FTP Locations window appears.

4. Click the Select box for each FTP location you want to delete, click Remove, and then click OK to confirm.

The FTP location is deleted from this system.

Data Destinations

The Data Destinations page lists the current data destinations for this system. The following choices are available:

FTP

When FTP is selected as the transport mechanism, the deployment data is shipped to the target system through FTP. The data is temporarily placed on the target system at the landing directory specified in the FTP Location information section of the system registry.

Shared DASD

When you specify shared DASD, CA MSM uses a virtual transport technique. That is, it does not actually copy the data from one system to the other. Because the two systems share DASD, there is no need to copy the data. All of the deployment data is kept in the USS file systems that CA MSM manages.

Even though the DASD is shared, it is possible that the remote system does not find the deployment data in the USS file system. Therefore, CA MSM temporarily unmounts the file system from the CA MSM driving system and mounts it in read-only mode on the remote system.

For CA MSM to determine where to mount the file system on the remote system, specify a mount point location in the data destination. In addition, you can provide allocation information for the creation of the deployment file system. The file system is created on the shared DASD, on the CA MSM driving system.

Data destinations are assigned to non-sysplex and sysplex systems, and shared DASD clusters. Data destinations are named objects, and can be assigned to multiple entities in the system registry. Data destinations can have their own independent maintenance dialogs.

The deployment process on the remote system uses the remote allocation information and lets you control, where the deployed software is placed. By specifying the GIMUNZIP VOLSER, CA MSM adds a volume= parameter to the GIMUNZIP instructions on the remote system. The list of zFS VOLSERS is needed only if both of the following situations occur:

- The software that you are deploying contains USS parts.
- You select a container copy option during the deployment process.

Note: The FTP and data destinations at the system level are not used when the sysplex is a monoplex. The only FTP locations and data destinations that are referenced are defined at the sysplex level.

Create Data Destinations

You can create data destinations that define the method that CA MSM uses to transfer the deployment data to the target systems.

Follow these steps:

1. Click the System Registry tab, and in the Actions section click the Maintain Data destinations link.

The Maintains Data Destinations dialog appears.

2. Click Create.

The New Data Destination dialog appears.

Note: The asterisk indicates that the field is mandatory.

3. Enter the following information, and click Save:

Name

Enter a meaningful name.

Limits: Maximum 64 characters.

Note: Each data destination name must be a unique name and it is not case-sensitive. For example DATAD1 and datad1 are the same data destination name.

Description

Enter the description.

Limits: Maximum 255 characters.

Transmission Method

Select the transmission method.

Default: Shared DASD.

Mount Point

(Shared DASD only) Enter the mount point directory path, which is a directory path that must exist on the target system. The user that is doing the deployment must have write permission to this directory, and mount authorization on the target system.

Note: A mount user must have UID(0) or at least have READ access to the SUPERUSER.FILESYS.MOUNT resource found in the UNIXPRIV class.

Limits: Maximum 120 characters

Note: SMS is not mutually exclusive with non-SMS. They can both be specified (usually one or the other is specified though). This is where you specify allocation parameters for the deployment on a target system.

Storage Class

(Shared DASD only) Enter the Storage Class.

Limits: Maximum 8 characters

Example: SYSPRG

VOLSER

(Shared DASD only) Enter the Volser.

Limits: Maximum 6 characters

Example: SYSP01 and SYSP02

GIMUNZIP Volume

Enter the GIMUNZIP volume.

Limits: Maximum 6 characters

zFS Candidate Volumes

Enter [zFS Candidate volumes](#) (see page 76).

Limits: Maximum 6 characters

The zFS candidate volumes allow the specification of an optional list of VOLSERs used during the allocation of zFS container data sets for USS parts.

The new data destination appears on the Data Destination list.

Note: Click Cancel to withdraw this create request.

Add a Data Destination

You can add current data destinations to an existing system.

Follow these steps:

1. Click the System Registry tab, and select Non-Sysplex Systems, Sysplexes, or Shared DASD Clusters from the tree on the left side.

Information about the systems related to the type you selected appears on the right side.

2. Select the system you want to add data destinations.

Detailed information about the system appears on the right side.

3. Click the Data Destination tab.

The Data Destination window appears.

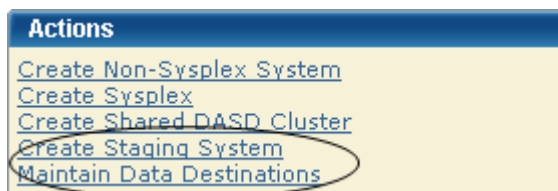
4. Click Add.
The Pick Data Destination dialog appears.
5. Select the data destinations you want to add and click Select.
The data destinations are added to the system.

Maintain Data Destinations

You can maintain, [delete](#) (see page 86), or [create](#) (see page 82) data destinations.

Follow these steps:

1. Click the System Registry tab, and in the Actions section, click the Maintain Data destinations link.



The Maintains Data Destinations dialog appears.

Note: A grayed select box indicates that the data destinations is assigned and cannot be removed. It can be edited.

2. Select Edit from the Actions drop-down list for the data destination you want to change.

The Edit Data Destinations dialog appears.

Note: The asterisk indicates that the field is mandatory.

3. Update the following and click Save:

Name

Enter a meaningful Name.

Limits: Maximum 64 characters.

Note: Each data destination name must be a unique name and it is not case-sensitive. For example DATAD1 and datad1 are the same data destination name.

Description

Enter the description.

Limits: Maximum 255 characters.

Transmission Method

Select the transmission method.

Default: Shared DASD.

Mount Point

(Shared DASD only) Enter the mount point directory path, which is a directory path that must exist on the target system. The user that is doing the deployment must have write permission to this directory, as well as mount authorization on the target system.

Note: A mount user must have UID(0) or at least have READ access to the SUPERUSER.FILESYS.MOUNT resource found in the UNIXPRIV class.

Limits: Maximum 120 characters

Note: SMS is not mutually exclusive with non-SMS. They can both be specified (usually one or the other is specified though). This is where you specify allocation parameters for the deployment on a target system.

Storage Class

(Shared DASD only) Enter the Storage Class.

Limits: Maximum 8 characters

Example: SYSPRG

VOLSER

(Shared DASD only) Enter the Volser.

Limits: Maximum 6 characters

Example: SYSP01 and SYSP02

GIMUNZIP Volume

Enter the GIMUNZIP volume.

Limits: Maximum 6 characters

zFS Candidate Volumes

Enter [zFS Candidate volumes](#) (see page 76).

Limits: Maximum 6 characters

The zFS candidate volumes let you specify an optional list of VOLSERS used during the allocation of zFS container data sets for USS parts.

The updated data destination appears on the list of data destinations.

Note: Click Cancel to withdraw this change request.

Set a Default Data Destination

You can set a default for a current data destination.

Follow these steps:

1. Click the System Registry tab, and select Non-Sysplex Systems, Sysplexes, or Shared DASD Clusters from the tree on the left side.
Information about the systems you selected appears on the right side.
2. Select the system link to which you want to set the data destination default.
Detailed information about the system appears on the right side.
3. Click the Data Destination tab.
The Data Destination window appears.
4. Select the data destination that you want as the default.
5. In the Action field, select Set as Default.
The word *Default* appears in the Default column.

Delete Data Destinations

You can delete current data destinations that have *not* been assigned.

Important: A grayed selection field indicates that the data destination is assigned and it cannot be deleted. The field can be edited.

Follow these steps:

1. Click the System Registry tab, and select Non-Sysplex Systems, Sysplexes, or Shared DASD Clusters from the tree on the left side.
Information about the systems that you selected appears on the right side.
2. Select the system where you want to delete a data destination.
Detailed information about the system appears on the right side.
3. Click the Data Destination tab.
The Data Destination window appears.
4. Click the Select field for each data destination you want to remove, click Remove, and then click OK to confirm.
The data destination is deleted from this system.

Remote Credentials

The Remote credentials page sets up remote credentials accounts by owner, remote user ID, and remote system name. Use the Apply button to apply and save your changes.

Important! Remote Credentials are validated during the deployment process when deploying to a nonstaging system. The user is responsible for having the correct owner, remote user ID, remote system name, password, and authenticated authorization before creating a new remote credential.

You can [add](#) (see page 87), [edit](#) (see page 88), or [delete](#) (see page 89) remote credentials.

Add Remote Credentials

Follow these steps:

1. Click the Settings tab, and select Remote Credentials from the tree on the left side. Detailed information appears on the right side.
2. In the Remote Credentials Accounts panel, click New. The New Remote Credential dialog appears.
3. Enter the following, and click OK:

Note: The asterisk indicates that the field is mandatory.

Remote User ID

Enter a correct remote user ID.

Limits: 64 characters

Remote System Name

Enter a remote system name.

Limits: Eight characters

Note: A remote credential default can be set up by creating a remote credential without the system name. This default would be for the user creating these remote credentials only.

Password

Enter a correct password.

Limits: 2 to 63 characters

Note: The password is case-sensitive. Verify that your password follows the correct case-sensitive rules for your remote system.

Confirm Password

Enter the correct confirm password.

Limits: 2 to 63 characters

Note: The password is case-sensitive. Verify that your password follows the correct case-sensitive rules for your remote system.

The remote credential entry appears on the Remote Credentials list.

4. Click Apply.

Your changes are applied.

Edit Remote Credentials

You can edit remote credentials.

Important! Remote Credentials are validated during the deployment process when deploying to a nonstaging system. The user is responsible for having the correct owner, remote user ID, remote system name, password, and authenticated authorization before creating a new remote credential.

Follow these steps:

1. Click the Setting tab, and select Remote Credentials from the tree on the left side.
Detailed information appears on the right side.
2. In the Actions drop-down list, click Edit for the remote credential you want to edit.
The Edit Remote Credential window appears.
3. Update the following and click OK:

Note: The asterisk indicates that the field is mandatory.

Remote User ID

Enter a correct remote user ID.

Limits: Maximum 64 characters.

Remote System Name

Enter a correct remote system name.

Limits: Maximum 8 characters.

Example: RMinPlex

Note: A remote credential default can be set up by creating a remote credential without the system name. This default would be for the user creating this remote credentials only.

Password

Enter a correct password.

Limits: Minimum 2 characters and Maximum 63 characters.

Note: Password is case sensitive, make sure that your password follows the correct case sensitive rules for your remote system.

Confirm Password

Enter the correct confirm password.

Limits: Minimum 2 characters and Maximum 63 characters.

Note: Password is case sensitive, make sure that your password follows the correct case sensitive rules for your remote system.

The remote credential entry appears on Remote Credentials list.

4. Click Apply

Your changes are applied.

Delete Remote Credentials

You can delete remote credentials.

Follow these steps:

1. Click the Setting tab, and select Remote Credentials from the tree on the left side.
Detailed information appears on the right side.
2. In the Actions drop-down list, click Delete for the remote credential you want to delete.
A Delete Confirmation window appears.
3. Click OK.
The remote credential is deleted.

Deploying Products

This section includes information about how to use CA MSM to deploy products.

A *deployment* is a CA MSM object that you create to deploy libraries and data sets using a process that copies target libraries defined to SMP/E and user data sets across both shared DASD and networked environments.

Deployment Status

Deployments exist in different statuses. Actions move deployments from one status to another. You can use the following available actions for each of the following deployment statuses.

Under Construction

The user is constructing the deployment.

Available Actions: All but Confirm

Snapshot in Progress

Snapshot is in Progress

Available Actions: Reset Status

Snapshot in Error

Snapshot failed

Available Actions: All but Confirm

Snapshot Completed

Snapshot Succeeded

Available Actions: Delete, Preview, Transmit, Deploy

Note: At this point, no editing, adding, or removing of products or systems is allowed.

Transmitting

The deployment archives are being transmitted using the FTP procedure.

Available Actions: Reset Status

Transmission Error

Transmission Failed

Available Actions: Delete, Preview, Transmit, Deploy

Transmitted

The deployment archives have been transmitted.

Available Actions: Delete, Preview, Deploy

Deploying

The deployment archives are being deployed.

Available Actions: Reset Status

Deploying Error

Deployment failed

Available Actions: Delete, Preview, Deploy

Deployed

The target libraries were deployed.

Available Actions: Delete, Summary, Confirm

Complete

The deployment is complete.

Available Actions: Delete, Summary

Creating Deployments

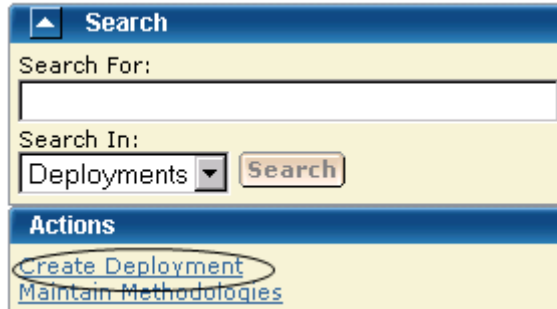
The deployment creation process consists of the following steps:

1. [Initiate deployment creation](#) (see page 92).
2. [Define a name and description](#) (see page 92).
3. [Select an SMP/E environment](#) (see page 93).
4. [Select a product](#) (see page 93).
5. [Select a custom data set](#) (see page 94).
6. [Select a methodology](#) (see page 94).
7. [Select a system](#) (see page 96).
8. [Preview and save](#) (see page 96).

Initiate Deployment Creation

You can create a new deployment by using the New Deployment wizard.

To initiate deployment creation, click the Deployments tab, and then in the Actions section, click the Create Deployment link.



The New Deployment wizard opens to the Introduction step.

Note: When creating a deployment, you can save this deployment at any step in this wizard. This "under construction" deployment is added to the current deployments list. You can [maintain this deployment](#) (see page 97) until a successful snapshot has been created.

Define Name and Description

When you create a deployment, you begin by defining the name and description so that it will be known and accessible within CA MSM.

Note: The asterisk indicates that the field is mandatory.

Follow these steps:

1. On the Introduction step, enter a meaningful deployment name.

Limits: Maximum 64 characters.

Note: Each deployment name must be unique and it is not case-sensitive. For example, DEPL1 and depl1 are the same deployment name.

2. Enter the description of this deployment.

Limits: Maximum 255 characters.

3. Click Next.

The CSI Selection step appears.

Note: When creating a deployment, you can save this deployment at any step in this wizard. This "under construction" deployment is added to the current deployments list. You can [maintain this deployment](#) (see page 97) until a successful snapshot has been created.

Select a CSI

After you define the name and description, you select a CSI for the deployment.

Follow these steps:


1. On the CSI Selection step, in CSIs to Deploy, click the CSI you want to select.
The CSI selections listed are preselected from the SMP/E Environments page.
2. Click Next.
The Product Selection step appears.

Note: When creating a deployment, you can save this deployment at any step in this wizard. This "under construction" deployment is added to the current deployments list. You can [maintain this deployment](#) (see page 97) until a successful snapshot has been created.

Select a Product

After you select a CSI for the deployment, you select a product for the deployment.

Follow these steps:

1. On the Product Selection step, select a product from the list.
Note: If you cannot select the product or product feature from the list, it is for one of the following reasons:
 - The product or feature is not deployable for the selected CSI.
 - The product feature is part of a product that you must select first.If a feature is mandatory for the selected product, the corresponding check box is also selected and disabled, and you cannot deselect the feature from the list.
2. If there is a  text icon in the Text column, click it to read the instructions supplied by CA Support for product, data set, and other necessary information.
3. Click the check box *I have read the associated text*, and click Next. The Next button is disabled until you click the check box.

Note: If there are no products displayed, the appropriate PTF that enables your products' deployment through metadata has not been installed.

The Custom Data Sets step appears.

Note: When creating a deployment, you can save this deployment at any step in this wizard. This "under construction" deployment is added to the current deployments list. You can [maintain this deployment](#) (see page 97) until a successful snapshot has been created.

Select a Custom Data Set

A *custom data set* is a data set that contains either a z/OS data set or USS path.

Follow these steps:

1. On the Custom Data Sets step, select a custom data set from the list and click Select.

Note: To add a new custom data set, click Add Data Set and [enter the custom data set information](#) (see page 109).

2. Click Next.

The Methodology Selection step appears.

Note: When creating a deployment, you can save this deployment at any step in this wizard. This "under construction" deployment is added to the current deployments list. You can [maintain this deployment](#) (see page 97) until a successful snapshot has been created.

More information:

[Add a Custom Data Set](#) (see page 109)

Select a Methodology

After you select a custom data set, you select a methodology, which lets you provide a single data set name mask that is used to control the target library names on the target system.

Follow these steps:

1. On the Methodology Selection step, select a Methodology from the list.

2. (Optional) Click the Create button and [enter the new methodology information](#) (see page 116).

New Deployment

1 Introduction 2 CSI Selection 3 Product Selection 4 Custom Data Sets 5 **Methodology Selection** 6 System Selection 7 Preview

Methodologies are named object with a description they provide the how of deployments. They have a single data set name mask that is used to control which target libraries are called on the target system. Select the applied methodology.

Methodologies Create

1 - 5 of 44

Select	Name	Description	DSN Mask
<input type="radio"/>	Method1	Methodology	&SYSID
<input type="radio"/>	Method2	Method2f	&MSMDID
<input type="radio"/>	Method3	Methodology for West	&SYSUID..&MSMDID.
<input type="radio"/>	Method4	CAPRODS.R12.CAEVENT	CARPRODS.&SYSID.&MSMD
<input type="radio"/>	Method5	Method for Test Environment	&SYSUID..&MSMDID.

Save Back Next Deploy Cancel Help

3. Click Next.

The System Selection step appears.

Note: When creating a deployment, you can save this deployment at any step in this wizard. This "under construction" deployment is added to the current deployments list. You can [maintain this deployment](#) (see page 97) until a successful snapshot has been created.

More information:

[Create a Methodology](#) (see page 116)

Select a System

After you select a methodology, you select a system.

Follow these steps:

1. On the System Selection step, select the systems to be deployed.

Note: When two systems have the same name, use the description to differentiate between these systems.

Sysplex systems are denoted by *sysplex system:system name*. For example, PLEX1:CO11, where PLEX1 is the sysplex system, and CO11 is the system name.

2. Click Next.

The Preview step appears.

Note: When creating a deployment, you can save this deployment at any step in this wizard. This "under construction" deployment is added to the current deployments list. You can [maintain this deployment](#) (see page 97) until a successful snapshot has been created.

Preview and Save the Deployment

After you select a system, you are ready to preview the deployment, and then save or deploy it.

- To save the deployment, click Save.
- To set up the deployment, click Deploy.

Note: Click Cancel to exit the wizard without saving.

The Preview identifies the deployment and describes the products, systems, means of transport, and target libraries (including source, target, and resolution), as well as the SMP/E environment and snapshot information.

Important! Data sets may need to be APF-authorized and added to the Link List and Link Pack Area. These data sets are identified in this dialog.

Note: ??? in the Preview indicates that CA MSM has yet to assign this value.

View a Deployment

To view a deployment, click the Deployments tab, and select the current or completed deployment from the tree on the left side. The detailed deployment information appears on the right side.

Change Deployments

You can change deployments any time before you snapshot the deployment.

Important! Each deployment must have at least one product defined, at least one system defined, and a methodology defined.

Follow these steps:

1. Click the Deployments tab. The Deployment window appears.
2. On the right, in the Deployments panel click the current deployment link.
The detailed deployment information appears.
3. Click the Deployment Name link for the Deployment you want to change.

This deployment's window appears.

Change the information on this window as needed. Each deployment name must be unique and it is not case-sensitive. For example DEPL1 and depl1 are the same deployment name.

Note: The methodology provides the means for deployment. It is used to control the target library names on the target system.

[There are actions that you can perform based on Deployment State](#) (see page 90).

4. To change a methodology, select a methodology from the drop-down list and click Edit.

The [Edit Methodology window](#) (see page 129) appears. The Deployment ID is the value of the MSMID variable.

Note: You can perform the following actions:

- You can [select](#) (see page 106), [add](#) (see page 107), or [remove](#) (see page 107) a product.
 - You can [select](#) (see page 133), [add](#) (see page 133), or [remove](#) (see page 134) a system.
 - You can [select](#) (see page 108), [add](#) (see page 109), or [remove](#) (see page 115) a custom data set.
5. Click Save on the Deployment Details window.

6. Click Actions drop-down list to do one of the following:

Preview (Summary)

Note: This action button changes to Summary after a successful deploy.

Generates a list of the following current information:

- Deployment's ID
- Name
- Products
- Systems
- Transport information
- Target libraries including: source, target, and resolved data set names.
- SMP/E environment
- Snapshot path and container

Snapshot

Takes a snapshot of the current deployment.

A *snapshot* of the set of target libraries is taken by CA MSM, by utilizing the IBM supplied utility GIMZIP to create a compressed archive of these libraries, along with a list of applied maintenance. The SMP/E environment is "locked" during this archive creation process to insure the integrity of the archived data.

Transmit

Transmit enables a customer to take their CA MSM installed software and copy it onto systems across the enterprise through FTP, in preparation for a subsequent deployment.

Deploy

Combines the snapshot, transmit, and deploy action into one action.

Confirm (see page 104)

Confirms that the deployment is complete. This is the final action by the user.

Note: A deployment is not completed until it is confirmed. Once it is confirmed the deployment moves to the Confirmed deployment list.

Delete

Deletes deployment and its associated containers, folders, and files. This does not include the deployed target libraries on the end systems. See [delete a deployment](#) for a list of deleted files.

Note: A deployment's deletion does not start until it is confirmed.

[Reset Status](#) (see page 102)

You can reset a deployment status when the deployment has a status of *snapshot in progress*, *transmitting*, or *deploying*. See [reset status](#) (see page 102) for a list of deleted files.

7. Click Save on the Deployment Details window.

Your changes are saved.

Deployment Maintenance

You can maintain a deployment in the following ways:

- Adding
 - [System](#) (see page 133)
 - [Product](#) (see page 107)
 - [Custom data sets](#) (see page 109)
- Delete
 - Deployment
- Removing
 - [System](#) (see page 134)
 - [Product](#) (see page 107)
 - [Custom data sets](#) (see page 115)
- Editing
 - [Maintain deployments](#) (see page 97)
 - [Edit a custom data set](#) (see page 112)
 - [Edit a methodology](#) (see page 129)
- Viewing
 - [System](#) (see page 133)
 - [Product](#) (see page 106)
 - [Custom data sets](#) (see page 108)

Failed Deployments

When a deployment fails, you investigate, correct, and deploy again. Use the following procedures in this section:

- [Investigate a Failed Deployment Using the Tasks Page](#) (see page 100)
- [Download a Message Log](#) (see page 74)
- [Save a Message Log as a Data Set](#) (see page 75)
- [View Complete Message Log](#) (see page 75)

Note: A deployment is processed in steps and in order as listed in the Deployment window. Each step must pass successfully before the next step is started. If a step fails, the deployment fails at that step, and all steps after the failed step are not processed.

More information:

[Download a Message Log](#) (see page 74)

[Save a Message Log as a Data Set](#) (see page 75)

[View Complete Message Log](#) (see page 75)

Investigate a Failed Deployment

When a deployment fails, you investigate, correct, and deploy again.

Follow these steps:

1. On the Deployments Page, in the left hand column, find the deployment with an error and note its name.
2. Click the Tasks tab and then click Task History.

Note: Click Refresh on the right hand side of the Task History bar to refresh the Task History display.

3. At the Show bar, select All tasks, or select My tasks to only see the tasks assigned to you.

Note: You can refine the task list further by selecting task and status types from the drop-down lists, and then sort by Task ID.

- Find the failed deployment step and click the link in the Name column.

The Task Output Browser appears.

#	Name	Description	Status
1	Validate deployable state	Validate that the deployment is in a state that can be deployed	Succeeded
2	Deployment Update Status: Snapshot In Progress	Update the deployment status of the deployment	Succeeded
3	Validate remote systems	Validate that the remote systems are valid, including contact systems	Succeeded
4	Lock CSIs in deployment	Serialize access to the CSIs in this deployment	Failed
5	Validate deployment	Validate the deployment settings	Not Started
6	Archive creation	Creating archives for products	Not Started
7	SYSMODS Extraction	Extracting SYSMODS from CSIs	Not Started
8	Freeze deployment	Creating a permanent location for this deployment	Not Started
9	Record target library names	Record the target libraries used by the deployment	Not Started
10	Unlock CSIs in this deployment	Release the serialization of CSIs in this deployment	Not Started
11	Deployment Update Status: Snapshot Completed	Update the deployment status of the deployment	Not Started
12	Deployment Update Status: Deploying	Update the deployment status of the deployment	Not Started
13	Deploy Products	Deploy the product libraries on the target systems	Not Started
14	Deployment Update Status: Deployed	Update the deployment status of the deployment	Not Started

- Click the link in the Name column to view the results, and click on the messages logs to review the details for each error.

Note: You can analyze the error results and determine the steps required to troubleshoot them.

- Correct the issue and deploy again.

More information:

[Download a Message Log](#) (see page 74)

[Save a Message Log as a Data Set](#) (see page 75)

[View Complete Message Log](#) (see page 75)

Download a Message Log

You can save the message log in the following ways:

- To download a zipped file of all the text messages for this validation, click the Deployment Name on the top left tree. Click the Download Zipped Output button on the General menu bar. Save this file.
- To download as TXT, click the Deployment Name or the Deployment Results on the left tree. Click the Action button on the Message Log bar and click the Download as TXT. Save this file.
- To download as ZIP, click the Deployment Name or the Deployment Results on the left tree. Click the Action button on the Message Log bar and click the Download as ZIP. Save this file.

Save a Message Log as a Data Set

You can save a message log as a data set.

Follow these steps:

1. Click the Deployment Name or the Deployment Results on the left tree. Click the Action button on the Message Log bar, and click the Save as Data Set.

The Save Output as Data Set dialog appears.

Note: This information is sent to CA Support to analyze the failed deployment.

Note: The asterisk indicates that the field is mandatory.

2. Enter the following information and click OK:

Data Set Name

Enter a data set name. CA MSM generates a value.

VOLSER

For non-SMS data, enter the Volser.

Example:

Volser: SYSP01 and SYSP02

Storage Class

For SMS Allocation data, enter the Storage Class.

The message log is saved as a data set.

View Complete Message Log

To view the complete message log for a failed validation, click Show All.

Note: To close the message log, click Close.

Reset Deployment Status

You can reset a deployment status when the deployment has a status of *snapshot in progress*, *transmitting*, or *deploying*. The message log explains if any containers, folders, and files were deleted during reset.

You can also [investigate a failed deployment](#) (see page 73) to see additional details in the message log.

The following statuses may be reset.

Snapshot in progress

Snapshot in progress is reset to *snapshot in error*.

Transmitting

Transmitting is reset to *transmit in error*.

Deploying

Deploying is reset to *deploy in error*.

The following artifacts are reset by status.

Snapshot in Progress

Archive located at Application Root/sdsroot/Dnnnn, where nnnn = Deployment ID automatic number. Application Root is defined in settings under mount point management,

Temp files located at Application Root/sdsroot/Deployment_nnnn, where nnnn = Deployment ID automatic number.

Transmit in Progress

Nothing is reset.

Deploy in Progress

Nothing is reset.

Delete a Deployment

You can delete deployments.

Note: You cannot delete deployments that are currently being deployed.

A deployment deletion must be confirmed before a deletion starts.

Note: If system information was changed, not all files may be deleted. In this case, you may need to delete these files manually. For example, if an FTP transmission was changed to a Shared DASD Cluster or if the remote credentials are incorrect or changed.

The message log explains which containers, folders, and files were deleted during processing and which ones were not deleted. See how to [investigate a failed deployment](#) (see page 73) for details on finding the message log.

Note: Target libraries are never deleted.

The following artifacts are deleted by status:

Under Construction

All applicable database records

Snapshot in Error

All applicable database records

Snapshot Completed

Archive located at Application Root/sdsroot/Dnnnn where *n* = Deployment ID automatic number. Application Root is defined in settings under mount point management.

All applicable database records.

Transmit in Error

Same as Snapshot Completed, plus attempts to delete any transmitted snapshots on target systems.

Transmitted

Same as Transmit in Error.

Deploy in Error

Same as Transmitted.

Deployed

Same as Snapshot Completed.

Complete

Same as Snapshot Completed.

Follow these steps:

1. Click the Deployments tab.
The Deployment window appears.
2. On the right, in the Deployments panel, click the Current Deployments or Complete Deployments link.
The detailed deployment information appears.
3. Click the deployment name link, and from the Actions drop-down list, select Delete, and then click OK to confirm.
The deployment is deleted.

Confirm a Deployment

You can use this procedure to confirm that the deployment is complete.

Note: A deployment is not completed until it is confirmed. After it is confirmed, the deployment moves to the Completed deployment list.

Important! Data sets may need to be APF-authorized and added to the Link List and Link Pack Area. These data sets are identified in this dialog.

Follow these steps:

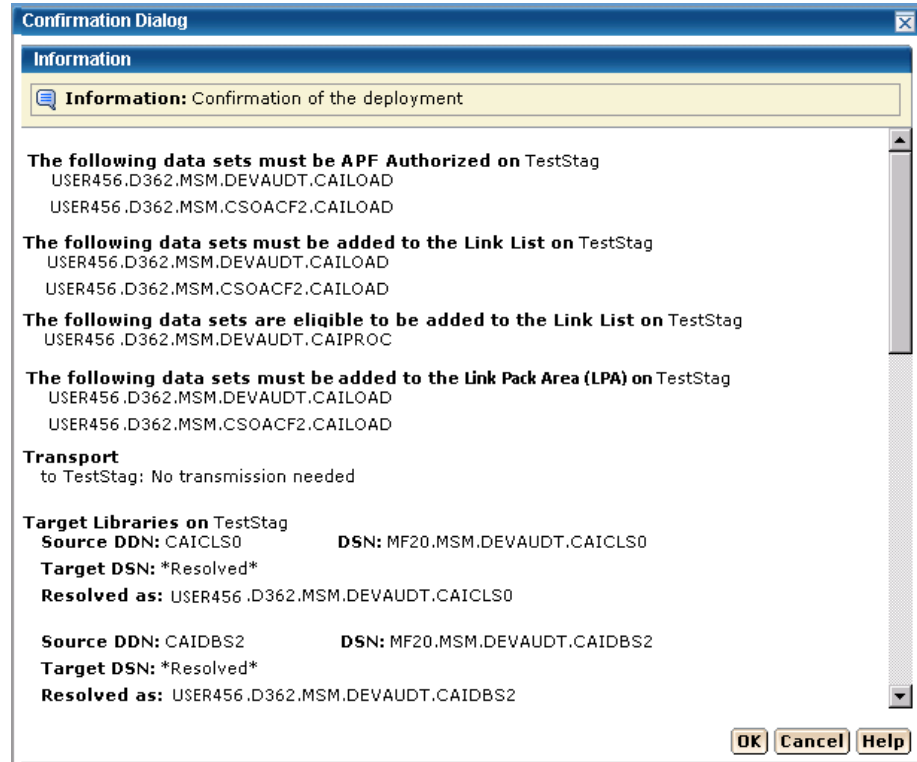
1. Click the Deployments tab.
The Deployment page appears.
2. Click Confirm.
The Confirmation dialog appears.
3. Review the confirmation.
4. Click OK when the deployment is correct.

Note: Click Cancel to exit this procedure without confirming.

The Deployment Summary window may contain the following:

- Deployment's ID
- Name
- Products
- Systems
- Data Sets actions
- Transport information
- Target libraries including: source, target, and resolved data set names.
- SMP/E environment
- Snapshot path and container

The following example shows the Data Sets actions, Transport, and Target libraries information.



Products

You can view, add, and remove products from a deployment.

View the Product List

You can view a product.


Follow these steps:

1. Click the Deployments tab.
2. Select the current deployment from the tree on the left side.
The detailed deployment information appears on the right side.

Add a Product

You can add a product to a deployment.

Follow these steps:

1. Click the Deployments tab. The Deployments window appears.
2. On the right, in the Deployments panel click the Current Deployment link.
A list of current deployments appears.
3. Click the deployment name link.
4. In the Product List panel click Add Products.
The Add Products wizard appears.
5. Select a CSI and click Next.
The Product Selection appears.
6. Select a product.
7. If there is a  text icon in Text column, click the text icon to read the instructions supplied by CA Support for product, data sets, and other necessary information.
8. Click the "I have read the associated text by selecting the text icon from the list about" box. This box appears only if there is a text icon.
Note: You will not be able to click Next until you click this box.
9. Click Next.
The Custom Data Set Selection appears
10. If needed, select or [add a custom data set](#) (see page 109).
11. Click Add Products.
The Product is added.

Remove a Product

You can remove a product from a deployment.

Note: This product will no longer be associated with the current deployment.

Follow these steps:

1. Click the Deployments tab. The Deployment window appears.
2. On the right, in the Deployments panel click the Current Deployment link.
A list of current deployments appears.
3. Select the deployment that you want to remove the product from.

4. In the Product List panel, select a product to remove.
5. Click the Remove link.
6. Click OK to the Remove Products confirmation window.
The product is removed.

Custom Data Sets

You can view, [add](#) (see page 109), [edit](#) (see page 112), and [remove](#) (see page 115) custom data sets from a deployment.

A *custom data set* is a data set that contains either a z/OS data set or USS path.

- For a z/OS data set, you need to provide a data set name that is the actual existing z/OS data set and a mask that names the data set on the target system. This mask may be set up using [symbolic qualifiers](#) (see page 119) and must be available to CA MSM. During the deployment process, the custom data set is accessed and copied to the target system the same way a target library is accessed and copied.
- For USS parts, you need to provide a local path, a remote path (which may be set up using [symbolic qualifiers](#) (see page 119)), and a type of copy. The type of copy can be either a container copy or a file-by-file copy.

View Custom Data Sets

You can view custom data sets.

Follow these steps:

1. Click the Deployments tab, and select the current deployment from the tree on the left side.

The detailed deployment information appears on the right side.

Product Name Sort Arrows

Click the up arrow to place the product names in alphabetic order or click the down arrow to place them in reverse alphabetic order.

Add a Custom Data Set

You can add custom data sets to a deployment.

Follow these steps:

1. Click the Deployments tab.
The Deployments window appears.
2. On the right, in the Deployments panel, click the Current Deployment link.
A list of current deployments appears.
3. Click the deployment name link.
4. In the Custom Data Sets List panel, click Add Data Sets.
The Add Custom Data Sets dialog appears.
Note: The asterisk indicates that the field is mandatory.
5. Select a Product from the drop-down list.
Note: When there are instructions, they are required and supplied by CA Support.
6. Select the Data Set Type, either data set (step 7) or USS (step 10).
Default: data set
7. For data set, enter the data set name.
Limits: Maximum 44 characters.
Note: This is the existing z/OS data set name that you want CA MSM to include in the deployment when it is deployed on the target systems.
8. Enter the data set name mask, click the file icon, and select a [symbolic name](#) (see page 119).

Mask

This is the mask that will be used to name the data sets that are being deployed. They can contain [symbolic qualifiers](#) (see page 119). For example, if you enter CAPRODS.&SYSID, the &SYSID is replaced by its values, and if the SYSID that is being deployed to is XX16, the DSN mask will be CAPRODS.XX16

Limits: Maximum 64 characters.

Note: Each deployed target data set is named using the resolved content of the data set name mask followed by the low-level qualifier of the source data set. Appending the low-level qualifier from the source data set helps ensure uniqueness of the final data set name. Verify that the mask that you entered does not exceed 35 characters when it is translated.

The mask consists of one or more qualifiers that are separated by periods. The maximum number of characters is 64, including the periods. While you are entering the mask, CA MSM validates the mask by replacing symbolics with the minimum possible values first, and then with the maximum values. If the validation with the minimum possible values fails, an error message appears at the top of the dialog, and you cannot proceed. If the validation with the maximum values fails, a warning message appears, and you can proceed.

When the mask is translated, it has a maximum length of 44 characters including the periods and the low-level qualifier from the source data set. The low-level qualifier from the source data set has a maximum length of nine characters including a period.

-

Two consecutive periods are required to separate the two masks.

9. Enter the Mask and click OK.
10. For USS data set type, enter the Local Path. The local path is the directory are where files are to be copied from.
Limit: Maximum 255 characters.
Note: The asterisk indicates that the field is mandatory.
11. Enter the Remote Path and/or click the file icon and select a [symbolic name](#) (see page 119). The remote path is the path where the files are to be copied to.
Limit: Maximum 255 characters.
12. Select the Type of Copy:
 - If you select Container Copy, proceed to step 14.
 - If you select File-by-file Copy, proceed to step 15, and ensure that the USS path exists on all of the remote systems of this deployment, and that there is sufficient space to hold these target libraries.
Default: Container Copy
13. Click OK.
14. For Container Copy, enter the container name and/or click the file icon and select a [symbolic name](#) (see page 119).
Limit: Maximum 64 characters.
Note: It consists of one or more qualifiers separated by periods, and has a maximum input length of 64 characters, including the periods. When it is translated, it has a maximum length of 44 characters, including the periods.

Note: For Container Copy, the following occurs during the deployment process:

- a. A file system of the requested type is created.
- b. The size of the file system is computed as follows:
 - The size of all of the constituent files and directories in the local path are added up as bytes.
 - These bytes are converted to tracks and used as the primary allocation value.
 - If there is a non-zero percent of free space entered, it is used to calculate the secondary allocation.
- c. All of the directories in the mount point are dynamically created.
- d. The file system is mounted at the requested mount point.

Note: The mount is not permanent. You will need to update your BPXPARMS to make this mount point permanent.

- e. The content from the local path is copied into the newly created and mounted file system.

Note: The asterisk indicates that the field is mandatory.

15. Select the Type of Container from the drop-down list.

16. Enter the Mount Point and/or click the file icon and select a [symbolic name](#) (see page 119).

Limit: Maximum 255 characters.

Note: The container is created and it is mounted at a position in the USS file system hierarchy. The place in the hierarchy where it is mounted is known as that container's mount point. Most nodes in the USS file system can be mount points, for any one container.

17. Enter the percentage of Free Space needed.

The percentage of free space is the amount of space to leave in the file system, after the size has been computed. This is done by specifying secondary space on the allocation. For example, the computed space was determined to be 100 tracks. Then 35 would be 35% free space and the space allocations would be in tracks, 100 primary 35 secondary. While 125 would be 125% over and allocation would be in tracks, 100 primary 125 secondary.

Limit: 0 to 1000.

18. Click OK.

The custom data set is added.

Edit a Custom Data Set

You can edit a custom data set.

Follow these steps:

1. Click the Deployments tab.
The Deployments page appears.
2. On the right, in the Deployments panel, click the Current Deployment link.
A list of current deployments appears.
3. Click the deployment name link.
4. In the Custom Data Sets List panel, click the Actions drop-down list and click Edit.
The Edit Custom Data Sets dialog appears.

Note: The asterisk indicates that the field is mandatory.

5. Select a Product from the drop-down list.
Note: When there are instructions, they are required and supplied by CA Support.
6. Select the Data Set Type, either data set (step 7) or USS (step 10).

Default: data set

7. For data set, enter the data set name.

Limits: Maximum 44 characters.

Note: This is the existing z/OS data set name that you want CA MSM to include in the deployment when it is deployed on the target systems.

8. Enter the data set name mask, click the file icon, and select a [symbolic name](#) (see page 119).

Mask

This is the mask that will be used to name the data sets that are being deployed. They can contain [symbolic qualifiers](#) (see page 119). For example, if you enter CAPRODS.&SYSID, the &SYSID is replaced by its values, and if the SYSID that is being deployed to is XX16, the dsn mask will be CAPRODS.XX16

Limits: Maximum 64 characters.

Note: Each deployed target data set is named using the resolved content of the data set name mask followed by the low-level qualifier of the source data set. Appending the low-level qualifier from the source data set helps ensure uniqueness of the final data set name. Verify that the mask that you entered does not exceed 35 characters when it is translated.

The mask consists of one or more qualifiers that are separated by periods. The maximum number of characters is 64, including the periods. While you are entering the mask, CA MSM validates the mask by replacing symbolics with the minimum possible values first, and then with the maximum values. If the validation with the minimum possible values fails, an error message appears at the top of the dialog, and you cannot proceed. If the validation with the maximum values fails, a warning message appears, and you can proceed.

When the mask is translated, it has a maximum length of 44 characters including the periods and the low-level qualifier from the source data set. The low-level qualifier from the source data set has a maximum length of nine characters including a period.

-

Two consecutive periods are required to separate the two masks.

9. Enter the Mask and click OK.
10. For USS data set type, enter the Local Path. The local path is the directory where files are to be copied from.
Limit: Maximum 255 characters.
Note: The asterisk indicates that the field is mandatory.
11. Enter the Remote Path and/or click the file icon and select a [symbolic name](#) (see page 119). The remote path is the path where the files are to be copied to.
Limit: Maximum 255 characters.
12. Select the Type of Copy:
 - If you select Container Copy, proceed to step 14.
 - If you select File-by-file Copy, proceed to step 15, and ensure that the USS path exists on all of the remote systems of this deployment, and that there is sufficient space to hold these target libraries.
Default: File-by-file Copy
13. Click OK.
14. For Container Copy, enter the container name and/or click the file icon and select a [symbolic name](#) (see page 119).
Limit: Maximum 64 characters.

It consists of one or more qualifiers separated by periods, and has a maximum input length of 64 characters, including the periods. When it is translated it has a maximum length of 44 characters including the periods.

For container copy the following occurs during the deployment process:

- a. A file system of the requested type is created
- b. The size of the file system is computed as follows:
 - The size of all of the constituent files and directories in the local path are added up as bytes.
 - These bytes are converted to tracks and used as the primary allocation value
 - If there is a non-zero percent of free space entered, it is used to calculate the secondary allocation.
- c. All of the directories in the mount point will be dynamically created.
- d. The file system will be mounted at the requested mount point
Note: The mount is not permanent. You will need to update your BPXPARMS to make this mount point permanent.
- e. The content from the local path will be copied into the newly created and mounted file system.

Note: The asterisk indicates that the field is mandatory.

15. Select the Type of Container from the drop down list.

16. Enter the Mount Point and/or click the file icon and select a [symbolic name](#) (see page 119).

Limit: Maximum 255 characters.

Note: The container is created and it is mounted at a position in the USS file system hierarchy. The place in the hierarchy where it is mounted is known as that container's mount point. Most nodes in the USS file system can be mount points, for any one container.

17. Enter the percentage of Free Space needed.

The percentage of free space is the amount of space to leave in the file system, after the size has been computed. This is done by specifying secondary space on the allocation. For example, the computed space was determined to be 100 tracks. Then 35 would be 35% free space and the space allocations would be in tracks, 100 primary 35 secondary. While 125 would be 125% over and allocation would be in tracks, 100 primary 125 secondary.

Limit: 0 to 1000.

18. Click OK.

The custom data set is changed.

Remove a Custom Data Set

You can remove a custom data set from a deployment.

Note: This data set will no longer be associated with the current deployment.

Follow these steps:

1. Click the Deployments tab.
The Deployment page appears.
2. On the right, in the Deployments panel click the Current Deployment link.
A list of current deployments appears.

Product Name Sort Arrows

Click the up arrow to place the product names in alphabetic order or click the down arrow to place them in reverse alphabetic order.

3. Select the custom data set that you want to remove from this deployment.
4. Click the Remove link.
5. Click OK to the Remove Custom Data Set confirmation window.
The custom data set is removed.

Methodologies

You can [create](#) (see page 116), maintain, [edit](#) (see page 129), and [delete](#) (see page 131) methodologies from a deployment.

A methodology has the following attributes:

- A single data set name mask that is used to control what target libraries are to be called on the target systems and where these deployment will go.

z/OS data sets

z/OS data sets use a data set name mask. The data set name mask is a valid data set name comprised of constants and [symbolic qualifiers](#) (see page 119).

The minimum methodology data consists of a data set mask and a target action. The symbolics in the data set mask are either symbolics defined by CA MSM or z/OS system symbolics.

- Deployment Style information is used to *create only* or *create and replace* a methodology.

Create Only

Use *Create Only* when you are creating a new methodology that does not have any target libraries already associated with a deployment.

Create or Replace

Use *Create or Replace* to:

- Create new data sets and/or files in a UNIX directory.
- Replace existing sequential data sets or files in a UNIX directory.
- For partitioned data sets, replace existing members, add new member without deletion of members that are not replaced.

Note: Using *Create or Replace* would not cause the deployment to fail due to data set name conflicts.

Create a Methodology

You can create a methodology.

Note: The asterisk indicates that the field is mandatory.

Follow these steps:

1. Click the Create button, in the Methodology Selection in the New Deployment wizard.

The Create a New Methodology dialog appears.

2. Enter the methodology name.

Limits: Maximum 64 characters.

Note: Each methodology name must be unique and it is not case-sensitive. For example Meth1 and meth1 are the same methodology name.

3. Enter the description of this methodology.

Limits: Maximum 255 characters.

4. Enter the data mask name, click the file icon, and select a [symbolic name](#) (see page 119).

Data Set Name Mask

This is the mask that will be used to name the data sets that are deployed. They can contain [symbolic qualifiers](#) (see page 119). For example, assume you enter, CAPRODS.&SYSID. In this case, the &SYSID. will be replaced by its values. If the SYSID that is being deployed to is X16, the DSN mask will be: CAPRODS.X16

Limits: Maximum 64 characters.

Note: Each deployed target data set is named using the resolved content of the data set name mask followed by the low-level qualifier of the source data set. Appending the low-level qualifier from the source data set helps ensure uniqueness of the final data set name. Verify that the mask that you entered does not exceed 35 characters when it is translated.

The mask consists of one or more qualifiers that are separated by periods. The maximum number of characters is 64, including the periods. While you are entering the mask, CA MSM validates the mask by replacing symbolics with the minimum possible values first, and then with the maximum values. If the validation with the minimum possible values fails, an error message appears at the top of the dialog, and you cannot proceed. If the validation with the maximum values fails, a warning message appears, and you can proceed.

When the mask is translated, it has a maximum length of 44 characters including the periods and the low-level qualifier from the source data set. The low-level qualifier from the source data set has a maximum length of nine characters including a period.

■

5. Select a style of Deployment.

Create only

Creates new data sets.

Note: Prior to creating any data sets on the remote system, a check is made, to see if the data sets already exist. The deployment is not allowed to continue if this occurs.

Create or Replace

Creates new data sets if they do not already exist, or replaces existing data sets.

Partitioned data set

Replaces existing members in a partitioned data set with members that have the same name as the source file. Any currently existing member that is not in the source file will remain in the PDS. Any member from the source that does not already exist in the target PDS will be added to the target PDS.

The amount of free space in the PDS will need to be sufficient to hold the additional content, since no automatic compress will be done.

Directory in a UNIX file system

Replaces files in a directory with files with the same name as the source. Any currently existing directory in a UNIX file system that is not in the source will remain in the UNIX file system.

Sequential data set or a file in the UNIX file system

Replaces the existing data set or file and its attributes with the data from the source file.

For a VSAM data set (cluster)

Populates an existing VSAM cluster with the data from the source file.

Note: The existing VSAM cluster must be of the same type as the source cluster (ESDS, KSDS, LDS, or RRDS), and it must have characteristics that are compatible with the source cluster (such as, record size, key size, and key offset). Replace does not verify the compatibility of these characteristics.

To replace the contents of an existing cluster, the cluster is altered to a reusable state by using an IDCAMS ALTER command, if necessary, before the data from the VSAM source is copied into the cluster by using an IDCAMS REPRO command. The REPRO command will use both the REPLACE and REUSE operands. Following the REPRO operation, the cluster is altered back to a non-reusable state if that was its state to begin with.

6. Click Save.

The methodology is saved.

Note: Click Cancel to close this dialog without saving.

Symbolic Qualifiers

The data set name mask and the directory path contain the following symbolic qualifiers:

Data Set Name Mask

This is a unique name that identifies each data set. It consists of one or more qualifiers separated by periods, and has a maximum input length of 64 characters, including the periods. When the data set name mask is translated it has a maximum length of 44 characters including the periods.

Directory Path

This is a USS path name, it consists of one or more directory leaves separated by forward slashes, and has a maximum input length of 255 characters including slashes. When the Directory Path is translated it has a maximum length of 255 characters.

Symbolic Substitution

Symbolic substitution, or translation, is a process performed by CA MSM to resolve the mask values specified in the data set name mask and directory path, into real names based upon the contents of the symbolic variables at translation time. A CA MSM symbol is defined in the list of symbols. Each symbol begins with an ampersand (&) and ends with a period (.). For example, the symbol &LYMMDD. would be completely replaced with its value at translation time, including the ampersand and trailing period. The trailing period is important and is considered part of the symbolic name.

Symbolic Variables

You can use symbolic variables in the construction of a data set name with the value of the symbolic variable to end a data set name segment.

Example: Assume MSMDID is 255.

SYSWORK.D&MSMDID..DATASET

Note: The double periods are necessary because the first period is part of the symbolic name, and therefore does not appear in the translated value.

The final data set name is SYSWORK.D255.DATASET.

Numeric Values

Some CA MSM symbolic names translate to numeric values. In the case where you want to use one of these symbolic variables in your data set name, you may have to precede it with an alpha constant. This is because z/OS data set naming rules do not allow a data set name segment to start with a numeric.

If you wanted to use a date value in your translated data set name, you could use one of the CA MSM defined date symbolic qualifiers such as &LYYMMDD. You must be careful how you construct the data set mask value.

Example: Assume that you want to have a middle level qualifier to have a unique value based upon the date of April 1, 2010.

Mask = SYSWORK.D&LYYMMDD..DATASET, translates to
SYSWORK.D100401.DATASET

An incorrect specification of the mask would be:

SYSWORK.&LYYMMDD..DATASET, translates to SYSWORK.100401.DATASET.
Because the middle-level qualifier starts with a numeric it is an invalid data set name.

Directory Paths

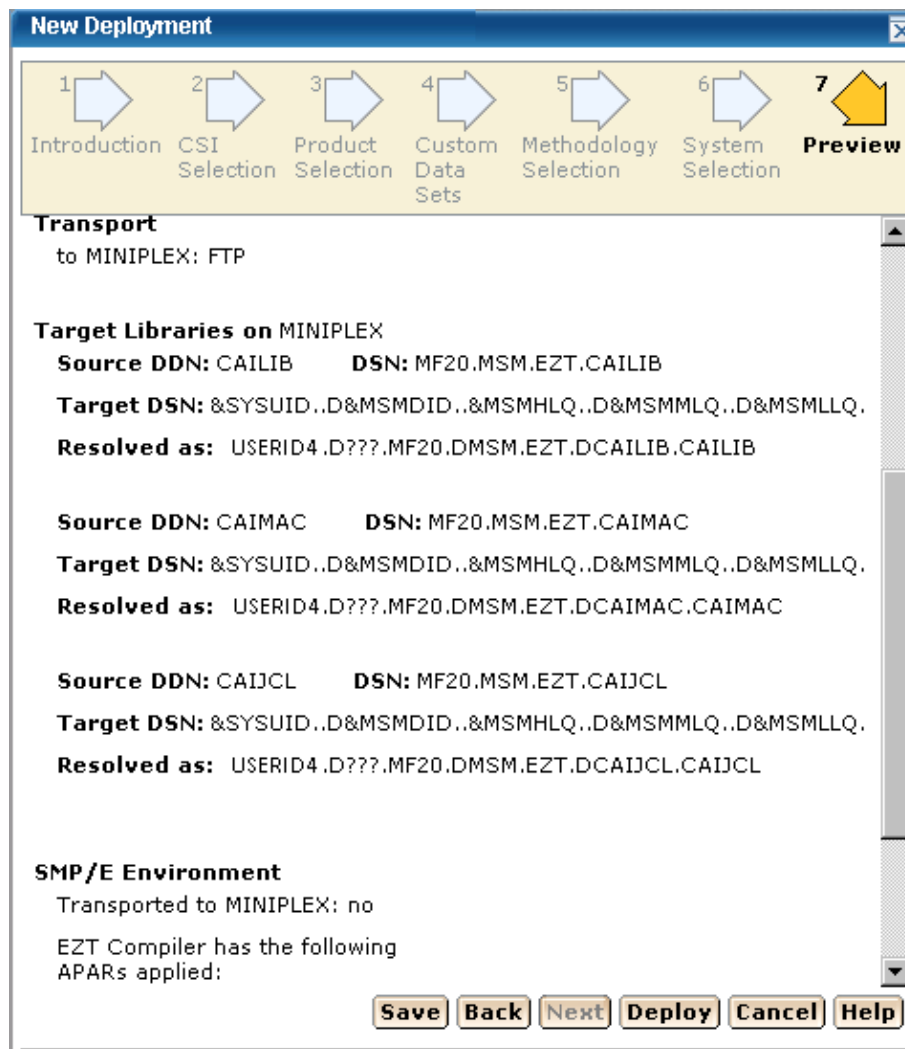
Symbolic substitution works in the same logical way for directory paths. However, directory paths do not typically have periods in them, so you will typically not see the double dots in directory paths.

Example: Assume the target system is SYSZ.

/u/usr/&MSMSYSNM./deployments translates to /u/usr/SYSZ/deployments.

Preview Example

Note: Before a Product Deployment is deployed, the MSMDID shows as ????. After deployment, the Automatic ID is assigned and this is the MSMDID.



Symbolic Qualifiers

ID and System Information

MSMDID

This is the CA MSM deployment ID.

Limits: This is automatically assigned by CA MSM when the Deploy button is clicked or when a deployment is saved.

MSMMPN

This is the CA MSM Mount Point Name. The value is entered into the mount point name field when [adding a custom data set](#) (see page 109) with both the USS radio button and the Container copy radio button set. It is of primary value in remote path.

Note: The Mount Point Name field can contain symbols when it is translated first, the value of the MSMMPN. variable is resolved.

Example: Assume the value of MSMDID is 253 and the user entered the following information.

Mount point name: /u/users/deptest/R&MSMDID./leaf

Remote path: &MSMMPN.

The translated value of &MSMMPN is /u/users/deptest/R253/leaf

MSMSYSNM

This is the CA MSM system object name.

SYSCLONE

This is the shorthand name of the system.

Limits: Maximum 2 characters.

SYSNAME

This is the system name entered when a non-sysplex, sysplex, Shared DASD Cluster, or Staging system is created.

SYSPLEX

This is the system name entered when a sysplex is created.

Note: This symbolic may not be used for a non-sysplex system.

SYSUID

The current user ID.

Target Libraries

MSMHLQ

MSMHLQ is the high-level qualifier for the target library.

Limits: It is the characters before the first period in a fully qualified data set name. The high-level qualifier can be from 1 to 8 characters.

Example: For the data set JOHNSON.FINANCE.DIVISION.SCRIPT, the high-level qualifier is JOHNSON.

MSMMLQ

MSMMLQ is the middle-level qualifier for the target library.

Limits: It is the characters after the first period and before the last period in a fully qualified data set name. The middle-level qualifier size can vary based on the number of qualifiers defined.

Example: For the data set JOHNSON.FINANCE.DIVISION.SCRIPT, the middle-level qualifier is FINANCE.DIVISION.

MSMLLQ

MSMLLQ is the low-level qualifier for the target library.

Limits: It is the characters after the last period in a fully qualified data set name. The low-level qualifier can be from 1 to 8 characters.

Example: For the data set JOHNSON.FINANCE.SCRIPT, the low-level qualifier is SCRIPT.

MSMSLQ

This is the secondary low-level qualifier for the target library and it is the "segment" of the data set name just before the low-level qualifier (MSMLLQ).

Limits: It is the characters after the second to last period and before the last period in a fully qualified data set name. The secondary low-level qualifier can be from 1 to 8 characters.

Example: For the data set JOHNSON.FINANCE.SECOND.SCRIPT, the low-level qualifier is SECOND.

MSMPREF

This is the target library prefix. The target library prefix is the entire data set name to the left of the MSMLLQ.

Example: For the data set JOHNSON.FINANCE.DIVISION.SCRIPT the prefix is JOHNSON.FINANCE.DIVISION.

MSMDLIBN

The deployed library number is a unique number, for each deployed library, within a deployment.

Example: Assume 3 target libraries in a deployment.

DSN = USER456.LIBR473.CAIPROC
DSN = USER456.LIBR473.CAILOAD
DSN = USER456.LIBR473.CAIEEXEC

Assume the methodology specified a mask of:

&SYSUID..D&MSMDID..LIB&MSMDLIBN

Assume USERID is USER789, and the deployment ID is 877, then the resolved DSNs would be,

Deployed library = USER789.D877.LIB1.CAIPROC
Deployed library = USER789.D877.LIB2.CAILOAD
Deployed library = USER789.D877.LIB3.CAIEEXEC

Local Date and Time

LYMMDD

This is the local two-digit year.

YY two-digit year

MM two-digit month (01=January)

DD two-digit day of month (01 through 31)

Example: 100311

LXR2

This is the local two-digit year.

LXR2 two-digit year

Example: 10

LXR4

This is the local four-digit year.

LXR4 four-digit year

Example: 2010

LXON

This is the local month.

LXON two-digit month (01=January)

Example: 03

LDAY

This is the local day of the month.

LDAY two-digit day of month (01 through 31)

Example: 11

LJDAY

This is the local Julian day.

LJDAY three-digit day (001 through 366)

Example: The Julian day for January 11th is 011.

LWDAY

This is the local day of the week.

LWDAY is three characters in length. The days are MON, TUE, WED, THR, FRI, SAT, and SUN.

Example: MON

LHHMMSS

This is the local time in hours, minutes, and seconds.

HH two digits of hour (00 through 23) (am/pm NOT allowed)

MM two digits of minute (00 through 59)

SS two digits of second (00 through 59)

Example: 165148

LHR

This is the local time in hours.

LHR two-digits of hour (00 through 23) (am/pm NOT allowed)

Example: 16

LMIN

This is the local time in minutes.

LMIN two-digits of minute (00 through 59)

Example: 51

LSEC

This is the local time in seconds.

LSEC two-digits of second (00 through 59)

Example: 48

UTC Date and Time

Coordinated Universal Time is abbreviated UTC.

YYMMDD

This is the UTC date.

YY two-digit year

MM two-digit month (01=January)

DD two-digit day of month (01 through 31)

Example: 100311

YR2

This is the UTC two digit year.

YR2 two-digit year

Example: 10

YR4

This is the UTC four digit year.

YR4 four-digit year

Example: 2010

MON

This is the UTC month.

MON two-digit month (01=January)

Example: 03

DAY

This is the UTC day of the month.

DAY two-digit day of month (01 through 31)

Example: 11

JDAY

This is the UTC Julian day.

JDAY three-digit day (001 through 366)

Example: The Julian day for January 11th is 011.

WDAY

This is the UTC day of the week.

WDAY is three characters in length. The days are MON, TUE, WED, THR, FRI, SAT, and SUN.

Example: MON

HHMMSS

This is the UTC time in hours, minutes, and seconds.

HH two-digits of hour (00 through 23) (am/pm NOT allowed)

MM two-digits of minute (00 through 59)

SS two-digits of second (00 through 59)

Example: 044811

HR

This is the UTC time in hours.

HR two digits of hour (00 through 23) (am/pm NOT allowed)

Example: 04

MIN

This is the UTC time in minutes.

MIN two-digits of minute (00 through 59)

Example: 48

SEC

This is the UTC time in seconds.

SEC two-digits of second (00 through 59)

Example: 11

Maintain Methodologies

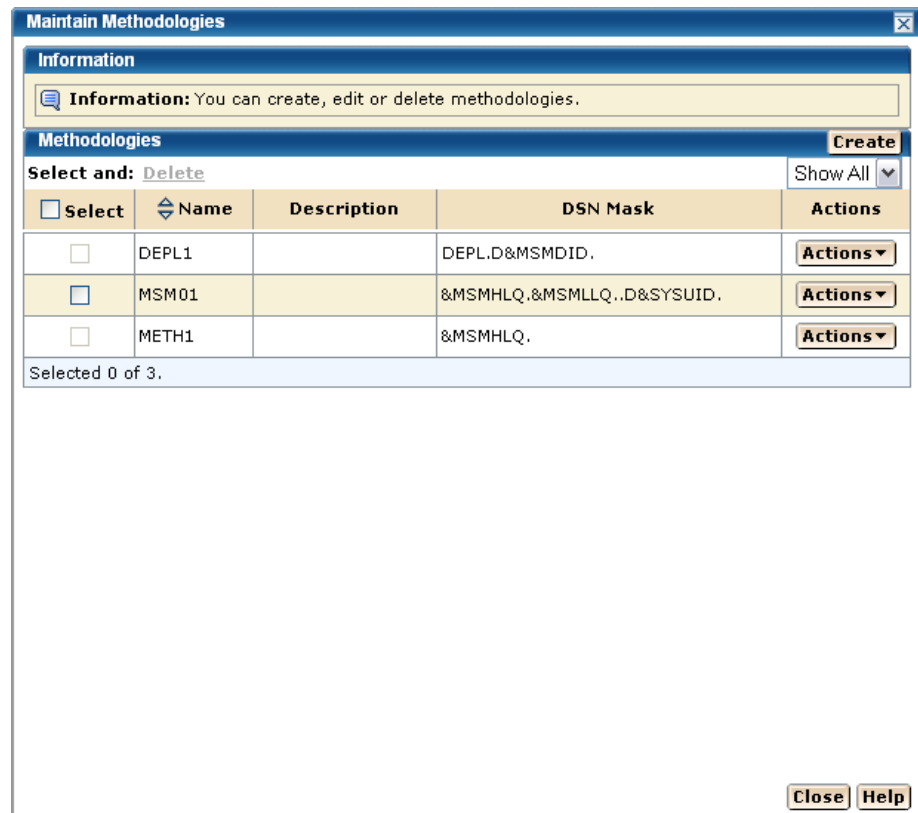
You can edit, replace, or [remove](#) (see page 131) methodologies.

Follow these steps:

1. Click the Deployments tab, and in the Actions section click the Maintain Methodologies link. The Maintain Methodologies select window appears.



Note: A grayed select box indicates that the methodology is assigned and cannot be removed. It can be edited.



2. Select a methodology. Select Edit from Actions list.

[The Methodology window appears for editing](#) (see page 129).

More information:

[Delete Methodologies](#) (see page 131)

[Edit a Methodology](#) (see page 129)

Edit a Methodology

You can edit a methodology by updating or modifying any of the fields on the Edit Methodology window.

Follow these steps:

1. Click the Deployments tab, and in the Actions section click the Maintain Methodologies link.
2. Select the methodology that you want to edit, click the Actions drop-down list, and then click Edit.

The Edit Methodologies dialog appears.

Note: The asterisk indicates that the field is mandatory.

As with Add a Methodology, all fields are available to be edited and the details for each field are listed.

3. Enter the Methodology Name.

Limits: Maximum 64 characters.

Note: Each methodology name must be unique and it is not case-sensitive. For example, Meth1 and meth1 are the same methodology name.

4. Enter the Description of this Methodology.

Limits: Maximum 255 characters.

5. Enter the data set name mask, click the file icon, and select a [symbolic name](#) (see page 119).

Data Set Name Mask

This is the mask that will be used to name the data sets that are deployed. They can contain [symbolic qualifiers](#) (see page 119).

Example: CAPRODS.&SYSID. - in this case the &SYSID. will be replaced by its values. If the SYSID that is being deployed to is XX16 the DSN mask will be: CAPRODS.XX16

Limits: Maximum 64 characters.

Note: Each deployed target data set is named using the resolved content of the data set name mask followed by the low-level qualifier of the source data set. Appending the low-level qualifier from the source data set helps ensure uniqueness of the final data set name. Verify that the mask that you entered does not exceed 35 characters when it is translated.

The mask consists of one or more qualifiers that are separated by periods. The maximum number of characters is 64, including the periods. While you are entering the mask, CA MSM validates the mask by replacing symbolics with the minimum possible values first, and then with the maximum values. If the validation with the minimum possible values fails, an error message appears at the top of the dialog, and you cannot proceed. If the validation with the maximum values fails, a warning message appears, and you can proceed.

When the mask is translated, it has a maximum length of 44 characters including the periods and the low-level qualifier from the source data set. The low-level qualifier from the source data set has a maximum length of nine characters including a period.

■

6. Select a Style of Deployment.

Create only

Creates new data sets.

Note: Prior to creating any data sets on the remote system, a check is made, to see if the data sets already exist. The deployment is not allowed to continue if this occurs.

Create or Replace

If you select *Create or Replace* and the target data sets do not exist, they will be created. If the target data sets exist, *Create or Replace* indicates that data in the existing data set, file or directory will be replaced.

Partitioned data set

Create or Replace indicates that existing members in a partitioned data set will be replaced by members with the same name from the source file. Any currently existing member that is not in the source file will remain in the PDS. Any member from the source that does not already exist in the target PDS will be added to the target PDS.

The amount of free space in the PDS will need to be sufficient to hold the additional content, since no automatic compress will be done.

Directory in a UNIX file system

Create or Replace indicates files in a directory will be replaced by files with same name from the source. Any currently existing directory in a UNIX file system that is not in the source will remain in the UNIX file system.

Sequential data set or a file in the UNIX file system

Create or Replace indicates the existing data set or file and its attributes will be replaced with the data from the source file.

For a VSAM data set (cluster)

Create or Replace indicates that an existing VSAM cluster should be populated with the data from the source file.

Note: The existing VSAM cluster must be of the same type as the source cluster (ESDS, KSDS, LDS, or RRDS), and it must have characteristics that are compatible with the source cluster (such as, record size, key size, and key offset). Replace does not verify the compatibility of these characteristics!

To replace the contents of an existing cluster, the cluster is altered to a reusable state by using an IDCAMS ALTER command, if necessary, before the data from the VSAM source is copied into the cluster by using an IDCAMS REPRO command. The REPRO command will use both the REPLACE and REUSE operands. Following the REPRO operation, the cluster is altered back to a non-reusable state if that was its state to begin with.

7. Click Save.

Your changes are saved.

Note: Click Cancel to close this dialog without saving your changes.

More information:

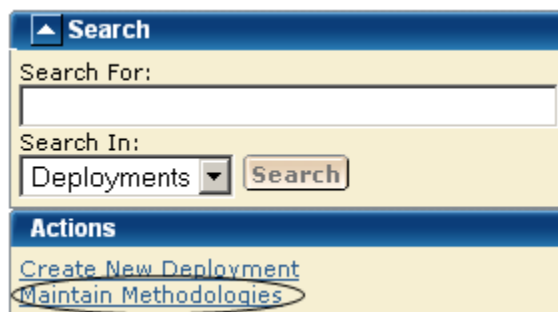
[Symbolic Qualifiers](#) (see page 119)

Delete Methodologies

Follow these steps:

1. Click the Deployments tab, and in the Actions section click the Maintain Methodologies link.

The Maintain Methodologies select window appears.



2. Select the methodology that you want to delete.

Note: A grayed select box indicates that the methodology is assigned and cannot be deleted. It can be edited.

3. Click Delete and then OK to the Delete Methodologies confirmation window.
The methodology is deleted.

Systems

You can view, add, and remove systems from a deployment.

Target System Types

There are two types of *target systems*.

Test Environment

Test Environment target systems isolate untested deployment changes and outright experimentation from the production environment or repository. This environment is used a temporary work area where deployments can be tested, modified, overwritten, or deleted.

Production

Production target systems contain current working product deployments. When activating products in a production target system care must be taken, CA MSM recommends using the following procedure.

1. Copy the product to that target system with the data set names set to private. This allows only those assigned to this area to test these deployed products. The purpose of this first stage is to test or verify that the product is working.
2. Use intermediate test phases for products as they move through various levels of testing. For example you may want to let the application development group as a whole use the product in its test mode prior to moving to production.
3. Move the deployed products to production.

View a System List

You can view a system list.

Follow these steps:

1. Click the Deployments tab, and select the current deployment from the tree on the left side.

The detailed deployment information appears on the right side.

System Name Sort Arrows

Click the up arrow to place the system names in alphabetic order or click the down arrow to place them in reverse alphabetic order.

Type Sort Arrows

Click the up arrow to place the types in alphabetic order or click the down arrow to place them in reverse alphabetic order.

Description Sort Arrows

Click the up arrow to place the descriptions in alphabetic order or click the down arrow to place them in reverse alphabetic order.

Add a System

You can add a system to a deployment.

Follow these steps:

1. Click the Deployments tab.
The Deployment page appears.
2. On the right, in the Deployments panel click the Current Deployment link.
A list of current deployments appears.
3. Click the deployment name link.
4. In the System List panel, click Add Systems.
The Add Systems window appears.
5. Select a system to add and click OK.

Note: When two systems have the same name, use the description to differentiate between the systems.

The Preview window appears, and the system is added.

Note: Sysplex systems are denoted by Sysplex System:System Name. For example, PLEX1:CO11, where PLEX1 is Sysplex name and CO11 is the system name.

Remove a System

You can remove a system from a deployment.

Follow these steps:

1. Click the Deployments tab.
The Deployment page appears.
2. On the right, in the Deployments panel, click the Current Deployment link.
A list of current deployments appears.
3. Select the deployment that you want to remove the system from.

System Name Sort Arrows

Click the up arrow to place the system names in alphabetic order or click the down arrow to place them in reverse alphabetic order.

Type Sort Arrows

Click the up arrow to place the types in alphabetic order or click the down arrow to place them in reverse alphabetic order.

Description Sort Arrows

Click the up arrow to place the descriptions in alphabetic order or click the down arrow to place them in reverse alphabetic order.

4. In the System List panel, select a system you want to remove.
5. Click Remove and then OK to the Remove Products confirmation window.
The system is removed.

Deployment Summary

The Action button is available after a successful deployment.

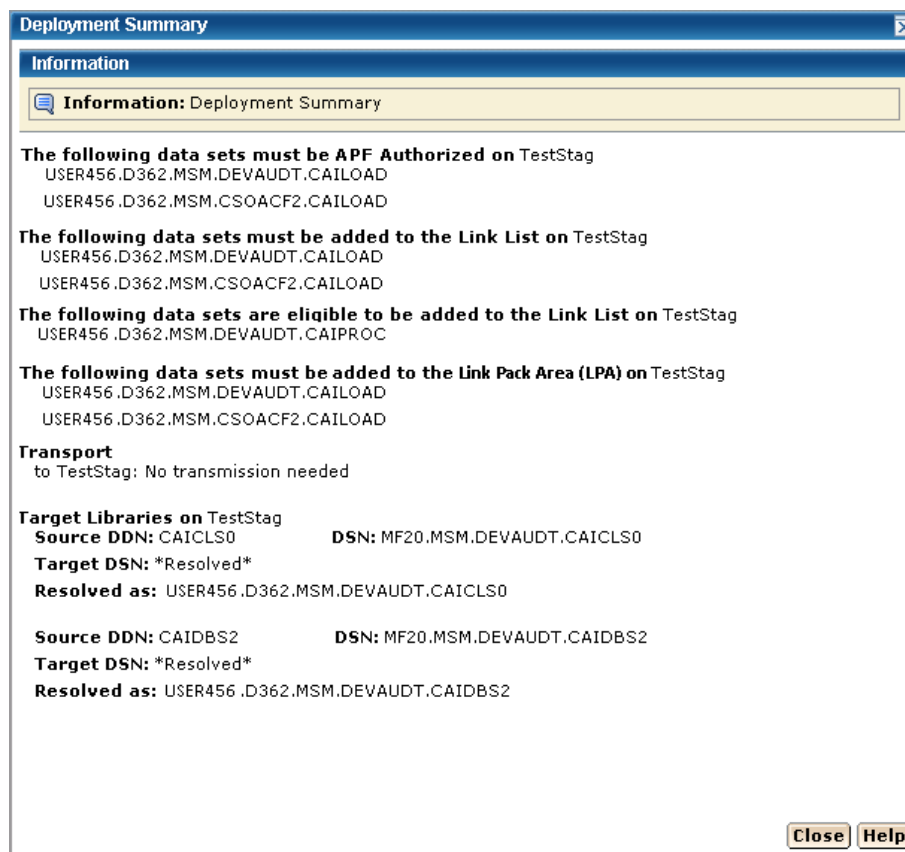
Important! Data sets may need to be APF-authorized and added to the Link List and Link Pack Area. These data sets are identified in this dialog.

The Deployment Summary window may contain the following:

- Deployment ID
- Name
- Products
- Systems
- Data Sets actions
- Transport information

- Target libraries including: source, target, and resolved data set names.
- SMP/E environment
- Snapshot path and container

The following example shows the Data Sets actions, Transport, and Target libraries information.



Note: When you have completed the procedures in this section, go to Configuring Your Product.

Chapter 4: Installing Your Product from Pax-Enhanced ESD

This section contains the following topics:

[How to Install a Product Using Pax-Enhanced ESD](#) (see page 137)

[Allocate and Mount a File System](#) (see page 143)

[Copy the Product Pax Files into Your USS Directory](#) (see page 146)

[Create a Product Directory from the Pax File](#) (see page 151)

[Copy Installation Files to z/OS Data Sets](#) (see page 152)

[Receiving the SMP/E Package](#) (see page 153)

[Clean Up the USS Directory](#) (see page 156)

[Apply Maintenance](#) (see page 157)

[Maintenance](#) (see page 158)

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](#) (see page 142)

[Allocate and Mount a File System](#) (see page 143)

[Copy the Product Pax Files into Your USS Directory](#) (see page 146)

[Create a Product Directory from the Pax File](#) (see page 151)

[Copy Installation Files to z/OS Data Sets](#) (see page 152)

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 139) 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](#)

				<input type="checkbox"/> 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	<input type="checkbox"/>	Download
CCS - MFNSM - ESD ONLY 140000AW040.pax.Z	14.0 /0000	07/06/2011	202.01MB	<input type="checkbox"/>	Download
CCS - BASE - ESD ONLY 140001AW010.pax.Z	14.1 /0000	06/05/2012	27.44MB	<input type="checkbox"/>	Download
CCS - OPTIONAL - ESD ONLY 140001AW020.pax.Z	14.1 /0000	06/05/2012	14.49MB	<input type="checkbox"/>	Download
CA EARL PRODUCT PACKAGE 610106AEO00.pax.Z	6.1 /0106	10/30/2008	1.85MB	<input type="checkbox"/>	Download
EARL PIPPACK AEO61010600.pdf	6.1 /0106	01/29/2010	93.92KB	<input type="checkbox"/>	Download
CA EASYTRIEVE PRODUCT PACKAGE B60000ESA00.pax.Z	11.6 /0000	07/05/2011	6.12MB	<input type="checkbox"/>	Download
DATACOM/AD PROD INFO PACKET CAIE00000P0.pdf	14.0 /0000	06/01/2012	220.53KB	<input type="checkbox"/>	Download
DATACOM/AD XPRESS INSTALL				<input type="checkbox"/>	Download

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](#)

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](#)

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 ▼

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,
// DSNTYPE=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(AGGRGROW)
```

- 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](#) (see page 139)
[ESD Product Download Window](#) (see page 139)

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 *CAtoMainframe.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://ftpdnloads.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](#) (see page 13) 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
```

4. If ICSF is not active, perform the following steps:
 - 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)*.

Receiving the SMP/E Package

If you are installing the package into a new SMP/E environment, use the sample jobs included with the product to set up an SMP/E environment before proceeding.

At this point, complete the SMP/E RECEIVE using files on DASD that the UNZIPJCL job created. Consult the product sample JCL library that contains a sample job customized to receive the product from DASD. Specifically, you must specify the following values:

- DASD data set names for SMPPTFIN and SMPHOLD (if applicable)
- The HLQ that you used in the UNZIPJCL job on the RFPREFIX parameter on the RECEIVE command

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 [set to your product name]. 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.

To prepare the SMP/E environment for your product

1. Customize the macro LIBSEDIT 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 LIBSEDIT 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.

Note: Set the DASD HLQ to the same value specified for *yourHLQ* for the unzip to DASD ESD JCL.

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

2. Open the SAMPJCL member LIB1ALL in an edit session and execute the LIBSEDIT macro from the command line.

LIB1ALL is customized.

3. Submit LIB1ALL.

This job produces the following results:

- The target and distribution data sets for CA Librarian are created.
- Unique SMPPTS, SMPMDS, SMPSCDS, and SMPSTS data sets for this target zone are created.

4. Open the SAMPJCL member LIB2CSI in an edit session and execute the LIBSEDIT macro from the command line.

LIB2CSI is customized.

5. Submit LIB2CSI.

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 Pax Installation

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

To run the installation jobs

1. Open the SAMPJCL member LIB3RECD in an edit session and execute the LIBSEEDIT macro from the command line.
LIB3RECD is customized.
2. Submit the *yourhlq*.SAMPJCL member LIB3RECD to receive SMP/E base functions.
CA Librarian is received and now resides in the global zone.
3. Open the SAMPJCL member LIB4APP in an edit session and execute the LIBSEEDIT macro from the command line.
LIB4APP is customized.
4. Submit the *yourhlq*.SAMPJCL member LIB4APP to APPLY SMP/E base functions.
Your product is applied and now resides in the target libraries.
5. Open the SAMPJCL member LIB5ACC in an edit session and execute the LIBSEEDIT macro from the command line.
LIB5ACC is customized.
6. Submit the *yourhlq*.SAMPJCL member LIB5ACC to ACCEPT SMP/E base functions.
Your product 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 [assign the value for hlq in your book]SEEDIT macro was customized in the installation steps. Verify that you still have the values from the base installation.
4. Open the SAMPJCL member [assign the value for hlq in your book]6RECP in an edit session and execute the [assign the value for hlq in your book]SEEDIT macro from the command line.

[assign the value for hlq in your book]6RECP is customized with your JOB statement, CSI location, and zone names.

5. Customize the [assign the value for hlq in your book]6RECP SMPPTFIN and SMPHOLD DD statements to reference the FB 80 data sets for the PTFs and HOLDDATA.
6. Submit [assign the value for hlq in your book]6RECP.
The PTFs and HOLDDATA are received.
7. Open the SAMPJCL member [assign the value for hlq in your book]7APYP in an edit session and execute the [assign the value for hlq in your book]SEEDIT macro from the command line.
[assign the value for hlq in your book]7APYP is customized.
8. Submit [assign the value for hlq in your book]7APYP.
The PTFs are applied.
9. (Optional) Open the SAMPJCL member [assign the value for hlq in your book]8ACCP in an edit session and execute the [assign the value for hlq in your book]SEEDIT macro from the command line.
[assign the value for hlq in your book]8ACCP is customized.
10. (Optional) Submit *yourHLQ.SAMPJCL* member [assign the value for hlq in your book]8ACCP.
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.

Maintenance

CA Support Online may have maintenance and hold data that have been published since the installation data was created.

To apply maintenance

1. Check CA Support Online and download any PTFs and hold data published since this release was created.
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 hold data.
The PTFs and hold data become accessible to the *yourhlq.SAMPJCL* maintenance members.
3. Edit and submit the [assign the value for hlq in your book]SEEDIT macro.
The *yourhlq.SAMPJCL* members LIB6RECP, LIB7APYP, and LIB8ACCP are customized.

4. Customize the LIB6RECP SMPPTFIN and SMPHOLD DD statements to reference the FB 80 data sets for the PTFs and hold data.
5. Submit LIB6RECP.
The PTFs and hold data are received.
6. Submit LIB7APYP.
The PTFs are applied.
7. (Optional) Customize and submit *yourhlq.SAMPJCL* member LIB8ACCP.
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's 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.

Note: When you have completed the procedures in this section, go to Configuring Your Product.

Chapter 5: Installing Your Product from Tape

This section contains the following topics:

[Installation Tape](#) (see page 163)

[Unload the Sample JCL from Tape](#) (see page 164)

[How to Install Products Using Native SMP/E JCL](#) (see page 165)

[Apply Maintenance](#) (see page 168)

Chapter 6: Installation Tape

CA Librarian is distributed on a standard label 3480 cartridge. It must be installed with SMP/E. The installation tape includes cumulative product maintenance. The volume serial number is *pcyymm*, where *pc* is the CA Librarian product ID (LR) *yy* is the last two digits of the year, and *mm* is the month (for example, LR0111).

This section contains the following topics:

[Contents of the Installation Tape](#) (see page 163)

Contents of the Installation Tape

The installation tape contains the following files:

File	DSNAME	Attributes	Description
1	CAI.SAMPJCL	IEBCOPY UNLOAD	Installation JCL.
2	CAI.SMPMCS	80/7200/FB	SMPE/PTFs in MCS format
3	CAI.SYSMOD.FN	IEBCOPY UNLOAD	PTF RELFILES begin here
21	CAI.LIBR44.PROD.MAST		Product testing data
22	CAI.LIBR44.SYS.MAST		Product testing data and files

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=nnnnnn,
//          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.

nnnnnn

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 [set to your product name]. 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.

To prepare the SMP/E environment for your product

1. Customize the macro LIBSEEDIT 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 LIBSEEDIT on the TSO command line, and press Enter to replace the defaults with your specifications.

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

Note: The following steps include instructions to execute the [assign the value for hlq in your book]SEEDIT macro each time you open a new SAMPJCL member. To edit all SAMPJCL members simultaneously, read and follow the instructions in the LIBEDALL member.

2. Open the SAMPJCL member LIB1ALL in an edit session and execute the LIBSEEDIT macro from the command line.

LIB1ALL is customized.

3. Submit LIB1ALL.

This job produces the following results:

- The target and distribution data sets for CA Librarian are created.
- Unique SMPLTS, SMPMTS, SMPSCDS, and SMPSTS data sets for this target zone are created.

4. Open the SAMPJCL member LIB2CSI in an edit session and execute the LIBSEEDIT macro from the command line.

LIB2CSI is customized.

5. Submit LIB2CSI.

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.

To run the installation jobs

1. Open the SAMPJCL member LIB3RECT in an edit session and execute the LIBSEEDIT macro from the command line.

LIB3RECT is customized.

2. Submit the *yourhlq*.SAMPJCL member LIB3RECT to receive SMP/E base functions.

CA Librarian is received and now resides in the global zone.

3. Open the SAMPJCL member LIB4APP in an edit session and execute the LIBSEEDIT macro from the command line.

LIB4APP is customized.

4. Submit the *yourhlq*.SAMPJCL member LIB4APP to APPLY SMP/E base functions.

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

5. Open the SAMPJCL member LIB5ACC in an edit session and execute the LIBSEEDIT macro from the command line.

LIB5ACC is customized.

6. Submit the *yourhlq*.SAMPJCL member LIB5ACC to ACCEPT SMP/E base functions.

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

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

Apply Maintenance

CA Support Online may have maintenance and HOLDDATA that have been published since the installation data was created.

To apply maintenance

1. Check CA Support Online and download any PTFs and HOLDDATA published since this release was created.
 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 LIBSEEDIT macro was customized in the installation steps. Verify that you still have the values from the base install.
 4. Open the SAMPJCL member LIB6RECP in an edit session and execute the LIBSEEDIT macro from the command line.

LIB6RECP is customized with your jobcard, CSI location, and zone names.
 5. Customize the LIB6RECP SMPPTFIN and SMPHOLD DD statements to reference the FB 80 data sets for the PTFs and HOLDDATA.
 6. Submit LIB6RECP.

The PTFs and HOLDDATA are received.
 7. Open the SAMPJCL member LIB7APYP in an edit session and execute the LIBSEEDIT macro from the command line.

LIB7APYP is customized.
 8. Submit LIB7APYP.

The PTFs are applied.
 9. (Optional) Open the SAMPJCL member LIB8ACCP in an edit session and execute the LIBSEEDIT macro from the command line.

LIB8ACCP is customized.
 10. (Optional) Submit *yourhlq*.SAMPJCL member LIB8ACCP.

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's 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.

Chapter 7: Deploying Your Product

We recommend that you deploy your product according to your site-specific requirements. If you have questions, contact us at <http://ca.com/support>.

Chapter 8: Configuring Your Product

This chapter describes the minimum configuration tasks needed before CA Librarian can be started, customized, and used in your environment.

This section contains the following topics:

[LIB/CCF System Master File Conversion](#) (see page 173)

[Upgrading from LIB/CCF r3.7 or Earlier](#) (see page 175)

[Allocate Optional VSAM Control File](#) (see page 187)

[Initialize VSAM Control File](#) (see page 188)

[Receive/Apply Customer ID USERMOD](#) (see page 188)

[Receive/Apply Module Rename USERMOD](#) (see page 189)

[Install External Security Interface, Activate LAM Subsystem](#) (see page 190)

[Execute LAMSERV \(Optional\)](#) (see page 194)

[Install ELIPS \(Optional\)](#) (see page 194)

[Install the CA Roscoe Interface \(Optional\)](#) (see page 205)

[Install the ISPF Options](#) (see page 206)

[Copy LIB/CCF Model System](#) (see page 207)

[Install LIB/TSO](#) (see page 207)

[Install LIB/CCF-CA Roscoe](#) (see page 219)

[Install LIB/CCF-ISPF\(TSO\)](#) (see page 226)

LIB/CCF System Master File Conversion

LIB/CCF supports VM/ESA, z/VM, and DB2. The format of certain LIB/CCF control records stored on the System Master File has changed:

- A library definition (LDR) now contains a four-character VM/ESA and z/VM address instead of a three-character VM/ESA and z/VM address.
- An LCDF chain now contains a field for a DB2 DBRM library name.

Therefore, an *automatic* conversion of these records takes place through release 4.4 LIB/CCF processing. When entering Option 12.11 of LIB/CCF, the conversion occurs automatically if there are release 3.8 chains or library definitions found on the System Master File. If no release 3.8 chains or library definitions are found, no conversion is necessary. Once the process is complete, LCDF displays the message CONVERSION PERFORMED. Press PF1 to display the message CDF066: LCDF HAS CONVERTED FROM 3.8 TO 4.4 FORMAT. LCDF checks for release 3.8 chains or library definitions every time Option 12.11 is entered and performs the conversion whenever necessary.

Attempting to use an unconverted release 3.8 format System Master File with any release 4.4 LIB/CCF function that requires LCDF information (other than Option 12.11) results in the message OLD CHAIN/LDR. Pressing PF1 displays the following message:

```
CDF067      T4nnnnn/T5nnnnnn MUST BE CONVERTED BEFORE USE.
```

Once the conversion process is complete, it is still possible to execute release 3.8 LIB/CCF against the release 4.4 System Master File. However, the following restrictions apply:

- If a library definition was updated with a four-character VM/ESA and z/VM address through Option 12.11.3 of release 4.4, release 3.8 displays the address as XXX. If this library definition is used with release 3.8 LIB/CCF, it must be corrected through Option 12.11.3 of release 3.8 by entering a valid three-character VM/ESA and z/VM address. Otherwise, LIB/CCF supplies the invalid address of XXX for subsequent processing. Thus, correcting the address converts the library definition back to the release 3.8 format.
- If Option 12.11.2 is used to modify a chain, that chain is converted back to the release 3.8 format, that is, the DBRM library name field is removed.

For the purposes of testing release 4.4, you can execute both release 3.8 and 4.4 LIB/CCF against the same 4.4 System Master File. However, once release 4.4 is fully implemented, we strongly recommend that you discontinue using release 3.8 to avoid confusion due to the restrictions listed previously.

Upgrading from LIB/CCF r3.7 or Earlier

This section is for sites that are upgrading from LIB/CCF r3.7 or earlier.

The Library Chain Definition Function (LCDF) eliminates certain LIB/CCF administrator tables. LCDF lets you define production and test master file pairs and their associated libraries (object, load, history) with any number of intermediate Q/A and reject libraries. Each set of files contains a library chain defining a promotion path for members under development.

One of the primary benefits of LCDF is that all master file definition information is collected into one set of members and is shared by all CCF systems. Also, a file's characteristics are defined only once, regardless of how many library chains it is used in.

LCDF is available in the CA Roscoe, ISPF(TSO) and ISPF(VM/ESA or z/VM) environments as Administrator option 12.11, replacing the Master File Definition Table (12.4), the Production Master File Table (12.6), the History Master File Table (12.7), and the VM/ESA and z/VM Master File Information Table (12.10). The information formerly carried in these tables is now in restructured members on the System Master File.

If you are upgrading to r4.4 from r3.7 or earlier, the information in the affected tables must be converted to the new format. LIB/CCF r4.4 does not operate in the above environments without the information in the new format.

To assist in the upgrade to r4.4, there is a program to reformat the existing table information and update the System Master File accordingly, allowing work in progress to continue.

CCFCNV37

The CCF conversion program is named CCFCNV37. It is link edited into the CCF load library during the install process. CCFCNV37 uses the contents of the following System Master File members to generate the LCDF members required by version 4.4.

For LIB/CCF-CA-Roscoe:

- \$CHGT004
- \$CHGT006
- \$CHGT007

For LIB/CCF-ISPF(TSO):

- \$CCFT004
- \$CCFT006
- \$CCFT007

For LIB/CCF-ISPF(VM/ESA and z/VM):

- \$CCCT004
- \$CCCT006
- \$CCCT007
- \$CCCT009

In addition, CCFCNV37 optionally converts the Language Definition Table, \$CxxT005, to the 4.4 format that allows eight characters for the language type.

Finally, CCFCNV37 inserts the appropriate chain entry number into existing MMR, MTR, and SLR entries.

Output from CCFCNV37 is a report of any error conditions detected, a file (CCFOUT) containing the CA Librarian control statements to implement the conversion and, if requested through the PARM, direct an update of the CCF System Master. You can define the CCF System Master explicitly or it can be picked up from the \$CCFCOMI module.

As CCFCNV37 converts the various tables, it analyzes the information to determine whether there are conflicts between different definitions of the same resources. Any such error writes a message to CCFPRINT and processing continues, but no updating of the System Master takes place.

In the event of any of the tables having an invalid format, processing terminates immediately.

You can execute the conversion for one or more of the CA Roscoe, TSO ISPF, and VM/ESA or z/VM ISPF environments for CCF; the PARM denotes which.

Execution of CCFCNV37

CCFCNV37 uses the following files:

MASTER

Defines the CCF System Master File to convert. If you omit this DD statement, CCFCNV37 tries to locate the correct System Master through the \$CCFCOMI module in the CCF load library. If you provide a MASTER DD, the SYSBASE= operand in the parm must define the MCD base for the file.

CCFPRINT

Defines the report file. If omitted, CCFCNV37 tries to use the \$CCFCOMI module to determine the printer definitions required.

CCFOUT

Defines the optional output file where CA Librarian control statements necessary to update the System Master File with the reformatted table and control members are written. If omitted, NOCCFOUT must be specified in the PARM.

STEPLIB

Can define the library containing the \$CCFCOMI module if MASTER or CCFPRINT DD statements are omitted.

The following PARM operands are valid for CCFCNV37:

ROSCOE

Converts the CA Roscoe CCF tables (see below for information on converting in the CA Roscoe environment).

TSO

Converts the TSO/ISPF CCF tables.

CMS

Converts the CMS/ISPF CCF tables.

NOTABLE5

Suppresses conversion of \$CxxT005 members.

NOCCFOUT

Suppresses use of CCFOUT to hold the CA Librarian update control stream.

SYSBASE=nnnn

Provides CA Librarian MCD base for the CCF System Master defined in the MASTER DD statement.

UPDATE

CCFCNV37 directly updates the CCF System Master during the execution of the conversion. If any table errors are detected during conversion, the update is suppressed.

The UPDATE parameter and the CCFOUT file are not mutually exclusive; you can write the control stream to the output file even though you request direct updating of the System Master File.

Note: If your site shares a CCF System Master File between CCF systems running under different environments (for example ISPF(TSO) and ISPF(VM/ESA or z/VM)), then one conversion must be done for all the environments. Failure to do this results in incomplete LCDF tables.

Reformatting the System Master File Under CA Roscoe

Where CCF is run under CA Roscoe, it is necessary to preprocess the conversion; the tables \$CHGT002, \$CHGT005 and \$CHGT006 normally reside only on the CA Roscoe library, and not on the CCF System Master. To handle this preprocessing and to provide the opportunity to run the whole conversion process online, CCF/CA-Roscoe supplies an RPF named CCFCN37R.

CCFCN37R allows conversion of \$CHGT005, reformats \$CHGT002 and \$CHGT006, and places them onto the CCF System Master, and can execute CCFCNV37 in foreground using ETSO.

Before exercising the option to convert in foreground, ensure that the CA Roscoe procedure ETSOLIB statement defines a library containing the module CCFCNV37, and that the ETSO EPL has CCFCNV37 defined to it. The following EPL entry has been shown to suffice in most circumstances, although a System Master with very large tables and xxxCNTLO members can require an increase in the CPU and memory values:

```
CCFCNV37 0256 0064 0032 N
```

CCFCN37R must be executed under the CA Roscoe CCF Administrator's prefix. The first panel describes the RPF. The second requests conversion options.

If N is placed against "Convert under ETSO," the RPF terminates after completing the conversion preprocessing. The batch conversion, as described elsewhere, should then be used. The other fields on the panel equate to the PARM entries for CCFCNV37.

Suggested Conversion Procedures (CA Roscoe and TSO)

Following is a guide to the steps to follow when converting to CCF release 4.4 from release 3.7 or earlier. You should suspend CCF activity during the conversion, although if you use the UPDATE parm in Step4, suspension is absolutely necessary during this step only.

1. Decide whether to provide a MASTER DD statement or allow CCFCNV37 to find a \$CCFCOMI module. Using JCL gives explicit control over the System Master converted, but does require the MCD base to be provided.
2. Run CCFCNV37 with the parm made up as follows:
 - CA Roscoe if you run CCF/CA-Roscoe with the chosen SYSMAST
 - TSO if you run CCF/ISPF(TSO) with the chosen SYSMAST

- VM/ESA and z/VM if you run CCF/ISPF(VM/ESA or z/VM) with the chosen SYSMAST
- SYSBASE=*nnnn* if you have a MASTER DD statement

Note: If you are converting the CA Roscoe tables, at least the preprocessing must be run under CA Roscoe first.

```
// CONVRT37 JOB B00TH,CLASS=7,MSGCLASS=X
// CONVERT EXEC PGM=CCFCNV37,
//          PARM='ROSCOE,TSO,SYSBASE=6789'      A
// STEPLIB DD DSN=cai.caljlink,DISP=SHR        B
// MASTER  DD DSN=libccf.sysmast,DISP=SHR      C
// CCFPRINT DD SYSOUT=*
// CCFOUT  DD DSN=libr.ccf.update.output,      D
//          VOL=SER=MULIB2,UNIT=3387,
//          DISP=(,CATLG),SPACE=(TRK,(1,1)),
//          DCB=(LRECL=87,BLKSIZE=3277,RECFM=FB)
```

The following explains values that appear in the sample JCL:

A

This parm requests conversion of CA Roscoe and TSO tables. The conversion is done against the System Master defined in C. The update stream is written to the CCFOUT file for subsequent execution.

B

Defines the load library containing the CCFCNV37 module, and \$CCFCOMI if the MASTER or CCFPRINT statements are not used.

C

The CCF System Master to convert.

D

The output file to contain CA Librarian update control stream.

3. Examine the CCFPRINT report. If there are no errors, proceed to the next step. Otherwise you must resolve any anomalies (a complete list of error messages produced by CCFCNV37 appears in a later section).

Most errors are due to conflicts in the definition of CCF resources in the different environments.

4. When all errors are resolved, the System Master can actually be converted. You can achieve this in one of two ways, but first you should take a backup of your System Master using the CA Librarian BKUPTAPE facility.

To convert during the CCFCNV37 run, add UPDATE to the parm and rerun CCFCNV37. The System Master is updated with the new tables and control members. CCF activity must be suspended during this run. Should any new errors arise, the System Master is not updated. Correct the errors and rerun.

As an alternative to directly updating the System Master, you can use the control stream placed into CCFOUT during the last error-free run of CCFCNV37 as input to CA Librarian. In this case, it is imperative that CCF activity be suspended between the run of CCFCNV37 and CA Librarian update run.

5. After conversion is complete, log on to CCF 4.4 and use option 8.9 (available only to the CCF administrator) that displays (or prints) the LCDF chains just generated. Having checked these, you can make any necessary adjustments by using the Administrator's LCDF option, 12.11.

Suggested Conversion Procedures (VM/ESA and z/VM)

The conversion program is link edited into your LIB/CCF load library during the installation of LIB/CCF. It must be executed under the control of CMS/ISPF, and the CCF System Master File information must be obtained from the \$CCFCOMI module.

The error report file is sent to the user's virtual printer, and the CA Librarian update control stream to the user's virtual punch. Direct updating of the System Master File is not supported.

Use the following steps to execute CCFCNV37:

1. Ensure that the FILEDEF statements for ISPLLIB in your ISPF EXEC define the libraries containing \$CCFCOMI and the LIB/CCF modules.
2. Enter ISPF and invoke Dialog Test - Functions (Option 7.1).
3. In the PGM field, enter CCFCNV37. In the PARM field, define the CCF environments to convert. Enter CMS if VM/ESA or z/VM only. Enter CMS/TSO to process both TSO and VM/ESA and z/VM environments. If you also share your LIB/CCF System Master File with CA Roscoe, you must run the conversion under CA Roscoe. See the previous section.
4. Press Enter. If CCFCNV37 ends with a non-zero return code, errors or anomalies were detected during processing. They are reported in the print file.
5. Exit ISPF and issue **SPOOL PRINT CLOSE** and **SPOOL PUNCH CLOSE**. You can view these files using normal procedures.
6. The print file contains any error messages. Analyze them and resolve any anomalies. You can rerun CCFCNV37 until no more errors are reported.
7. The punch file contains the CA Librarian update control stream necessary to convert the System Master File. Fill in the -MCD statement with the correct management code for the System Master File. Next, pass the control stream to the LIBEXP command.

You can use the following commands as an example of this process:

```
SPOOL PUNCH *
SPOOL PRINT *
  Invoke ISPF 7.1 to run CCFCNV37
SPOOL PUNCH CLOSE
SPOOL PRINT CLOSE
RECEIVE spoolid fn ft fm
LIBEXP / fn ft fm
```

CCFCNV37 Error and Informational Messages

CCF000 PARM DATA WAS:

Reason:

Informational. Echoes the parameters supplied.

Action:

None.

CCF001 NO PARM FIELD SUPPLIED

Reason:

Error: A parm was not supplied to CCFCNV37.

Action:

Supply the parm to CCFCNV37.

CCF002 INVALID PARM SUPPLIED

Reason:

Error. A parm or parms contained unknown data.

Action:

None.

CCF003 INVALID PARM COMBINATION

Reason:

Error. An invalid combination of parameters was supplied on the parm.

Action:

None.

CCF004 JCL MASTER PRE-ALLOCATION USED

Reason:

Informational. The CCF SYSMAST used was defined in the MASTER DD statement

Action:

None.

CCF005 JCL CCFPRINT PRE-ALLOCATION USED

Reason:

Informational. A CCFPRINT DD statement was supplied.

Action:

None.

CCF006 SYSBASE= ON PARM, BUT NO MASTER DD SUPPLIED

Reason:

Error. The CCF System Master was determined from \$CCFCOMI, but MCD information was found on the parm.

Action:

Add MASTER DD or remove SYSBASE= from the parm.

CCF007 CCFOUT DD MISSING (NOCCFOUT NOT ON PARM)

Reason:

Error. If CCFOUT use is not suppressed, the DD statement must be supplied.

Action:

None.

CCF008 DIRECT UPDATE STREAM FLUSHED

Reason:

Informational. UPDATE was supplied on the parm, but an error was detected during conversion. The System Master was not updated.

Action:

None.

CCF010 MASTER DD SUPPLIED, BUT NO SYSBASE= ON PARM

Reason:

Error. If the CCF System Master is allocated through JCL, SYSBASE= must be used to provide the MCD base.

Action:

Remove MASTER DD or provide SYSBASE=.

CCF011 TABLE xxxxxxxx NOT ON SYSTEM MASTER

Reason:

Error. The table printed could not be found.

Action:

If all the tables are missing, check the MCD Lock base. If \$CHGT006 is missing, check if RPF CFCN37R was run.

CCF012 ERROR IN LIBRARIAN PROCESSING; SEE REPORT

Reason:

Error. UPDATE was specified, but an error occurred while updating the System Master. The CA Librarian error report was placed on the CCFPRINT data set.

Action:

None.

CCF013 CHAIN GROUP INCONSISTENCY FOR APPLICATION: XXXXXXXXXXXX

Reason:

Error. The printed application name has conflicting chain names defined in the \$CxxT002 tables. Only one chain name is allowed per application. Resolve the conflict and rerun.

Action:

None.

CCF014 INSUFFICIENT MEMORY FOR INTERNAL TABLES.

Reason:

Error.

Action:

Increase the region size and retry.

CCF015 QUASAR ISSUED RETURN CODE: Nn

Reason:

Error. The internal table-handler detected a logic error.

Action:

Contact Technical Support.

CCF016 FOR CHANGE REQUEST WOnnnnnn, NO CHAIN GROUP EXISTS FOR APPL: xxxxxxxx

Reason:

Warning. The printed change request is for an application not defined in CCF \$CxxT002 tables. This is not in itself an error, but can cause later error messages.

Action:

None.

CCF017 CONVERSION TERMINATED DUE TO PREVIOUS ERROR(S)

Reason:

Informational. Appears at the end of CCFPRINT listing if an error was detected.

Action:

None.

CCF018 FORMAT ERROR IN MEMBER xxxxxxxx

Reason:

Error. Member xxxxxxxx has invalid format. Processing terminates immediately.

Action:

Refer to CCF documentation for formats of control members.

CCF019 ERROR IN MEMBER xxxxxxxx STARTING AT RECORD nnnnnnnn

Reason:

Error. An error was detected at CA Librarian sequence number nnnnnnnn in member xxxxxxxx. The actual error is described in a subsequent message.

Action:

None.

CCF020 INVALID RECORD TYPE: X

Reason:

Follows CCF019. The record type of the T004 set is not P, Q, F, or R.

Action:

Correct the record type and retry.

**CCF021 CHARACTERISTICS INCONSISTENT WITH EARLIER DEFINITION
(xxxxxxx) FOR: Dsn**

Reason:

Follows CCF019. Where the same resource is defined for a second or subsequent time, CCFCNV37 checks that key information is not conflicting. In checking *dsn*, the type of data xxxxxxxx does not agree with a previous entry.

Action:

Resolve conflict and rerun.

CCF022 NO PREVIOUS LDR ENTRY FOR xxxxxxxx DATA SET dsn

Reason:

Error. LDR (Library Definition Record) entries are created from data held in CCF tables \$CxxT004, \$CxxT006, and \$CCCT009. While processing table xxxxxxxx, a reference was made to *dsn* which was not previously encountered.

Action:

None.

CCF023 \$CCCT009 LIBRARY TYPE CONFLICT FOR: Dsn

Reason:

Error. Under VM/ESA and z/VM, an CA Librarian Master File can be BDAM, VSAM, or VM/ESA and z/VM format. For *dsn*, the format conflicts with an earlier definition.

Action:

None.

CCF024 NO "F" ENTRY FOR CHAIN GROUP xxxxxxxx PROD MASTER dsn

Reason:

Error. A chain with Q/A entries must have an F entry to define the first-level Q/A library for a Production master.

Action:

Correct the conflict and retry.

CCF025 C/R WOnnnnnn FOUND IN xxxxxxxx HAS NO WOnnnnnn ENTRY IN SYSMAS

Reason:

Error. The xxxxxxxx table contains an entry referring to the printed change request, but this does not exist in the System Master.

Action:

Correct the error and retry.

CCF026 COMBINATION OF PROD AND CURRENT MASTERS AT xxxxxxxx SET FROM nnnnnnnn IS NOT IN A DEFINED CHAIN

Reason:

Error. The record set starting at CA Librarian sequence number *nnnnnnnn* in table xxxxxxxx contains a combination of masters that does not exist in any chain defined for the entry's application.

Action:

Correct the error and retry.

CCF028 SLRCNTL0 ENTRY AT nnnnnnnn HAS UNLOCATEABLE PRODMAS/PRODLOAD-LDR Combination

Reason:

Error. The System Link Record (SLR) entry at CA Librarian sequence number *nnnnnnnn* refers to a Production Load library that was not defined as used by the Production Master in any \$CxxT006 entry.

Action:

Correct the error and retry.

**CCF029 MVS TABLES \$CHGT006 AND \$CCFT006 CONFLICT AT ENTRY *nnnnnnnn*.
\$CHGT006 ENTRY WILL BE USED.**

Reason:

Warning. If both CCF/CA Roscoe and CCF/TSO/ISPF are in use with the same SYSMAS, the T006 table should agree. A conflict was found in the TSO table \$CCFT006 at Librarian sequence number *nnnnnnnn*. The previously defined \$CHGT006 entry for the Production master is used during later processing.

Action:

None.

CCF099 FOLLOWING SYSMAS DYNAMICALLY ALLOCATED: Dsn

Reason:

Informational. A MASTER DD statement was not supplied, and the printed data set name was obtained from \$CCFCOMI.

Action:

None.

Allocate Optional VSAM Control File

The member LI44SVM in the CALJJCL library allocates this optional VSAM file.

To allocate the optional VSAM control file

1. Edit the JCL in member LI44VSM conform to your site standards.
2. Submit the job

Review the output to verify that the file was allocated successfully.

Note: This file serves as a catalog of CA Librarian wide record files and must be shared by all CPUs where CA Librarian executes.

Initialize VSAM Control File

This step is optional, but must be performed if the optional VSAM control file was allocated (that is, if wide record master files are to be used).

The member LI44INIT in the CALJCL library initializes the VSAM file created in the Allocate Optional VSAM Control File step.

To initialize the VSAM control file

1. Edit the JCL in the member LI44INT.
Conform to your site's standards.
2. Submit the job.
Review the output to verify that both steps ran successfully.

Receive/Apply Customer ID USERMOD

USERMOD MLJ4405 provides a way to customize the CA Librarian with a customer site name and customer ID. The customer site name prints out on the batch CA Librarian job output header page and on the Comparator II default report. The customer ID is required when assigning a management code (MCD) to a master file. See the *Security Administration Guide* for details on the MCD.

Note: This USERMOD is optional and, if omitted, the site name defaults to CA Librarian and the customer ID defaults to INITM.

Member LJMODRID on the CALJCL library contains the SMP/E statements required for this USERMOD.

The LIBRID macro options for USERMOD MLJ4405 are:

CUSTID=INITM

Specify a five-character customer ID. The first character must be alphabetic. The next four characters can be alphanumeric. The default is INITM.

INSTID=CA-Librarian

Specify the name of your site. You must use apostrophes if the site name contains embedded blanks. The default name is CA-Librarian.

KANJIYN=N

Specify Y (yes) if your site uses DBCS characters or N (no) if it does not..

LANGUAGE=A

CA Librarian uses this parameter internally. Do not alter it.

RUNMASTX=NO

Specify YES to automatically call both input and output exits defined in the master file. The default, NO, requires that exits defined in the master file be specified on PARM= when AFOLIBR is executed.

WORKUNIT=VIO

Specifies a temporary work DASD. If you leave this parameter blank, it defaults to VIO. You can override this parameter setting with a work volume for temporary data sets.

Receive/Apply Module Rename USERMOD

During installation, the CA Librarian batch program is given a default name of AFOLIBR and Comparator II is given a default name of COMP2. You can rename these modules through USERMOD MLJ4400.

Member LJMADAFO on the CALJCL library contains the SMP/E job to rename these modules.

Alter the SMP/E control statements as follows:

```
++RENAME(AFOLIBR) TONAME(xxxxxxx)  
++RENAME(COMP2) TONAME(yyyyyyyy)
```

xxxxxxx

Specifies the new name for the batch CA Librarian.

yyyyyyyy

Specifies the new name for Comparator II.

Delete the appropriate ++RENAME statement if you want to rename only one of the modules.

Note: The default name of AFOLIBR is used in subsequent steps of the installation process. If you rename AFOLIBR to xxxxxxxx in this step, you must change all references of AFOLIBR to xxxxxxxx. For example, you must change LIBNAME=AFOLIBR to reflect the new name when you assemble and link the \$CCFGEN macro.

Install External Security Interface, Activate LAM Subsystem

CAIRIM must be executed on each CPU where CA Librarian executes to install the external security interface and LAM Subsystem. CA Librarian uses SVC168 to implement the external security interface. During the RECEIVE and APPLY step of FMID CALJ440 (the base CA Librarian), an SVC routine module (LVSSVC) and a CAIRIM initialization module (LJ44INIT) were link edited into the CA Librarian target load library (CAI.CAILIB). CA Librarian requires the LVSSVC module when an external security system such as CA Top Secret, CA ACF2, or RACF is installed. LJ44INIT is a required module for CA Librarian, regardless of whether an external security system is installed.

CAIRIM is used to install the SVC without an IPL. CAIRIM can be run as a started task. See the *CA Common Services for z/OS and OS/390 Getting Started* and *CA Common Services for z/OS and OS/390 Administrator Guide* for details on executing the CAIRIM programs. Member LLIBRIM on the CALJCL library contains the necessary CAIRIM initialization parameter for CA Librarian to install the SVC and activate the LAM subsystem.

Note: As previously mentioned, if a STEPLIB for CA Common Services for z/OS and OS/390 CAS9 initialization is employed, you should add the CA Librarian CAILIB and a compatible CA Common Services for z/OS and OS/390 CAILIB to the concatenation. This avoids back-leveling CA Librarian or the CA Librarian Access Method (LAM).

ECSA Requirement

During initialization, the LAM Subsystem acquires storage from the Extended Common Service Area (ECSA) to contain the anchor points for control blocks. You can compute ECSA space for the LAM Subsystem using the following formula:

$$\text{ECSA bytes equals } ((\text{MAXUSER plus } 1) \text{ times } 4) = 876 + ((\text{number of wide record master file} - 17) * 48)$$

The MAXUSER parameter is defined in the IEASYSxx member of SYS1.PARMLIB.

Activate LAM Subsystem

At this point, the LAM z/OS and OS/390 Subsystem is ready to be activated. In Release 4.4, LJ44INIT automatically calls LR44INIT to start the LAM subsystem.

A successful initialization of LAM is acknowledged by the following message:

```
LAM0020 LAM SUBSYSTEM SUCCESSFULLY INITIALIZED
```

If the subsystem was not successfully initialized, you can receive any of the following messages:

```
LAM0010 LAM SUBSYSTEM UNSUCCESSFULLY INITIALIZED
```

Indicates that the LAM initialization module was unable to obtain CSA storage.

```
CA-LIBRARIAN *WARNING* LIB/AM OPTION LOAD MODULE (LAMMVS) NOT LOADED, LAM0030 LAM
SUBSYSTEM SUCCESSFULLY INITIALIZED; LIB/AM OPTION IS INACTIVE; LAMMVS NOT FOUND.
```

Indicates CA Librarian did not find the LIB/AM module LAMMVS.

```
CA-LIBRARIAN INITIALIZATION ERROR - SUBSYSTEM INITIALIZATION FAILED
```

Indicates that an error occurred while CAIRIM was initializing the subsystem. This message can be accompanied by CAIRIM messages.

```
CA-LIBRARIAN INITIALIZATION ERROR - INVALID PARAMETERS SPECIFIED
```

Indicates that an invalid CAIRIM parameter was specified.

```
CA-LIBRARIAN INITIALIZATION ERROR - LAMMVS MODULE ALREADY LOADED
```

Indicates that LAM was already initialized.

If you do not receive any of these messages, the LAM subsystem was incorrectly defined to the operating system. Review the activation step.

How to Run Two Versions of the LAM Subsystem

The following procedure is provided for those sites that want to test a new release of the LAM Subsystem and do not have a test system on which to run the new release. This procedure requires the use of the CAIRIM LAM initialization program LJ44INIT. After performing this procedure, you can invoke the new version of LAM by coding the SUBSYS=LAMX JCL parameter instead of SUBSYS=LAM.

Note: This procedure uses a four-character subsystem name of LAMX. You can change the last character. However, the first three characters must be LAM.

CALJJCL library member LRLAMXRM contains a sample CAIRIM parameter to activate the LAMX subsystem. See the *CA Common Services for z/OS and OS/390 Getting Started* and the *CA Common Services for z/OS and OS/390 Administrator Guide* for details on starting or restarting CAIRIM.

To deactivate the LAMX subsystem, restart the CAIRIM task with PARM(DELETE,NAME=LAMX). Deactivating the LAMX subsystem frees any CSA storage that LAMX acquired. Once LAMX is deactivated, you cannot activate it again until the next operating system IPL. However, you can activate another LAM Subsystem with a different name (for example, LAMY).

Note: Access to both CA Librarian CAILIBs (one for each subsystem) must be available to CAIRIM. You can do this by putting it in either the CAS9 STEPLIB or in the system LINKLIB. If you are running a previous version of CA Librarian from the LINKLIST, you must use a STEPLIB to go to the new version in the CAS9 procedure to pick up the new version modules with like names.

Because LIB/AM loads CA Librarian modules at run time, there must be a STEPLIB to the CA Librarian CAILIB if it is not installed in the linklist.

Modifying CAIRIM

To replace an active version of LIB/AM, you must modify the CAIRIM parameter for LIB/AM from:

```
PRODUCT(CA-LIB44) VERSION(LJ44) INIT(LJ44INIT)
```

to:

```
PRODUCT(CA-LIB44) VERSION(LJ44) INIT(LJ44INIT) PARM(REINIT)
```

To execute two versions of LIB/AM concurrently (for testing purposes), you must modify the CAIRIM parameter for LIB/AM from:

```
PRODUCT(CA-LIB44) VERSION(LJ44) INIT(LJ44INIT)
```

to:

```
PRODUCT(CA-LIB44) VERSION(LJ44) INIT(LJ44INIT)  
PARM(REINIT,NAME=LAMX)
```

To invoke the new version of LIB/AM, simply code SUBSYS=LAMX in the JCL.

RIM Rules

The only RIM parm card is:

```
PRODUCT (CA-LIBRARIAN) VERSION (LJ44) INIT(LJ44INIT)
```

The LR44INIT is no longer executed separately, but is called by the LJ44INIT program.

The default function is INIT. The default subsystem name is LAM. Because of these changes, the following parms are accepted as the results:

```
PRODUCT (CA-LIB) VERSION (LJ44) INIT(LJ44INIT) PARM(INIT) or  
PRODUCT (CA-LIB) VERSION (LJ44) INIT(LJ44INIT)  
PARM(INIT,NAME=LAMA)
```

The INIT function searches and uses the CA Librarian load modules, LVSSVC, LAMMVS, and LAMMVS9, if found. Otherwise, they are dynamically loaded into the MLPA (if the LIB/AM option is present). The LAM Subsystem name can be specified for INIT.

```
PRODUCT (CA-LIB) VERSION (LJ44) INIT(LJ44INIT) PARM(DELETE) or  
PRODUCT (CA-LIB) VERSION (LJ44) INIT(LJ44INIT)  
PARM(DELETE,NAME=LAMA)
```

The DELETE function deactivates the CA Librarian Subsystem. It also deletes the dynamically loaded LAMMVS module from the MLPA if the current one is in use by this subsystem.

```
PRODUCT (CA-LIB) VERSION (LJ44) INIT(LJ44INIT) PARM(REINIT) or  
PRODUCT (CA-LIB) VERSION (LJ44) INIT(LJ44INIT)  
PARM(REINIT,NAME=LAMA)
```

Note: Do not use the 'PARM(DELETE)' option on the initial startup of LJ44INIT. This causes the subsystem and CA Librarian to initialize incorrectly and can cause various SOC4 abends.

The REINIT function activates the CA Librarian subsystem (or creates and activates it) and dynamically adds a new copy of LAMMVS to the MLPA (if the LIB/AM option is present).

Optional External Security USERMOD

USERMOD MLJ4406 is provided for sites that have an external security system and *do not* want to have the CA Librarian basic or member level security managed master files. If you apply this USERMOD, CA Librarian uses MCD security for MCD-protected master files, but the CA Librarian security interface to CA Top Secret, CA ACF2, and RACF is disabled. However, you can still use those access control products to protect a master file at the data set level (which does not require the CA Librarian security interface).

Member LJMODSEC on the CALJCL library contains the SMP/E statements required to receive and apply the USERMOD.

Note: Applying this USERMOD does not eliminate the need to install the S910 component.

Execute LAMSERV (Optional)

Execute this step if you are using wide record master files.

The member LAMSERV in the CALJJCL library must be customized and subsequently copied into a valid system procedure library (for example, SYS1.PROCLIB). You must then invoke the LAMSERV proc through a z/OS and OS/390 START command issued from any z/OS and OS/390 system console. LAMSERV must be started on each CPU where CA Librarian executes.

Note: The LAMSERV region requires UPDATE security authority to the VSAM control file that was allocated in Step 9. No other users need access to the control file.

Install ELIPS (Optional)

Important! Each user must recover any pending members and delete member LIBEDRT from the ISPF profile data set if you are going to use the new Wide Record Master Files. ELIPS release 4.2 rebuilds this table to include an LRECL variable.

If you selected FMID CAL4400 at RECEIVE and APPLY time during installation, the ELIPS load modules were link edited into CA Librarian target load library.

Note: You can use the CA Librarian target load library, CAI.CALJLINK, as a LNKLST or a STEPLIB library. If an ISPF ISPLLIB concatenation is used, specify the library in that concatenation.

The following steps are required to complete the installation of ELIPS:

- Assemble and link the ELIPSGEN macro
- (Optional) Customize the ELIPS panels

Assemble and Link the ELIPSGEN Macro

The ELIPSGEN macro must be assembled and link edited to complete the installation of ELIPS. The ELIPSGEN macro is the installation macro for ELIPS. It resides on the macro library (CAI.CALJMAC). Member LUELIGEN on the CALJJCL library contains a job stream to assemble and link edit the macro into your CA Librarian target library.

Note: You must assemble and link edit the ELIPSGEN macro outside of SMP/E.

See the following ELIPSGEN macro parameters for the installation options that ELIPS provides. You can tailor these for your own site's needs.

APANEL=(panelname[,panelname[...[,panelname]]) | (LIBIAS00,LIBIAS01)

This option lets your site define the name of the MAIN and ALTERNATE panels to use for the ARCHIVE LEVEL selection list function.

The first panel defined is the default panel, the one shown when the user first enters the ALT function after entering ELIPS. It is also the ALT 0 screen.

panelname

The name of the panels to use for the ARCHIVE LEVEL selection list function. If a single screen is defined with no alternates, then the parentheses are not needed.

(LIBIAS00,LIBIAS01)

The default, specifies the panels that are provided on the installation tape.

ATYPn=(type,lang,seqcol,seqlen)

Defines the ELIPS Member Type-Language Code translation table.

n

The position in the type/language table where the entered information is placed. A table of default values is shown below. Any position can be changed. Positions 18 through 32 can be added.

type

The member type to enter in the type/language table. The type is used for such purposes as allowing the user to enter a member type for the LONG selection list and naming the edit profile to use.

lang

The 1- to 3-character CA Librarian language code to associate with the member type specified.

seqcol

The default starting column for sequence numbers for this type of member. It must be specified as two digits, in the form nn.

When you add a new member using the ELIPS EDIT function and you enter the language or type on the control information panel, the sequence number starting column is taken from the Type/Language Table starting column specification for the language or member type that you specify in this parameter. If the type is not found in the table, then the master file default is used.

Note: If a starting sequence of 00 is placed in this position, the master file default starting sequence column is used. (These are identified by asterisks in the table below.)

seqlen

The default sequence number length for this type of member. When you add a new member using the ELIPS EDIT function and enter a language or type as required on the control information panel, the sequence number length is changed if the language is found in the type/language table. Otherwise, the master file default is used.

If you place 0 in this position, then the master file default sequence number length is used. (These are identified by asterisks in the table below.)

Note: If an entry is duplicated in the table, it is found on a sequential basis. For example, the default shown in the following table for member type PL1 is language code PL1. For type PL1F, it is also PL1. Therefore, if a language code of PL1 is translated, it is always translated to the member type of PL1 since this appears first on the table; but if a member type of PL1F is entered, it is translated from the table to a language code of PL1.

The following table lists the defaults used in type/language translation.

ATYPn	Member Type	Language Code	Sequence Start	Length
ATYP1	ASM	ASM	73	8
ATYP2	COBOL	COB	01	6
ATYP3	PL1	PL1	73	8
ATYP4	PLIF	PL1	73	8
ATYP5	FORT	FOR	73	8
ATYP6	FORTGI	FRG	73	8
ATYP7	FORTH	FRH	73	8
ATYP8	GOFORT	GOF	73	8
ATYP9	TEXT	TXT	73	8
ATYP10	DATA	DAT	00*	0*
ATYP11	CLIST	CMD	00*	0*
ATYP12	CNTL	JCL	73	8

ATYPn	Member Type	Language Code	Sequence Start	Length
ATYP13	BASIC	BAS	00*	0*
ATYP14	VS BASIC	VS B	00*	0*
ATYP15	RPG	RPG	75	6
ATYP16	GIS	GIS	00*	0*
ATYP17	MACRO	MAC	73	8
ATYP18	COBOL2	CB2	01	6
ATYP19	COBOL3	CB3	01	6
ATYP20	EZTRIEV	EZT	81	6
ATYP21	DYL260	D26	73	8
ATYP22	DYL280	D28	73	8
ATYP23 - 32	Not used	Not used	Not used	Not used

CCFCHK=YES|NO

Cross-checking is done with LIB/CCF to see if the master file is a LIB/CCF-controlled production master file. If it is, only the BROWSE function is allowed on that master file.

YES

Cross checks with LIB/CCF each time a new master file is allocated and restricts access to a LIB/CCF-controlled production master file to BROWSE only.

Note: When CA Top Secret protects all master files in all chains, you do not need to use the ELIPSGEN option CCFCHK=YES. Using CCFCHK=YES adds considerable overhead (to read all the chains in the CCF system master file) to determine the chain access allowed to the master file being opened.

NO

(Default) Does not do this checking.

Note: If LIB/CCF-ISPF is not yet installed at your site, specify CCFCHK=NO. Failure to do so results in an S806 abend for LIB/CCF load module \$CCFCOMI when attempting to access any master file through ELIPS.

CHECK=YES|NO

Specifies whether the LIB/TSO TLICD file checks for access to any update-type function in ELIPS (Edit, Update, Rename). This parameter is provided for sites that use the LIB/TSO interface. If you do not use LIB/TSO, allow this parameter to default to CHECK=NO.

YES

Specifies TLICD checking for each update-type access.

NO

The default. Does not do this checking.

DESC=NO|ADD|ADDSAVE

Specifies whether the DESCRIPTION field must be filled in before an add or an edit update can take place.

NO

The default. Indicates that the user can leave the description field blank.

ADD

Indicates that the user must enter a description for a member being added.

ADDSAVE

Indicates that the user must fill in the blank description field for ADDs, SAVEs, and INFO updates.

EXITnd=(C|L|O,name)

Defines the user exits for ELIPS.

nd

The exit node where the defined exec executes. At present, the only available nodes are FE (function entrance), GA (general allocation), CR (command route), and SE (sub-function entrance). See the System Services Guide for details on the exits.

C|L|O

Specifies the type of exit program used.

C

Command (CLIST or command processor) to execute using the ISPF SELECT CMD service.

L

Load module to execute using the ISPF SELECT PGM service.

O

Object code to link into the ELIPSGEN load module at installation.

name

Name of the CLIST, load module, or program to execute every time this exit node is reached.

HIST=YES|NO

Specifies whether HISTory records are required when updating a member.

YES

HISTory records are required on all updates. If HIST=YES is specified, then, before an update takes place, the CONTROL INFORMATION panel displays with a message indicating that HISTORY is required. If the INFO command is used during EDIT and history records are inserted, they are used and the panel does not redisplay.

NO

HISTory records are not required.

KANA=YES|NO

Specifies whether the HISTORY and DESCRIPTION fields entered on the information update panel are converted to uppercase.

NO

(Default) The HISTORY and DESCRIPTION fields are not converted to uppercase, allowing the use of Katakana in these fields.

YES

The HISTORY and DESCRIPTION fields are converted to uppercase.

Note: History cards are converted to upper case by the ISPF editor when displayed as NOTE lines by the ELIPS HIST command if CAPS(ON) is set in the edit profile. If these were entered using KATAKANA characters, they can be unreadable until the user sets CAPS(OFF).

LMCPAN={panelname,[panelname[...panelname]]} |(ELIPUML0,ELIPUML1,ELIPUML2)

Defines the names of the ALTERNATE panels to use for EDIT COPY Selection lists.

panelname

Indicates the name of the panels to use for the LONG Member Selection list. If a single screen is defined with no alternates, then the parentheses are not needed.

LPANEL=(panelname,[panelname[...panelname]]) (LIBLIBS01,LIBS02)

Defines the name of the MAIN and ALTERNATE panels to use for the LONG Member Selection list. See the section titled Customize Panels later in this chapter for restrictions on the contents of these panels.

The first panel defined is the default panel, and the one shown when the user first enters the LONG selection list after entering ELIPS. It is also the ALT 0 screen.

panelname

Indicates the name of the panels to use for the LONG Member Selection list. If a single screen is defined with no alternates, then the parentheses are not needed.

(LIBS00,LIBS01,LIBS02)

(The default.) Specifies the panels that are provided on the installation tape.

LUDPAN=(panelname[,panelname]) (UTILPN10,UTILPN11)

Specifies the panels for the move/copy utility LONG PDS selection lists.

LUMPAN=(panelname[,panelname[...panelname]]) (UTILPN00,UTILPN01,TILPN02)

Specifies the panels for the move/copy utility LONG master file selection.

MODE=EDIT|BROWSE

Specifies whether selected CA Librarian members can be updated (EDIT mode) or just read (BROWSE mode). If you omit this parameter, the default, EDIT mode, is assumed.

PGMR=NO|ADD|ADDSAVE|SYSUID

Specifies whether PROGRAMMER NAME is required for an update.

NO

Specifies that the user optionally fills in the PROGRAMMER NAME field. The TSO USERID is put into the PROGRAMMER NAME field automatically if the user does not enter a value.

ADD

(The default.) Specifies the PROGRAMMER NAME field must be filled in for an ADD.

ADDSAVE

The user is required to fill in the field for ADDs and SAVEs if it is blank.

SYSUID

ELIPS automatically uses the TSO ID as the PROGRAMMER NAME for all updates.

PRTBLK=blksize|3990

Specifies the transient file block size for the BROWSE function for printer members.

blksize

The block size to use when allocating the transient file when browsing a printer (133 byte) member. The block size must be a multiple of 133.

3990

The default value.

Note: For efficiency, do not change this when using UNIT=VIO, the recommended default.

PSWD=U|R|D|N

Lets the site require the member password for the ELIPS functions listed following:

- U—Requires a password for SAVE, EDIT, RENAME, and EDIT REPLACE.
- R—Requires a password for BROWSE, COPY, PRINT, and EDIT COPY.
- D—Requires a password for DELETE.
- N—(The default.) Requires no passwords.

Note the following:

- Master files initialized with the NOBYPP option require passwords for any type of member access (except for the INFO function), regardless of the PSWD keyword specification in this macro.
- CA Librarian passwords are not intended for use as a security mechanism as they appear in various batch CA Librarian listings and in many online displays. However, you can use them as a check to verify that a member name has been keyed correctly.
- To specify multiple values for the PSWD macro keyword, place the values in parenthesis, separated by a comma. For example: PSWD=(U,R,D).

QALLOW=YES|NO

Specifies whether the SHORT member selection list is allowed to show PROD2 members, even when the MCD was not provided, to force the SHORT member list to use the quick path processing.

Quick path processing accesses member index information only. It is much quicker and more efficient than the normal path.

- YES—You can use quick path processing for all master files. Displays the names of all members, including those with a status of PROD2.
- NO—(The default.) You cannot use quick path processing for Software-Lock-protected master files without a management code.

Note the following:

- If you specify QALLOW=YES, you can modify the ELIPS Main Panel by removing the Q from the selection list choices (L/S/Q). See the section titled ELIPS Main Panel Customization in this chapter for instructions. The reason for doing this is that S and Q provide the same display when QALLOW=YES. However, although removed from the choices displayed on the panel, the Q option is still processed if entered.
- If you are using the access control facility interface, access to a master file or member is determined by the access rules for that master file or member. Therefore, specifying QALLOW=YES can still require that you provide an MCD for a SHORT member selection list. Consult the *Security Administration Guide* for details on the access control facility interface, MCD, and PROD2 status.

SOPGMN=name

The SYSOUT program name (for example: DSPRINT) that is allowed for the PRINT function, in addition to SYSOUT class and destination.

Note: In a CA Spool environment, if you want to allow the dynamic allocation of SYSOUT to a printer from CA Librarian:

1. Set SOPGMN to ESF (or to whatever your system uses to identify the subsystem ID for CA Spool).
2. Apply the special fix that references ESF found in the CALJCL member LSrrLIST.

The CA Spool subsystem must be active.

Alternatively, you can create print files in JES and let CA Spool capture the JES SYSOUT files by way of the XFER or NJE interfaces. If you want to create the files in JES, then the SOPGMN is not required. See your CA Spool documentation for more information on these interfaces.

TLICD=dsname|LIBR.TLICD

The data set name of the TLICD file to use for CHECK= checking. If you specify CHECK=NO, this option is ignored.

- dsname—The data set name of the TLICD file.
- LIBR.TLICD—The default data set name of the TLICD file.

Note: This parameter is for sites that use the LIB/TSO interface. If your site does not use the LIB/TSO interface, allow the CHECK= parameter to default to CHECK=NO and the TLICD= parameter is ignored.

TSOBLK=blksize | 4080

The transient file block size for members.

- blksize—The block size to use when allocating the transient file for EDIT and BROWSE of a non-printer (80 byte) member.
- 4080—The default value.

Note: For efficiency, do not change this block size when using UNIT=VIO (the recommended default).

TYPE=COBOL|type

The default member type to use as a low-level qualifier when allocating any necessary TSO files. Also use for requesting the correct edit profile when the CA Librarian language code for the member is not in the installation Type/Language Table.

UNIT=VIO|unitname

Specifies the UNIT name to use for the EDIT and BROWSE transient file.

- VIO—(The default.) The name of the virtual I/O unit name for your system.
Note: Wide record master file users should be aware that the device, or the device being emulated when VIO, must support the LRECL of the largest members being placed in wide record master files.
- unitname—Can be any normal DASD device unit name, but failing to use VIO substantially degrades ELIPS EDIT and BROWSE performance.

ZEDBDSN=PREFIX|NOPREFIX

Specifies whether the high level qualifier of the RECOVERY DATASET DSN begins with the PREFIX or USERID.

- PREFIX—(The default.) The prefix begins the data set name (for example, prefix.userid.LIB 00NN.BACKUP).
- NOPREFIX—The user ID begins the data set name (for example, userid.LIB 00NN.BACKUP).

ZEDDISP=D|K

Specifies whether the RECOVERY DATASET is deleted or kept.

- D—(The default.) Deletes the data set.
- K—Keeps the data set.

Note: IBM has documented how to pre-allocate the recovery data sets. This keyword is supplied ONLY to allow you to change this table variable per their instructions.

ZEDNUM=8|nn

Specifies the number of entries in the EDIT RECOVERY TABLE. Specify any number from 1 through 99, inclusive. The default is 8.

Customize Panels

A site can choose to modify or add to the panels delivered with ELIPS. The panels are in the form of ISPF table panels. They are modified by directly editing the panel library member; no other steps are necessary. Details on how to create and modify panels are available in the documentation offered by IBM on ISPF Dialog Management Services.

Identifying Panels

Panel names are easily identified using the ISPF command PANELID. This command displays the panel name in the upper left corner of each panel as it is presented. PANELID OFF removes the panel name from the display.

ELIPSGEN Panel Options

You can use the ELIPSGEN options APANEL, LPANEL, LUDPAN, LMCPAN, and LUMPAN to redefine the names of the panels used for various selection lists. If these parameters are not coded, the default ELIPS panels are used. If you choose to modify or completely replace any of these panels, do it with great care. Copy the existing panel member to a new member where you can edit the new member, thereby keeping the original ELIPS panel intact.

Nonmodifiable Panel Content

The following fields, when found in any ELIPS selection panel, are required. Never remove them:

- Selection field
- Member name field
- Password field
- Newname field
- Level field, as found on ARCLIST panels or last updated field.

Removal of any of these fields results in ISPF dialog errors.

ELIPS Main Panel Customization

If the ELIPSGEN option QALLOW=YES is specified, you modify the ELIPS main panel (LIBIP02) to remove the Q from the selection list choices.

To do this, perform the following steps:

1. Edit panel LIBIP02.
2. Change the line containing
`?SELECTION LIST #==>! (L/S/Q)`
to
`?SELECTION LIST #==>! (L/S)`
3. Save the edit change.

Install the CA Roscoe Interface (Optional)

For an CA Roscoe user to access CA Librarian, CA Roscoe must have access to various I/O modules that are contained in the CA Librarian target library (CAI.CALJLINK). You must add the CAI.CALJLINK library name to the CA Roscoe STEPLIB so that CA Roscoe can automatically load the required CA Librarian load modules.

If upgrading from a previous release of CA Librarian, ensure that the pre-4.2 load modules are not accessed by performing the following steps:

1. Delete any of the following CA Librarian load modules from the CA Roscoe load library:
 - FAIRMCLS
 - FAIRMOD
 - FAIRLOC
 - FAIROPN
 - FAIRREC
 - FAIRSEC
 - FAIRERR
 - LVSIUO
 - LVSCOG01
 - LVS4500
2. Remove any pre-4.2 CA Librarian load libraries from the STEPLIB in the CA Roscoe initialization JCL.

3. Add the APF authorized CA Librarian CALJLINK to the CA Roscoe STEPLIB.
4. Optionally, pre-load the CA Librarian base programs. Modify CA Roscoe startup by placing a pre-load statement for each module in the CA Roscoe startup stream. The format of the load statement is:

```
PRELOAD=name,E
```

See CALJLINK member LJLIBPRE for the pre-load parameters.

5. If you use wide-record master files, then make sure LAMSERV is active.
LAMSERV is the started task that keeps a record of all the wide-record master files in the system. Having LAMSERV active is important in a CA Roscoe environment because it enables CA Roscoe commands to present wide-record master files in CA Librarian format rather than in PDS/PDSE format.

Install the ISPF Options

The tables, panels, messages, skeletons, and CLISTS for ELIPS and LIB/CCF were unloaded during Step 8 (APPLY). Before using any of these ISPF options, you must perform the following steps:

1. Concatenate the CA Librarian ISPF libraries *before* the ISPF libraries in your TSO procedure or allocation CLIST as follows:

```
//ISPTLIB DD DSN=CAI.CALJTENU,DISP=SHR LIB/CCF -CLU4401
// DD DSN=CAI.CALUTENU,DISP=SHR ELIPS -CLU4401
//*PANELS
//ISPPLIB DD DSN=CAI.CALJPENU,DISP=SHR LIB/CCF -CLU4401
// DD DSN=CAI.CALUPENU,DISP=SHR ELIPS -CLU44
//*MESSAGES
//ISPMLIB DD DSN=CAI.CALJMENU,DISP=SHR LIB/CCF -CLU4401
// DD DSN=CAI.CALUMENU,DISP=SHR ELIPS -CLU44
//*SKELETONS
//ISPSLIB DD DSN=CAI.CALJSENU,DISP=SHR LIB/CCF -CLU4401
// DD DSN=CAI.CALUSENU,DISP=SHR ELIPS -CLU4401
```

2. Add the CA Librarian option to the ISPF primary menu (IBM panel ISR PRIM):

Note: You can modify ISR PRIM in the IBM panel library or copy ISR PRIM from the IBM panel library to CAI.CALUPENU and modify the copy.

- a. Insert the following in the panel body:

```
L +LIBRARIAN - CA-Librarian options menu
```

- b. Add the following to the &ZSEL parameter:

```
L, 'PANEL(LIBRPDF) NEWAPPL(LIB)'
```

3. (Optional) Modify the CA Librarian panel LIBRPDF in CAI.CALUPENU to remove the LIB/CCF options (If you are not installing LIB/CCF) by deleting lines 6 and 22.

The ISPF options are now properly installed and ready for use.

Copy LIB/CCF Model System

If your site is installing LIB/CCF for the first time, install the LIB/CCF model system. CALJCL library member LJCCFMDL contains sample JCL to allocate and define the LIB/CCF model system and restore the system files from the installation tape.

Important! You must modify the -MCD statements in the LJCCFMDL with client-specific and date-specific information. INITM is the default customer ID. If the customer ID was changed in Step 11, supply the new customer ID on the -MCD statements in LJCCFMDL. See the *Security Administration Guide* for details on the -MCD statement, specifically, the section titled Assigning a Base Code. The model system base code for the System, Test, and History master files is 0000, whereas the base code for the production master file is 0001.

Install LIB/TSO

LIB/TSO is the CA Librarian/TSO interface that consists of nine TSO command processors that can be executed from a CLIST to process members on an CA Librarian master file. The following table lists the command processors, their aliases, and their functions.

Module	Alias	Function
LIBADD	LIBA	LIBADD command adds a new member to a master file.
LIBGET	LIBG	Copies a member from a master file into a TSO data set.
LIBSAVE	LIBS	Updates a member retrieved by the LIBGET command.
LIBDLM	LIBD	Deletes a member from the master file.
LIBINDEX	LIBI	Indexes the members for a single programmer or an entire master file.
LIBLIST	LIBL	Displays information about a member.
LIBCTL	LIBC	Lists the installation requirements and defaults for the LIB/TSO and lists information about the members copied by LIBGET.
LIBEXP	LIBX	Updates a member retrieved by LIBGET or still residing on the master file.
LIBUTI	LIBU	Performs delete and rename functions on the TLICD.

Module	Alias	Function
LIBTSOGN	None	Load module containing common routines and installation defaults for all LIB/TSO commands. The FAIR routines can also be in this module.
LIBTLICD	None	A utility program that creates and maintains the LIB/TSO Control Directory (TLICD).

Installation of LIB/TSO consists of the following steps:

- 19A—Apply USERMOD MLJ4407.
- 19B—Create The LIB/TSO Control Directory (TLICD).
- 19C—Install the HELP commands.

The \$LIBTSO Macro

The \$LIBTSO macro tailors LIB/TSO to your site's requirements. The \$LIBTSO macro generates the LIBTSOGN load module. CALJJCL member LUTSOIN2 contains USERMOD MLJ4407 to let you alter the \$LIBTSO macro parameters.

ATYPn=(type,lan,comment-start,comment-symbol)

This optional parameter adds to or changes any of the CA-supplied entries on the TSO type table. See the section titled LIB/TSO Type Table later in this chapter for complete information on the ATYPn parameters. See also the TYPE= parameter.

CHECK=[NO|YES|ALL]

Specifies whether additional TSO/SPF member checking is performed.

- NO—No checking is performed.
- YES—LIBGET and LIBDLM checks the TLICD to verify that the member is not outstanding to another user through LIBGET.
- ALL—Checking is performed by LIBGET, LIBDLM, and LIBEXP.

CONTROL=[RESERVE|ENQ]

Specifies that the integrity of the TLICD file directory is maintained by either the RESERVE or ENQ facility. (See the section on the TLICD.)

DESC=[YES|NO]

Specifies whether a member description is required when a new member is added to master file through the LIBADD command.

EXITxx=(exit-routine-name,exit-processing-symbols)

Specify an EXITxx keyword for each LIB/TSO command that you want exit processing performed for, where xx is:

- LA for LIBADD
- LC for LIBCTL
- LD for LIBDLM
- LG for LIBGET
- LI for LIBINDEX
- LL for LIBLIST
- LS for LIBSAVE
- LU for LIBUTI
- LX for LIBXP

The *exit-routine-name* identifies the program where control is passed during exit processing. You can specify only one program per command but can use the same program for more than one command. The *exit-routine-name* can be 1 to 8 alphanumeric characters long. The first character is alphabetic or a national character.

The *exit-processing-symbols* identify the type of exit processing to perform for the command. The symbols are:

- CB—Command buffer exit
- FA—File allocation exit
- OP—TSO output exit (LIBGET only)
- TE—Command termination exit

You must specify at least one *exit-processing-symbol*, and can specify two or more by separating them with commas. For example:

```
EXITA=(EXITPGM,CB)
EXITLG=(EXITPGM,CB,FA,OP)
```

Note: See the MASTX= parameter for information on the master file allocation exit.

If you do not specify any EXITxx parameter, exit processing is not performed.

See the *Systems Services Guide* for information on LIB/TSO exit processing.

HIST=[YES|NO]

Specifies whether a history record is required when updating an CA Librarian member through the LIBSAVE or LIBEXP commands.

INC=[NO|RESEQ|NORESEQ|ASIS]

Specifies -INC statement expansion

- **NO**—(Default) Does not expand the -INC statements in an CA Librarian member when the member is copied into a TSO data set through the LIBGET command. Instead, they are converted into comment records.
- **RESEQ**—Expands all -INC statements of an CA Librarian member and resequences the records from an included member according to the sequence numbering attributes of the main member.
- **NORESEQ**—Expands all -INC statements of an CA Librarian member, but the records of the included member are not resequenced. The data set can be out of sequence as a result of using NORESEQ.
- **ASIS**—Copies the member into the data set unchanged, without -INC statement expansion or comment statements.

See the *Batch Command Reference Guide* for further information on -INC statement processing and sample comment statements.

KANA=[YES|NO]

Specifies whether KATAKANA characters are accepted on the HIST and DESC of the LIBADD, LIBSAVE, and LIBEXP commands.

LIBMSG=[TEMP|PERM|TERM]

Specifies where the CA Librarian Update Report is placed during LIBADD, LIBSAVE, LIBDLM, LIBEXP, and LIBINDEX command processing.

- **TEMP**—(Default) Writes the report to a temporary data set and deletes it at the end of command processing.
- **PERM**—Writes the report to a permanent data set.
- **TERM**—Displays the report on the terminal. It is not written to any file.

LIBPARM=['parameter-string'|'NRJS,NJTA']

Specifies execution parameters to use for CA Librarian when it is executed in response to the LIBADD, LIBSAVE, LIBDLM, LIBEXP, or LIBINDEX commands. The parameter string can be no more than 50 characters long and must be enclosed in single quotation marks.

Note: An IEX or OEX parameter included in the *parameter-string* is ignored during execution if the master file being accessed already has an input exit name or an output exit name permanently assigned to it. In such cases, the permanently assigned exit name is used. If the master file does not have a permanently assigned input or output exit name, the exit name specified on this parameter is used. See the *Systems Services Guide for z/OS and OS/390* for information on permanently assigning an input or output exit name to a master file.

LIBRPGM=[batch-program-name | AFOLIBR]

Specifies the nonreentrant program name of CA Librarian used on the PGM field on the Job Control Language EXEC statement. The program must either be link edited into a library in the system LINK list or in a library referenced by the STEPLIB DD statement in the LOGON procedure.

Note: The name specified here must be the same name specified for CA Librarian in Step 12 of the installation procedure.

LIST=[YES | NO]

Specifies whether a member listing is written to a data set when a new member is added to the master file through the LIBADD command or when an existing member is updated through the LIBSAVE and LIBUPD commands.

MASTER=[master-file-name | LIBR.MASTER]

Specifies the default CA Librarian master file used if one is not identified through the SOURCE or DSSOURCE option. The master file name must be a fully qualified data set name from 1 to 44 characters long.

MASTEXT=user-dair-exit-name

Identifies the master file allocation exit program. See the *Systems Services Guide for z/OS and OS/390*. The exit program name must be from 1 to 8 characters long. The user exit program must exist as a load module in a library in the system link list or in a library referenced by the STEPLIB DD in the LOGON procedure.

MASTHI=[high-order-mast-name | LIBR]

Specifies the high-order (leftmost) portion of master file name for the SOURCE option. The high-order portion can consist of one field or several fields separated by periods. Each field can consist of 1 to 8 alphanumeric characters with an initial non-numeric character. The entire high-order portion can be no more than 42 characters long including periods.

MAXMOD=[nn | 5]

Specifies the maximum number of outstanding members per user allowed by the LIBGET command. An outstanding member is one that a LIBGET command retrieved but did not yet return to the master file through a LIBSAVE command. Members retrieved by a LIBGET with the READONLY option specified are not considered outstanding members. The LIB/TSO Control Directory (TLICD) keeps track of outstanding members. You can permit from 1 to 99 outstanding members per user; the number should be the same as in the TLICD.

PDSDIR=[nnnnn | 25]

Specifies the number of directory blocks allocated to a new TSO partitioned data set created by the LIBGET command.

PDSPRI=[nnnnn | 50]

Specifies the primary number of blocks allocated to a new partitioned data set created by the LIBGET command. The size of the block is specified by the TSOBLK parameter.

PDSSEC=[nnnnn | 50]

Specifies the secondary number of blocks allocated to a new TSO partitioned data set created by the LIBGET command. The size of the block is specified by the TSOBLK parameter.

PGMR=[NO|ADD|ADDSAVE]

Specifies whether a programmer name must be specified on the LIBADD, LIBSAVE, and LIBEXP commands.

- NO—Programmer name is not required.
- ADD—(Default) Programmer name is required on the LIBADD command only.
- ADDSAVE—Programmer name is required on the LIBSADD, LIBSAVE, and LIBEXP commands.

PREFIX=[YES|NO]

This parameter determines the prefix to use as the leftmost field of:

- The TSO data set name generated by the LIBADD, LIBGET, LIBSAVE, and LIBEXP commands.
- The TSO data set name if it is specified without quote marks on the TSODSN parameter.
- Master file name if it is specified without quote marks on the DSSOURCE parameter.
- The MSGS, LIST, and INDEX file names generated by LIBADD, LIBDLM, LIBINDEX, LIBSAVE, and LIBEXP.

Under z/OS and OS/390, if PREFIX=YES is specified and a prefix is specified in the profile, the prefix is attached to the data set or master file name. If PREFIX=YES is specified and a prefix is not specified in the profile, the user ID is prefixed to the data set or master file name. If PREFIX=NO is specified, the user ID is used as the prefix. PREFIX=NO must be specified for SVS.

PRTBLK=[nnnnn | 3990]

Specifies the block size of the listing (LIST) and message (PERMMSG, TEMPMSG, and LONGT) files used by the batch CA Librarian. The block size must be specified in multiples of 133 and must be less than the maximum track size of the device or 32718, whichever is less.

PSWD=[D|DG|DGSX|DGSXL|NO]

Specifies whether the member password is required when accessing a member through the LIBDLM, LIBGET, LIBSAVE, LIBEXP, and LIBLIST commands. The password is required when the following variables are specified:

- D—Required only on LIBDLM command.
- DG—Required on LIBDLM and LIBGET commands.
- DGSX—Required on LIBDLM, LIBGET, LIBSAVE, and LIBEXP commands.
- DGSXL—Required on LIBDLM, LIBGET, LIBSAVE, LIBEXP, and LIBLIST commands.
- NO—(Default) Specifies that the password is not required to access an CA Librarian member through LIB/TSO.

Note the following:

- If the master file was initialized with NOBYPP specified, this parameter is ignored and the password is required for all commands.
- CA Librarian passwords are not intended for use as a security mechanism as they appear in various batch CA Librarian listings and in many online displays. However, you can use them as a check to verify that a member name has been keyed correctly.

SPFQN=[major-qname|SPFDSN|SPFEDIT]

Specifies the 1- to 8-character major-qname used by the SPF or ISPF/PDF editor. The default name is SPFEDIT. The qname enforces data set integrity during LIB/ISPF-TSO command processing against SPF or ISPF/PDF editor and utility processing. Since the qname can vary from release to release of SPF and ISPF/PDF, you must be sure to obtain the correct qname. See the *ISPF Installation and Customization Guide*.

TLICD=[data-set-name|LIBR.TLICD]

Specifies the data-set-name of the CA Librarian ISPF-TSO Control Directory (TLICD). The specified data set name must be fully qualified and can be 1 to 44 characters long. The name specified here must be the same as the data set name specified on the FILEOUT DD statement on the LIBTLICD utility execution that creates TLICD. See the *Systems Services Guide* for more information on TLICD.

Note: If you are upgrading from LIB/TSO Release 3.0 or later, the name specified for TLICD must be the same as the currently existing TLICD.

TSOBLK=[nnnnn|3120]

Specifies the block size of a new TSO data set created by the LIBGET command. The data set can be sequential or partitioned. The block size must be specified in multiples of 80 and must be less than the maximum track size of the device or 32720, whichever is less.

TYPE=[type|COBOL]

Specifies the default mode or TSO data set language type if not specified on the LIBADD, LIBGET, and LIBEXP commands.

The type specified here should be the one most commonly used at the site. CA provides 16 assigned types plus 10 unassigned types. You can override the 16 CA-supplied types and reassign all 26 entries.

The following lists the valid types and their meanings.

- ASM—Assembly statements
- BASIC—BASIC statements
- CLIST—TSO commands
- CNTL—JCL and SYSIN for SUBMIT command
- COBOL—ANS COBOL statements
- DATA—Uppercase data
- FORT—FORTRAN statements
- FORTGI—FORTRAN GI statements
- FORTH—FORTRAN H statements
- GIS—Generalized Information System (GIS) routines
- GOFORT—FORTRAN code and Go statements
- PLI—PL/I checkout or PL/I optimizing compiler statements
- PLIF—PL/I(F) Compiler statements
- RPG—Report program generator statements
- TEXT—Upper and lower case text
- VSBASIC—VSBASIC statements

UPDBLK=[nnnn|4080]

Specifies the block size of the update file used by the batch CA Librarian for the LIBADD, LIBSAVE, LIBEXP, LIBDLM, and LIBINDEX commands. The block size must be specified in multiples of 80 and must be less than the maximum device track size or 32720, whichever is less.

Create the TLICD File

TLICD is a directory of users that used the LIBGET command and the members that they copied from CA Librarian master files to TSO data sets through the LIBGET command.

TLICD is a partitioned data set, initialized by the LIBTLICD utility program. Through this utility, you specify the number of TSO users permitted to access members through the LIBGET command and the number of members a single user can access concurrently.

When each user of the system issues a LIBGET command for the first time, a permanent, unique TLICD member is created for that user. The user's user ID is the member name.

LIBGET records the status of the retrieved member and the TSO data set on TLICD file entry. Later, the LIBSAVE command uses the status information in the entry to update the member. The entry on TLICD file is deleted automatically by the LIBSAVE command, or can be deleted on request by the LIBCTL command.

Important! If upgrading from a previous release of CA Librarian and using an existing TLICD file, the file should not be re-initialized as that deletes all the information in the existing TLICD.

Modifying the Sample JCL

CALJJCL member LUTSOIN1 contains sample JCL to create the TLICD file.

The FILEOUT DD statement that defines the new TLICD file must have the same data set name as the data set specified by the keyword TLICD= of the \$LIBTSO macro and ELISPGEN macro. The values for the SPACE= parameter and block size must be calculated as follows:

```
Blksize = 150 x a  
Primary = b + (b/6)  
Secondary = b/6  
Directory= (B/20) + 1
```

where:

a

The number of outstanding members allowed per user (specified in the \$LIBTSO MAXMOD parameter).

b

The number of TSO users.

For example, if the parameter MAXMOD=5 is specified and there are 30 TSO users, then:

```
Blksize = 150 x 5 = 750
Primary = 30 + 30/6 = 35
Secondary = 30/6 = 5
Directory = (30/20) + 1 = 3
```

The block size specified must not exceed the maximum track size of the device or 32720, whichever is less. The SYSIN DD statement of defines the input control statement to the program LIBTLICD.

- FORMAT causes LIBTLICD to create a new TLICD file.
- MODULES specifies, for any one user, the number of members outstanding through the LIBGET command. The number must be the same as that specified on the MAXMOD= parameter of the \$LIBTSO macro.
- USERS specifies the number of TSO users who can access the TLICD file through LIB/TSO.

Example

For example, if the parameter MAXMOD=5 is specified and there are 30 TSO users, then:

```
FORMAT MODULES=5,USERS=37
```

For further information on generating TLICD and for information on maintaining the file, see the *Systems Services Guide*.

Install the LIB/TSO HELP Commands

The LIB/TSO HELP commands reside in the CAI.CALUHENU target library. This library can be made available using one of the following methods:

- Copy CAI.CALUHENU to LUTSOIN4.
- Add CAI.CALUHENU to the SYSHELP concatenation in the TSO logon procedure.

The HELP commands are LIBADD, LIBCTL, LIBDLM, LIBGET, LIBINDEX, LIBLIST, LIBSAVE, and LIBEXP.

Help Aliases

You can assign the CA Librarian/TSO HELP command aliases (LIBA, LIBC, LIBD, LIBG, LIBI, LIBL, LIBS, and LIBX) to the commands using the CALJCL CLIST LUTSOIN3. The assignment of aliases is optional. If the alias names conflict with names currently in use in other commands, you can assign other aliases or no aliases.

Modifying the TSO Command Table

If all LIB/TSO load modules are installed in the link pack area, you must modify the TSO command table (ISPTCM) to include all LIB/TSO command names.

For more information on table modification, see the IBM *SPF for z/OS and OS/390 Installation and Customization Guide*.

LIB/TSO Type Table

The LIBADD, LIBEXP, and LIBGET commands all have a type option to specify the member's contents: program, data, or control records (and if program records, the language). By interpreting the type entry, CA Librarian formats any comment statements it might insert into the member during command processing. To interpret the type entry, CA Librarian relies on the LIB/TSO type table. The type table is generated during installation and contains an entry for each valid member type. Each entry provides the following information:

- Type
- CA Librarian language code
- Starting column for a comment statement for the type
- Symbol used for the comment statement for the type.

CA supplies 16 default entries for the type table and 10 additional unassigned entries. You can use the ATYPn parameter of the \$LIBTSO macro to alter the CA-supplied entries and to generate additional entries on the type table. The 16 CA-supplied default entries are presented on the following table .

Note: The type option is also used for default data set name processing. If default name processing is in effect, the type entry becomes the descriptive-qualifier for the data set name built by the command.

The format for the ATYPn parameter is:

ATYPn=(*type, lan, comment-start, comment-symbol*)

ATYPn

The parameter where n can be any integer from 1 to 26.

type

A 1- to 8-character TSO type. This entry is the type entry for the LIBADD, LIBGET, and LIBEXP commands and the descriptive qualifier for TSO data sets used by these commands. The TSO type *cannot* duplicate any of these command operands.

lan

A 1- to 3-character language code identifying the contents of the member. The code is stored as a -LANG record with the member.

comment-start

The column number where the comment statement for the TSO type must start. Acceptable values are 1 through 10.

comment-symbol

A 1- to 3-character comment statement symbol that the TSO type must use.

For example, to establish a new type entry with the name EBASIC, a language code of EBS, and a double asterisk beginning in column 1 as a comment indicator, specify the following:

```
ATYP17=(EBASIC,EBS,1,**)
```

On the other hand, if you wanted to change any of the established default assignments, you would enter the appropriate ATYPn parameter, indicating the change. When making a change, you must specify all the fields even if you are modifying one of them. For example, if you want to change the comment symbol for BASIC from an asterisk to an at sign (), enter the following:

```
ATYP13=(BASIC,BAS,1,)
```

The following table lists the defaults used in type/language translation.

ATYPn	Member Type	Language Code	Comment Start	Comment Symbol
ATYP1	ASM	ASM	1	*
ATYP2	COBOL	COB	7	*
ATYP3	PL1	PL1	2	/*
ATYP4	PLIF	PLI	2	/*
ATYP5	FORT	FOR	1	C
ATYP6	FORTGI	FRG	1	C
ATYP7	FORTH	FRH	1	C
ATYP8	GOFORT	GOF	1	*
ATYP9	TEXT	TXT	1	*
ATYP10	DATA	DAT	1	*
ATYP11	CLIST	CMD	1	*
ATYP12	CNTL	JCL	1	/**

ATYPn	Member Type	Language Code	Comment Start	Comment Symbol
ATYP13	BASIC	BAS	1	*
ATYP14	VS BASIC	VS B	1	*
ATYP15	RPG	RPG	1	*
ATYP16	GIS	GIS	1	*

Install LIB/CCF-CA Roscoe

In the CA Roscoe environment, LIB/CCF is implemented as a set of RPFs, panels, and ETSO programs.

FMID CLJ4402 (for LIB/CCF CA Roscoe) must be installed.

Release 6.0 or later of CA Roscoe is required if VSAM or PDS masters are used.

The CA Roscoe ETSO facility must be installed.

The following CA Roscoe startup parameters must be specified:

```
RUN=(SOR)
LOOP=32760
LOOPRST=YES
ENQTYPE=ISPF
```

If you are upgrading from CCF release 3.7 or earlier, you must:

- Transfer certain LIB/CCF tables from the CCF-CA-Roscoe library to your system master file using the CCFCN37R RPF.
- Convert your system master file with the supplied conversion routine (CCFCNV37).

Release 4.3 does not operate unless the system master file was converted. See Appendix B of this guide for details on the RPF and conversion program. After you perform this conversion, an additional, *automatic* system master file conversion occurs when selecting Option 12.11.

If you are upgrading from LIB/CCF release 3.8, an automatic system master file conversion occurs.

If you are upgrading from LIB/CCF release 3.9, 4.1, or 4.2, no conversion is necessary.

The LIB/CCF-CA-Roscoe installation procedure involves the following substeps:

- a. Install the LIB/CCF RPF members.
- b. Assemble and link the \$CCFGN macro to specify installation options.
- c. Optionally apply LIB/CCF USERMODS.
- d. Update the Eligible Program List (EPL).
- e. Review the JCL skeletons and modify if necessary.
- f. Modify the LIB/CCF system tables to reflect your installation options.

The following sections describe each substep in detail.

Install the LIB/CCF RPF Members

The LIB/CCF system is composed mainly of CA Roscoe RPFs. These RPFs are contained in CAI.CALJRPF that was downloaded in step 7, where *CAI* is your high-level qualifier. The RPF named LIBCCFGN should be imported, saved as LIBCCFGN, and executed under the CA Roscoe key where the RPFs are to be installed (this key is the LIB/CCF administrator's key). The LIB/CCF RPFs require about 30,000 lines in the CA Roscoe library.

The format of the execution is:

```
LIBCCFGN FROM(CAI.CALJRPF)
```

CAI is replaced with your high-level qualifier. Executing LIBCCFGN installs the following CA Roscoe members:

- \$CHGT100—CCF definition member
- \$CHGJ*nnn*—JCL skeletons

When upgrading to a new LIB/CCF release, the existing tables and JCL skeletons (which were probably customized during the previous installation) are not replaced, with the exception of:

- \$CHGJ002
- \$CHGJ004
- \$CHGJ005
- \$CHGJ009
- \$CHGJ102

Panels:

- \$CHGPAN*n*
- \$CHGPN*nn*

- CDFRPNnn
- CDFRHnnn

LIBCCFGN will rename these existing RPFs:

Name	Renamed to
\$CHGT000	\$CHGT00o
\$CHGT001	\$CHGT01o
\$CHGT002	\$CHGT02o
\$CHGT003	\$CHGT03o
\$CHGT005	\$CHGT05o
\$CHGT008	\$CHGT08o
\$CHGT012	\$CHGT0Co

The corresponding new 4.3 RPFs will then be installed:

- CCF—Driver program
- \$CHGPnnn—Function programs
- \$CHGHnnn—Tutorial programs
- \$CHGSnnn—Service programs
- \$CHGTnnn—System table programs

Update \$CHGT100

Fetch and attach the CA Roscoe member \$CHGT100 and make sure that the following lines reflect the correct values for your site.

- SYSMAST
- SYSBASE

SYSMAST is the data set name of your LIB/CCF system master file. SYSBASE is the MCD base code for the LIB/CCF system master file.

Edit (by overtyping) any incorrect values and update the member.

Note: Only \$CHGT100 will contain SYSMAST and SYSBASE information. If these fields exist in table \$CHGT000 (ISPF Option 12.0), remove them.

Assemble and Link the \$CCFGEN Macro

You must assemble and link edit the \$CCFGEN macro to provide installation options, such as the name of the CA Librarian batch program and the System Master file data set name.

CALJJCL member LJCCFGEN contains a sample job stream to assemble and link edit the \$CCFGEN macro contained in CAI.CAIMAC. Optionally, a LIB/CCF-CA-Roscoe execution library can be allocated.

Note the following:

- You must assemble and link edit the \$CCFGEN macro outside of SMP/E.
- The CCFGEN options load module can be shared between LIB/CCF-CA-Roscoe and LIB/CCF-ISPF if both are installed and share the same System Master file.

You can specify the following keywords where necessary to override the distribution defaults:

LIBCOPY=LIBRCOPY

(Default) The name of the LIBRCOPY program.

LIBNAME=AFOLIBR

The name of the batch CA Librarian program. If your site has renamed CA Librarian, you must specify the new name with this keyword. The default is AFOLIBR. The default is 0000.

SYSMAST=LIBR.LIBCCF.SYSMAST

The data set name of the LIB/CCF System Master file. The default is LIBR.LIBCCF.SYSMAST.

SYSBASE=0000

The BASE MCD of the LIB/CCF System Master file. The default is 0000.

FORMAT=MIXED|UPCASE

The format for printed reports.

- MIXED—Prints reports in mixed case.
- UPCASE—Prints reports in uppercase.

Apply Optional LIB/CCF USERMODS

To apply optional LIB/CCF usermods, follow these steps:

1. Rename LIBRCOPY.
2. Receive/apply optional usermods.

Rename LIBRCOPY

If the LIBRCOPY keyword of the \$CCFGEN macro specified a new name for the LIBRCOPY program in Step 20B, USERMOD MLJ4401 must be applied. Member LJMODCPY on the CALJJCL library contains the SMP/E JCL to receive and apply the USERMOD. Modify the following SMP/E control statement in LJMODCPY:

```
++RENAME(LIBRCOPY) TONAME(xxxxxxxx) .
```

The value of xxxxxxxx is the new name for LIBRCOPY.

DB2 for z/OS and OS/390 Support

If DB2 for z/OS and OS/390 is installed and LIB/CCF is to track changes to DB2 for z/OS and OS/390 source, LIB/CCF USERMODs MLJ4401 and MLJ4303 are required. Members LJMODDB2 and LJMD2DB2 on the CALJJCL library contain the SMP/E JCL to receive and apply the USERMODs. In member LJMODDB2, modify the REP DDDEF statement data set name to reflect the name of your DB2 load library. For more information on DB2 for z/OS and OS/390 support in LIB/CCF, See the *LIB/CCF Implementation Guide*.

Note: When doing the CA Roscoe receives, be sure that you receive LJMODDB2 before LJMD2DB2.

Also, be sure to use members LJMD2DB2, LJMODDB2, and LJMODDB2 for the SMP/E environment.

Update the Eligible Program List

You must identify programs to execute under ETSO in the CA Roscoe Eligible Program List (EPL). This list must be in ascending EBCDIC order. See the *CA Roscoe System Reference Guide* for details on updating the EPL. Use the values specified in CALJJCL member LJCCFEPL. If AFOLIBR or LIBRCOPY were renamed in Step 12 or Step 20C, respectively, modify the EPL entries for those load modules accordingly.

Specifically, update member LJCCFEPL for CAI.CALJJCL by specifying Y under MODE for all CCF programs, AFOLIBR, and LIBRCOPY.

Note the following:

- Add the LIB/CCF execution library to the CA Roscoe ETSOLIB DD statement.
- If the CA Roscoe LIB/CCF access control option is used (that is, if LIBRCCF=px is present in the CA Roscoe startup parameters), the LIB/CCF execution library must also be accessible to a CA Roscoe LOAD at initialization time. Either the LIB/CCF load modules must be in the LPA or the CA Librarian target library, CAI.CALJLINK, and (if created) LIB/CCF load library must be authorized and concatenated to the CA Roscoe load library in the STEPLIB DD concatenation. CA Roscoe does not load modules from the LNKST.
- Verify that the mode for all CA Librarian programs added to the EPL is set to Y. This is necessary to avoid sporadic ETS 30 messages (for example, message ETS30 ILLEGAL SVC ISSUED BY CALLING PROGRAM-SVC 107"). You can alter the mode using CALJCL member LJCCFEPL by inserting a Y in the MODE column for the appropriate member.

Preloading Programs

CA Roscoe allows reentrant programs that execute under ETSO to be loaded at CA Roscoe initialization. Using this option improves performance because the programs are already resident in memory when they are needed for execution. Using this facility is optional. The format of the option is as follows:

```
PRELOAD=name,E
```

name is the name of the program to pre-load. The PRELOAD statement is placed in the CA Roscoe startup stream.

See CALJCL member LJCCFPRE for the pre-load parameters.

Review the JCL Skeletons

After the LIB/CCF JCL skeleton members are copied to the LIB/CCF CA Roscoe key, you need to review the JCL skeletons.

Note: For more information about JCL skeleton members, see the *LIB/CCF Implementation Guide*.

1. Review the following compiler JCL skeletons for conformation with your installation:
 - \$CHGJ010
 - \$CHGJ011
 - \$CHGJ012
 - \$CHGJT10

- \$CHGJT11
 - \$CHGJT12
2. If necessary, add a STEPLIB DD statement for the batch CA Librarian load library to the following skeletons:
- \$CHGJ001
 - \$CHGJ002
 - \$CHGJ004
 - \$CHGJ006
 - \$CHGJ010
 - \$CHGJ011
 - \$CHGJ012
 - \$CHGJ030
 - \$CHGJ031
 - \$CHGJ032
 - \$CHGJ200
 - \$CHGJ201
 - \$CHGJ500
 - \$CHGJ501
 - \$CHGJ102
 - \$CHGJT10
 - \$CHGJT11
 - \$CHGJT12
 - \$CHGJ009
3. Modify \$CHGJ500 to provide the ISPF library names.
4. If necessary, add a STEPLIB DD statement for the LIB/CCF load library that contains the \$CCFCOMI load module to the following skeletons:
- \$CHGJ009
 - \$CHGJ102
5. Execute RPF CCFCBHSK to create skeletons for the batch login skeletons as follows:
- ```
CCFCBHSK DS(CAI.CALJSENU)
```
- Note:** If you are using external security, ensure the SYSMASST has sufficient update access before running CCFCBHSK. For details, see "Basic Security Access Authorities" for your security package in the *Security Administration Guide*.

## Modify the LIB/CCF System Tables

You must do the following from the LIB/CCF administrator CA Roscoe key before you can use the LIB/CCF model system:

- Update Option 12.0 (PROFILE) to specify control group members (using the CNTLID keyword).
- Update Option 12.1 (USER) to specify users.
- Update Option 12.2 (MANAGER) to specify managers.
- Update Option 12.3 (PROGRAMMER) to specify programmers.

See the *LIB/CCF Implementation Guide* for details on the administrator functions, the model system configuration, and a demo script that you can use to walk through a LIB/CCF cycle.

## Executing LIB/CCF-CA Roscoe

After LIB/CCF is installed, you can execute it by entering the name of the entry program:

CCF

Optionally, you can make an option specification as either of the following:

- CCF 3
- CCF 8.2

## Install LIB/CCF-ISPF(TSO)

LIB/CCF-ISPF(TSO) is implemented as an ISPF dialog application.

FMID CALU441 (for LIB/CCF-ISPF) must have been received and applied.

TSO/E version 1.2 or above must be installed.

ISPF/PDF version 2.2 or above must be installed.

If you are upgrading from LIB/CCF release 3.7 or earlier, you must convert your system master file with the supplied conversion routine (CCFCNV37). Release 4.3 does not operate unless the system master file was converted. For more information, see the appendix "Upgrading from LIB/CCF Release 3.7 or Earlier". After you perform this conversion, an additional automatic system master file conversion occurs.

If you are upgrading from LIB/CCF release 3.8, an automatic system master file conversion occurs. For more information, see the appendix "LIB/CCF System Master FileConversion".

If you are upgrading from LIB/CCF release 3.9, 4.1, or 4.2, no conversion is necessary.

The LIB/CCF-ISPF(TSO) installation procedure involves the following substeps:

**Note:** If you are upgrading from a previous release of LIB/CCF, skip substeps D and E.

- A. Assemble and link the \$CCFGEN macro to specify installation options.
- B. (Optional) Apply LIB/CCF USERMODS.
- C. (Optional) Update the TSO authorized program name table.
- D. Review the JCL skeletons and modify as necessary.
- E. Modify the LIB/CCF system tables to reflect your installation options.

## Assemble and Link the \$CCFGEN Macro

You must assemble and link edit the \$CCFGEN macro to provide installation options such as the LIB/CCF administrator ID and the System Master file data set name. CALJJCL member LUCCFGEN contains a sample job stream to assemble and link edit the \$CCFGEN macro contained in CAI.CAIMAC. Optionally, you can allocate a LIB/CCF-ISPF(TSO) execution library.

Note the following:

- You must assemble and link edit the \$CCFGEN macro outside of SMP/E.
- The CCFGEN options load module can be shared between LIB/CCF-CA-Roscoe and LIB/CCF-ISPF if both are installed and share the same System Master file.

You can specify the following keywords where necessary to override the distribution defaults:

### **ADMINID=userid**

The SYSUID of the LIB/CCF administrator responsible for defining default system processing, user IDs, and file information to LIB/CCF through the administrator function panels. Once LIB/CCF is installed, this administrator can define other administrators through the LIB/CCF Option 12.0 ADMINID keyword. See the *LIB/CCF Implementation Guide* for details.

### **APFLIB=SYS1.LINKLIB**

The data set name of the authorized program library where \$CCFP101 resides. \$CCFP101 is an optional program. See Step 21C for more information. If \$CCFP101 is not used, this keyword is ignored. The default is SYS1.LINKLIB.

#### **EXITn=LINK|LOAD**

The value of *n* is the number of the user exit program (0 through 15, excluding 11). LOAD is the default. Regardless of the EXITn= specification, LIB/CCF exits are not invoked unless specified in Option 12.0 of the LIB/CCF administrator functions. See the *LIB/CCF Implementation Guide* for details on the Option 12.0 EXITn keyword and user exits.

- LINK—The exit is linked with the LIB/CCF programs.
- LOAD—(The default.) LIB/CCF issues a program LOAD for the exit at execution time.

#### **FORMAT=MIXED|UPCASE**

The format for printed reports.

- MIXED—Prints reports in mixed case.
- UPCASE—(Default) Prints reports in uppercase.

#### **IEBCLIB=SYS1.LINKLIB**

The data set name of the authorized program library where IEBCOPY resides. The default is SYS1.LINKLIB.

#### **IEBCOPY=IEBCOPY**

The name of the IBM IEBCOPY program. If your site renamed IEBCOPY, you must specify the new name in the \$CCFGEN macro.

IEBCOPY is used when a site chooses to back up load modules before link editing into these libraries. It is used if a test object library is defined to LIB/CCF, so that object modules are moved into a production object library. The default is IEBCOPY.

#### **INTRUPT=YES|NO**

Indicates whether the LIB/CCF programs are interruptable (can be specified as YES to allow testing under TSO TEST). The default is NO.

#### **LNKEDIT=IEWL**

The name of the linkage editor program. The default is IEWL.

#### **LIBCOPY=LIBRCOPY**

The name of the LIBRCOPY program. The default is LIBRCOPY.

#### **LIBNAME=AFOLIBR**

The name of the batch CA Librarian program. If your site renamed CA Librarian, you must specify the new name with this keyword. The default is AFOLIBR.

**SYSBASE=0000**

The BASE MCD of the LIB/CCF System Master file. The default value is 0000.

**SYSMAST=LIBR.LIBCCF.SYSMAST**

The data set name of the LIB/CCF System Master file. The default is LIBR.LIBCCF.SYSMAST.

## Apply Optional LIB/CCF USERMODS

To apply optional LIB/CCF usermods, follow these steps:

1. Rename LIBRCOPY.
2. Receive/apply optional usermods.

### Rename LIBRCOPY

If the LIBRCOPY keyword of the \$CCFGEN macro specified a new name for the LIBRCOPY program in Step 21A, USERMOD MLJ4401 must be applied. Member LJMODCPY on the CALJJCL library contains the SMP/E JCL to receive and apply the USERMOD. Modify the following SMP/E control statement in LJMODCPY:

```
++RENAME(LIBRCOPY) TONAME(xxxxxxxx) .
```

xxxxxxxx is the new name for LIBRCOPY.

**Note:** USERMOD MLJ4401 might already be applied if LIB/CCF-CA-Roscoe is installed.

### DB2 for z/OS and OS/390 Support

If DB2 for z/OS and OS/390 is installed and you are going to use LIB/CCF to track changes to DB2 for z/OS and OS/390 source, LIB/CCF USERMODs MLJ4402 and MLJ4404 are required. CALJJCL members LJMODDB2 and LUMODDB2 contain the SMP/E statements to receive/apply the USERMODs. In member LJMODDB2, modify the REP DDDEF statement data set name to reflect the name of your DB2 load library.

**Note:** USERMOD MLJ4402 (CALJJCL member LJMODDB2) might already be applied if you performed Step 20C (Apply Optional LIB/CCF USERMODS). If so, you only need to apply USERMOD MLJ4404 (CALJJCL member LUMODDB2).

### Update the TSO Table (Optional)

Update the TSO authorized program name table, IKJEFTE8, to add program names \$CCFP101 (optional) and IEBCOPY. Program \$CCFP101 is used only if LIB/CCF option 12.0 specifies EXIT9=YES. See the *IBM System Programming Library for TSO* for more information on IKJEFTE8.

## Review the JCL Skeletons

The LIB/CCF JCL skeleton library (CAI.CALJSENU) is created in Step 7. Review the following compiler JCL skeletons for conformation with your installation:

- \$CCFJ010
- \$CCFJ011
- \$CCFJ012
- \$CCFJT10
- \$CCFJT11
- \$CCFJT12

If necessary, add a STEPLIB DD statement for the batch CA Librarian load library to the following skeletons:

- \$CCFJ001
- \$CCFJ002
- \$CCFJ004
- \$CCFJ006
- \$CCFJ010
- \$CCFJ011
- \$CCFJ012
- \$CCFJ030
- \$CCFJ031
- \$CCFJ032
- \$CCFJ200
- \$CCFJ201
- \$CCFJ500
- \$CCFJ501

Modify \$CCFJ500 to include ISPF libraries.

If necessary, add a STEPLIB DD statement for the LIB/CCF load library that contains the \$CCFCOMI load module to the following skeletons:

- \$CCFJ100
- \$CCFJ102

See the *LIB/CCF Implementation Guide* for more information on JCL skeletons.

## Modify the LIB/CCF System Tables

The LIB/CCF administrator (defined in Step 21A by the \$CCFGEN macro keyword ADMINID) must do the following before you can use the LIB/CCF-ISPF model system:

- Update Option 12.0 (PROFILE) to specify control group members (using the CNTLID keyword).
- Update Option 12.1 (USER) to specify users.
- Update Option 12.2 (MANAGER) to specify managers.
- Update Option 12.3 (PROGRAMMER) to specify programmers.

See the *LIB/CCF Implementation Guide* for details on the administrator functions, the model system configuration, and a demo script that you can use to walk through a LIB/CCF cycle.

## Executing LIB/CCF-ISPF(TSO)

Execute LIB/CCF by selecting Option C on the CA Librarian selection menu (Option L from the main ISPF menu).

## Install LIB/DD

LIB/DD integrates CA Librarian with CA-Datadictionary using interface components of both. During installation, the installation libraries for CA Common Services VPE and the CA Librarian SMP/E target library (CAI.CAILIB) must be available.

Member LJDDLNK on the CALJCLU library contains sample JCL to receive and apply the LIB/DD interface, USERMOD MLJ4408.

Note the following:

- CA-Datadictionary must be installed to install LIB/DD.
- You must specify the CA Common Services VPE distribution library in the USERMOD where noted if CA Common Services is installed in a different SMP/E zone.
- The CWU40LLD DD statement in member LJDDLNK refers to the CA Common Services CWU4000 distribution library.
- Unresolved WXTRN messages are normal. Ignore them.

## Verify the Product

Use CALJCL member LJ44VER (if you installed CA Librarian without LIB/AM) and LR44VER (if you installed LIB/AM). Review the JCL for the following and modify as necessary:

- STEPLIB DD statement data set name.
- EXEC statement for the AFOLIBR program name.
- MASTER DD statement for the library name.

## Install UCRs (Optional)

The member in the CAI.CALJSAMP library (created during the Install) contains INSTUCR to install User Contributed Routines (UCRs). You can find additional information on UCRs in the *Systems Services Guide*.



# Appendix A: Upgrading from LIB/CCF Release 3.7 or Earlier

---

**Note:** This appendix is only for sites that are upgrading from LIB/CCF Important! release 3.7 or earlier.

Release 3.8 introduced the Library Chain Definition Function (LCDF) that eliminated certain LIB/CCF Administrator tables. LCDF lets you define production and test master file pairs and their associated libraries (object, load, history) with any number of intermediate Q/A and reject libraries. Each set of files contains a library chain defining a promotion path for members under development.

One of the primary benefits of LCDF is that all master file definition information is collected into one set of members and is shared by all CCF systems. Also, a file's characteristics are defined only once, regardless of how many library chains it is used in.

LCDF is available in the CA Roscoe, ISPF(TSO) and ISPF(VM/ESA or z/VM) environments as Administrator option 12.11, replacing the Master File Definition Table (12.4), the Production Master File Table (12.6), the History Master File Table (12.7), and the VM/ESA and z/VM Master File Information Table (12.10). The information formerly carried in these tables is now in restructured members on the System Master File.

If you are upgrading to release 4.4 from release 3.7 or earlier, the information in the affected tables must be converted to the new format. LIB/CCF release 4.4 does not operate in the above environments without the information in the new format.

To assist in the upgrade to release 4.4, there is a program to reformat the existing table information and update the System Master File accordingly, allowing work in progress to continue.

This section contains the following topics:

[CCFCNV37](#) (see page 233)

[Execution of CCFCNV37](#) (see page 235)

[Reformatting the System Master File Under CA Roscoe](#) (see page 236)

[Suggested Conversion Procedures \(CA Roscoe and TSO\)](#) (see page 237)

[Suggested Conversion Procedures \(VM/ESA and z/VM\)](#) (see page 238)

[CCFCNV37 Error and Informational Messages](#) (see page 239)

## CCFCNV37

The CCF conversion program is named CCFCNV37. It is link edited into the CCF load library during the install process. CCFCNV37 uses the contents of the following System Master File members to generate the LCDF members required by version 4.4.

For LIB/CCF-CA-Roscoe:

- \$CHGT0004
- \$CHGT0006
- \$CHGT0007

For LIB/CCF-ISPF(TSO):

- \$CCFT0004
- \$CCFT0006
- \$CCFT0007

For LIB/CCF-ISPF(VM/ESA and z/VM):

- \$CCCT0004
- \$CCCT0006
- \$CCCT0007
- \$CCCT0009

In addition, CCFCNV37 optionally converts the Language Definition Table, \$CxxT005, to the 4.4 format that allows eight characters for the language type.

Finally, CCFCNV37 inserts the appropriate chain entry number into existing MMR, MTR, and SLR entries.

Output from CCFCNV37 is a report of any error conditions detected, a file (CCFOUT) containing the CA Librarian control statements to implement the conversion and, if requested through the PARM, direct an update of the CCF System Master. You can define the CCF System Master explicitly or it can be picked up from the \$CCFCOMI module.

As CCFCNV37 converts the various tables, it analyzes the information to determine whether there are conflicts between different definitions of the same resources. Any such error writes a message to CCFPRINT and processing continues, but no updating of the System Master takes place.

In the event of any of the tables having an invalid format, processing terminates immediately.

You can execute the conversion for one or more of the CA Roscoe, TSO ISPF, and VM/ESA or z/VM ISPF environments for CCF; the PARM denotes which.

## Execution of CCFCNV37

CCFCNV37 uses the following files:

### **MASTER**

Defines the CCF System Master File to convert. If you omit this DD statement, CCFCNV37 tries to locate the correct System Master through the \$CCFCOMI module in the CCF load library. If you provide a MASTER DD, the SYSBASE= operand in the parm must define the MCD base for the file.

### **CCFPRINT**

Defines the report file. If omitted, CCFCNV37 tries to use the \$CCFCOMI module to determine the printer definitions required.

### **CCFOUT**

Defines the optional output file where CA Librarian control statements necessary to update the System Master File with the reformatted table and control members are written. If omitted, NOCCFOUT must be specified in the PARM.

### **STEPLIB**

Can define the library containing the \$CCFCOMI module if MASTER or CCFPRINT DD statements are omitted.

The following PARM operands are valid for CCFCNV37:

### **ROSCOE**

Converts the CA Roscoe CCF tables (see below for information on converting in the CA Roscoe environment).

### **TSO**

Converts the TSO/ISPF CCF tables.

### **CMS**

Converts the CMS/ISPF CCF tables.

### **NOTABLE5**

Suppresses conversion of \$CxxT005 members.

### **NOCCFOUT**

Suppresses use of CCFOUT to hold the CA Librarian update control stream.

**SYSBASE=nnnn**

Provides CA Librarian MCD base for the CCF System Master defined in the MASTER DD statement.

**UPDATE**

CCFCNV37 directly updates the CCF System Master during the execution of the conversion. If any table errors are detected during conversion, the update is suppressed.

The UPDATE parameter and the CCFOUT file are not mutually exclusive; you can write the control stream to the output file even though you request direct updating of the System Master File.

**Note:** If your site shares a CCF System Master File between CCF systems running under different environments (for example ISPF(TSO) and ISPF(VM/ESA or z/VM)), then one conversion must be done for all the environments. Failure to do this results in incomplete LCDF tables.

## Reformatting the System Master File Under CA Roscoe

Where CCF is run under CA Roscoe, it is necessary to preprocess the conversion; the tables \$CHGT002, \$CHGT005 and \$CHGT006 normally reside only on the CA Roscoe library, and not on the CCF System Master. To handle this preprocessing and to provide the opportunity to run the whole conversion process online, CCF/CA-Roscoe supplies an RPF named CCFCN37R.

CCFCN37R allows conversion of \$CHGT005, reformats \$CHGT002 and \$CHGT006, and places them onto the CCF System Master, and can execute CCFCNV37 in foreground using ETSO.

Before exercising the option to convert in foreground, ensure that the CA Roscoe procedure ETSOLIB statement defines a library containing the module CCFCNV37, and that the ETSO EPL has CCFCNV37 defined to it. The following EPL entry has been shown to suffice in most circumstances, although a System Master with very large tables and xxxCNTLO members can require an increase in the CPU and memory values:

```
CCFCNV37 0256 0064 0032 N
```

CCFCN37R must be executed under the CA Roscoe CCF Administrator's prefix. The first panel describes the RPF. The second requests conversion options.

If N is placed against "Convert under ETSO," the RPF terminates after completing the conversion preprocessing. The batch conversion, as described elsewhere, should then be used. The other fields on the panel equate to the PARM entries for CCFCNV37.

## Suggested Conversion Procedures (CA Roscoe and TSO)

Following is a guide to the steps to follow when converting to CCF release 4.4 from release 3.7 or earlier. You should suspend CCF activity during the conversion, although if you use the UPDATE parm in Step4, suspension is absolutely necessary during this step only.

1. Decide whether to provide a MASTER DD statement or allow CCFCNV37 to find a \$CCFCOMI module. Using JCL gives explicit control over the System Master converted, but does require the MCD base to be provided.
2. Run CCFCNV37 with the parm made up as follows:
  - CA Roscoe if you run CCF/CA-Roscoe with the chosen SYSMAST
  - TSO if you run CCF/ISPF(TSO) with the chosen SYSMAST
  - VM/ESA and z/VM if you run CCF/ISPF(VM/ESA or z/VM) with the chosen SYSMAST
  - SYSBASE=nnnn if you have a MASTER DD statement

**Note:** If you are converting the CA Roscoe tables, at least the preprocessing must be run under CA Roscoe first.

```
// CONVRT37 JOB B00TH,CLASS=7,MSGCLASS=X
// CONVERT EXEC PGM=CCFCNV37,
// PARM='ROSCOE,TSO,SYSBASE=6789' A
// STEPLIB DD DSN=cai.caljlink,DISP=SHR B
// MASTER DD DSN=libccf.sysmast,DISP=SHR C
// CCFPRINT DD SYSOUT=*
// CCFOUT DD DSN=libr.ccf.update.output, D
// VOL=SER=MULIB2,UNIT=3387,
// DISP=(,CATLG),SPACE=(TRK,(1,1)),
// DCB=(LRECL=87,BLKSIZE=3277,RECFM=FB)
```

The following explains values that appear in the sample JCL:

### A

This parm requests conversion of CA Roscoe and TSO tables. The conversion is done against the System Master defined in C. The update stream is written to the CCFOUT file for subsequent execution.

### B

Defines the load library containing the CCFCNV37 module, and \$CCFCOMI if the MASTER or CCFPRINT statements are not used.

### C

The CCF System Master to convert.

### D

The output file to contain CA Librarian update control stream.

3. Examine the CCFPRINT report. If there are no errors, proceed to the next step. Otherwise you must resolve any anomalies (a complete list of error messages produced by CCFCNV37 appears in a later section).

Most errors are due to conflicts in the definition of CCF resources in the different environments.

4. When all errors are resolved, the System Master can actually be converted. You can achieve this in one of two ways, but first you should take a backup of your System Master using the CA Librarian BKUPTAPE facility.

To convert during the CCFCNV37 run, add UPDATE to the parm and rerun CCFCNV37. The System Master is updated with the new tables and control members. CCF activity must be suspended during this run. Should any new errors arise, the System Master is not updated. Correct the errors and rerun.

As an alternative to directly updating the System Master, you can use the control stream placed into CCFOUT during the last error-free run of CCFCNV37 as input to CA Librarian. In this case, it is imperative that CCF activity be suspended between the run of CCFCNV37 and CA Librarian update run.

5. After conversion is complete, log on to CCF 4.4 and use option 8.9 (available only to the CCF administrator) that displays (or prints) the LCDF chains just generated. Having checked these, you can make any necessary adjustments by using the Administrator's LCDF option, 12.11.

## Suggested Conversion Procedures (VM/ESA and z/VM)

The conversion program is link edited into your LIB/CCF load library during the installation of LIB/CCF. It must be executed under the control of CMS/ISPF, and the CCF System Master File information must be obtained from the \$CCFCOMI module.

The error report file is sent to the user's virtual printer, and the CA Librarian update control stream to the user's virtual punch. Direct updating of the System Master File is not supported.

Use the following steps to execute CCFCNV37:

1. Ensure that the FILEDEF statements for ISPLLIB in your ISPF EXEC define the libraries containing \$CCFCOMI and the LIB/CCF modules.
2. Enter ISPF and invoke Dialog Test - Functions (Option 7.1).
3. In the PGM field, enter CCFCNV37. In the PARM field, define the CCF environments to convert. Enter CMS if VM/ESA or z/VM only. Enter CMS/TSO to process both TSO and VM/ESA and z/VM environments. If you also share your LIB/CCF System Master File with CA Roscoe, you must run the conversion under CA Roscoe. See the previous section.
4. Press Enter. If CCFCNV37 ends with a non-zero return code, errors or anomalies were detected during processing. They are reported in the print file.

5. Exit ISPF and issue **SPOOL PRINT CLOSE** and **SPOOL PUNCH CLOSE**. You can view these files using normal procedures.
6. The print file contains any error messages. Analyze them and resolve any anomalies. You can rerun CCFCNV37 until no more errors are reported.
7. The punch file contains the CA Librarian update control stream necessary to convert the System Master File. Fill in the -MCD statement with the correct management code for the System Master File. Next, pass the control stream to the LIBEXP command.

You can use the following commands as an example of this process:

```
SPOOL PUNCH *
SPOOL PRINT *
 Invoke ISPF 7.1 to run CCFCNV37
SPOOL PUNCH CLOSE
SPOOL PRINT CLOSE
RECEIVE spoolid fn ft fm
LIBEXP / fn ft fm
```

## CCFCNV37 Error and Informational Messages

### **CCF000 PARM DATA WAS:**

**Reason:**

Informational. Echoes the parameters supplied.

**Action:**

None.

### **CCF001 NO PARM FIELD SUPPLIED**

**Reason:**

Error: A parm was not supplied to CCFCNV37.

**Action:**

Supply the parm to CCFCNV37.

**CCF002 INVALID PARM SUPPLIED**

**Reason:**

Error. A parm or parms contained unknown data.

**Action:**

None.

**CCF003 INVALID PARM COMBINATION**

**Reason:**

Error. An invalid combination of parameters was supplied on the parm.

**Action:**

None.

**CCF004 JCL MASTER PRE-ALLOCATION USED**

**Reason:**

Informational. The CCF SYSMAST used was defined in the MASTER DD statement

**Action:**

None.

**CCF005 JCL CCFPRINT PRE-ALLOCATION USED**

**Reason:**

Informational. A CCFPRINT DD statement was supplied.

**Action:**

None.

**CCF006 SYSBASE= ON PARM, BUT NO MASTER DD SUPPLIED**

**Reason:**

Error. The CCF System Master was determined from \$CCFCOMI, but MCD information was found on the parm.

**Action:**

Add MASTER DD or remove SYSBASE= from the parm.



**CCF007 CCFOUT DD MISSING (NOCCFOUT NOT ON PARM)**

**Reason:**

Error. If CCFOUT use is not suppressed, the DD statement must be supplied.

**Action:**

None.

**CCF008 DIRECT UPDATE STREAM FLUSHED**

**Reason:**

Informational. UPDATE was supplied on the parm, but an error was detected during conversion. The System Master was not updated.

**Action:**

None.

**CCF010 MASTER DD SUPPLIED, BUT NO SYSBASE= ON PARM**

**Reason:**

Error. If the CCF System Master is allocated through JCL, SYSBASE= must be used to provide the MCD base.

**Action:**

Remove MASTER DD or provide SYSBASE=.

**CCF011 TABLE xxxxxxxx NOT ON SYSTEM MASTER**

**Reason:**

Error. The table printed could not be found.

**Action:**

If all the tables are missing, check the MCD Lock base. If \$CHGT006 is missing, check if RPF CCFCN37R was run.

**CCF012 ERROR IN LIBRARIAN PROCESSING; SEE REPORT**

**Reason:**

Error. UPDATE was specified, but an error occurred while updating the System Master. The CA Librarian error report was placed on the CCFPRINT data set.

**Action:**

None.

**CCF013 CHAIN GROUP INCONSISTENCY FOR APPLICATION: XXXXXXXXXXXX**

**Reason:**

Error. The printed application name has conflicting chain names defined in the \$CxxT002 tables. Only one chain name is allowed per application. Resolve the conflict and rerun.

**Action:**

None.

**CCF014 INSUFFICIENT MEMORY FOR INTERNAL TABLES.**

**Reason:**

Error.

**Action:**

Increase the region size and retry.

**CCF015 QUASAR ISSUED RETURN CODE: Nn**

**Reason:**

Error. The internal table-handler detected a logic error.

**Action:**

Contact Technical Support.

**CCF016 FOR CHANGE REQUEST WOnnnnnn, NO CHAIN GROUP EXISTS FOR APPL: xxxxxxxx**

**Reason:**

Warning. The printed change request is for an application not defined in CCF \$CxxT002 tables. This is not in itself an error, but can cause later error messages.

**Action:**

None.

**CCF017 CONVERSION TERMINATED DUE TO PREVIOUS ERROR(S)**

**Reason:**

Informational. Appears at the end of CCFPRINT listing if an error was detected.

**Action:**

None.

**CCF018 FORMAT ERROR IN MEMBER xxxxxxxx**

**Reason:**

Error. Member xxxxxxxx has invalid format. Processing terminates immediately.

**Action:**

Refer to CCF documentation for formats of control members.

**CCF019 ERROR IN MEMBER xxxxxxxx STARTING AT RECORD nnnnnnnn**

**Reason:**

Error. An error was detected at CA Librarian sequence number nnnnnnnn in member xxxxxxxx. The actual error is described in a subsequent message.

**Action:**

None.

**CCF020 INVALID RECORD TYPE: X**

**Reason:**

Follows CCF019. The record type of the T004 set is not P, Q, F, or R.

**Action:**

Correct the record type and retry.

**CCF021 CHARACTERISTICS INCONSISTENT WITH EARLIER DEFINITION  
(xxxxxxx) FOR: Dsn**

**Reason:**

Follows CCF019. Where the same resource is defined for a second or subsequent time, CCFCNV37 checks that key information is not conflicting. In checking *dsn*, the type of data xxxxxxxx does not agree with a previous entry.

**Action:**

Resolve conflict and rerun.

**CCF022 NO PREVIOUS LDR ENTRY FOR xxxxxxxx DATA SET dsn**

**Reason:**

Error. LDR (Library Definition Record) entries are created from data held in CCF tables \$CxxT004, \$CxxT006, and \$CCCT009. While processing table xxxxxxxx, a reference was made to *dsn* which was not previously encountered.

**Action:**

None.

**CCF023 \$CCCT009 LIBRARY TYPE CONFLICT FOR: Dsn**

**Reason:**

Error. Under VM/ESA and z/VM, an CA Librarian Master File can be BDAM, VSAM, or VM/ESA and z/VM format. For *dsn*, the format conflicts with an earlier definition.

**Action:**

None.

**CCF024 NO "F" ENTRY FOR CHAIN GROUP xxxxxxxx PROD MASTER dsn**

**Reason:**

Error. A chain with Q/A entries must have an F entry to define the first-level Q/A library for a Production master.

**Action:**

Correct the conflict and retry.

**CCF025 C/R WOnnnnnn FOUND IN xxxxxxxx HAS NO WOnnnnnn ENTRY IN SYSMAST**

**Reason:**

Error. The xxxxxxxx table contains an entry referring to the printed change request, but this does not exist in the System Master.

**Action:**

Correct the error and retry.

**CCF026 COMBINATION OF PROD AND CURRENT MASTERS AT *xxxxxxxx* SET FROM *nnnnnnnn* IS NOT IN A DEFINED CHAIN****Reason:**

Error. The record set starting at CA Librarian sequence number *nnnnnnnn* in table *xxxxxxxx* contains a combination of masters that does not exist in any chain defined for the entry's application.

**Action:**

Correct the error and retry.

**CCF028 SLRCNTLO ENTRY AT *nnnnnnnn* HAS UNLOCATEABLE PRODMAST/PRODLOAD-LDR Combination****Reason:**

Error. The System Link Record (SLR) entry at CA Librarian sequence number *nnnnnnnn* refers to a Production Load library that was not defined as used by the Production Master in any *SCxxT006* entry.

**Action:**

Correct the error and retry.

**CCF029 MVS TABLES *CHGT006* AND *CCFT006* CONFLICT AT ENTRY *nnnnnnnn*. *CHGT006* ENTRY WILL BE USED.****Reason:**

Warning. If both CCF/CA Roscoe and CCF/TSO/ISPF are in use with the same SYSMAS, the T006 table should agree. A conflict was found in the TSO table *CCFT006* at Librarian sequence number *nnnnnnnn*. The previously defined *CHGT006* entry for the Production master is used during later processing.

**Action:**

None.

**CCF099 FOLLOWING SYSMAS, DYNAMICALLY ALLOCATED: *Dsn*****Reason:**

Informational. A MASTER DD statement was not supplied, and the printed data set name was obtained from *CCFCOMI*.

**Action:**

None.



# Appendix B: LIB/CCF System Master File Conversion

---

This appendix describes the automatic conversion of the LIB/CCF System Master File records that occurs through the normal operation of LIB/CCF release 4.3.

LIB/CCF now supports VM/ESA, z/VM, and DB2. Consequently, the format of certain LIB/CCF control records stored on the System Master File has changed:

- A library definition (LDR) now contains a four-character VM/ESA and z/VM address instead of a three-character VM/ESA and z/VM address.
- An LCDF chain now contains a field for a DB2 DBRM library name.

Therefore, an *automatic* conversion of these records takes place through release 4.3 LIB/CCF processing. When entering Option 12.11 of LIB/CCF, the conversion occurs automatically if there are release 3.8 chains or library definitions found on the System Master File. If no release 3.8 chains or library definitions are found, no conversion is necessary. Once the process is complete, LCDF displays the message CONVERSION PERFORMED. Press PF1 to display the message CDF066: LCDF HAS CONVERTED FROM 3.8 TO 4.3 FORMAT. LCDF checks for release 3.8 chains or library definitions every time Option 12.11 is entered and performs the conversion whenever necessary.

Attempting to use an unconverted release 3.8 format System Master File with any release 4.3 LIB/CCF function that requires LCDF information (other than Option 12.11) results in the message OLD CHAIN/LDR. Pressing PF1 displays the following message:

```
CDF067 T4nnnnn/T5nnnnnn MUST BE CONVERTED BEFORE USE.
```

Once the conversion process is complete, it is still possible to execute release 3.8 LIB/CCF against the release 4.3 System Master File. However, the following restrictions apply:

- If a library definition was updated with a four-character VM/ESA and z/VM address through Option 12.11.3 of release 4.3, release 3.8 displays the address as XXX. If this library definition is used with release 3.8 LIB/CCF, it must be corrected through Option 12.11.3 of release 3.8 by entering a valid three-character VM/ESA and z/VM address. Otherwise, LIB/CCF supplies the invalid address of XXX for subsequent processing. Thus, correcting the address converts the library definition back to the release 3.8 format.
- If Option 12.11.2 is used to modify a chain, that chain is converted back to the release 3.8 format, that is, the DBRM library name field is removed.

For the purposes of testing release 4.3, you can execute both release 3.8 and 4.3 LIB/CCF against the same 4.3 System Master File. However, once release 4.3 is fully implemented, we strongly recommend that you discontinue using release 3.8 to avoid confusion due to the restrictions listed previously.



# Index

---

## A

- acquiring the product • 13, 38
- acquisition
  - download • 28, 39
- adding
  - custom data set • 109
  - data destination • 83
  - FTP locations • 78
  - product • 107
  - system • 133
- aggregated package, viewing • 54
- allocate and mount • 143
- authorization
  - modes • 69

## C

- CA MSM access
  - login • 37
- CA MSM usage scenarios • 28
- CAI.SAMPJCL
  - library • 164
  - sample jobs • 164
- catalog, update • 38
- confirming deployment • 104
- contact system • 75
- contacting technical support • 4
- copy files to USS directory • 146, 147, 150
- creating
  - data destination • 82
  - deployment • 92
  - methodology • 116
  - monoplex • 66
  - shared DASD cluster • 67
  - staging • 68
  - sysplex • 66
- custom data sets
  - add • 109
  - edit • 112
  - remove • 115
  - view • 108
- customer support, contacting • 4

## D

- data class • 132

- data set name mask • 119
- data sets, file systems
  - data destinations
    - add • 83
    - create • 82
    - delete • 86
    - edit • 84
    - maintain • 84
    - set default • 86
- default
  - data destination • 86
  - FTP location • 80
- deleting
  - data destination • 86
  - development • 103
  - system registry • 77
- delivery, product acquisition • 13
- deployments
  - confirm • 104
  - create • 92
  - current state • 90
  - delete • 103
  - maintain • 99
  - preview • 96
  - reset status • 102
  - select a product • 106
  - select a system • 133
  - summary • 134
  - validation, failed • 73
  - view • 96
- distribution
  - tape • 13
- distribution tape • 13
- download • 28, 39
  - files using ESD • 139
  - installation packages • 28, 39
  - LMP keys • 49
  - maintenance packages • 28, 51, 52
  - options • 146
  - overview • 137
  - to mainframe through a PC • 150
  - using batch JCL • 147

## E

- edit

---

- custom data set • 112
- edit, data destination • 84
- methodology • 129
- ESD (Electronic Software Delivery) • 13
- external HOLDDATA • 159
- external packages
  - installation • 41, 43
  - migration • 40, 53

## F

- failed validation • 73
- free space • 142
- FTP locations
  - add • 78
  - edit • 79
  - remove • 80
  - set default • 80

## G

- GIMUNZIP utility • 152
- GROUPEXTEND mode • 59

## H

- hash setting • 152
- high-level qualifier • 152
- HOLDDATA • 159
  - external • 159
  - internal • 159

## I

- IEBCOPY • 164
- installation • 28, 43
- installation packages
  - download • 39
  - migration • 40
- installing
  - from Pax-Enhanced ESD • 137
  - from tape • 161
- Integrated Cryptographic Services Facility (ICSF) • 152
- internal HOLDDATA • 159
- investigating failed validation • 73

## J

- Java version support • 152

## L

- libraries
  - acquiring the product • 13, 38
  - acquisition
    - download • 28, 39
  - adding
    - custom data set • 109
    - data destination • 83
    - FTP locations • 78
    - product • 107
    - system • 133
  - aggregated package, viewing • 54
  - allocate and mount • 143
  - authorization
    - modes • 69
  - CA MSM access
    - login • 37
  - CA MSM usage scenarios • 28
  - CAI.SAMPJCL
    - library • 164
    - sample jobs • 164
  - catalog, update • 38
  - confirming deployment • 104
  - contact system • 75
  - contacting technical support • 4
  - copy files to USS directory • 146, 147, 150
  - creating
    - data destination • 82
    - deployment • 92
    - methodology • 116
    - monoplex • 66
    - shared DASD cluster • 67
    - staging • 68
    - sysplex • 66
  - custom data sets
    - add • 109
    - edit • 112
    - remove • 115
    - view • 108
  - customer support, contacting • 4
  - data class • 132
  - data set name mask • 119
  - data sets, file systems
    - data destinations
      - add • 83
      - create • 82
      - delete • 86
      - edit • 84

---

- maintain • 84
- set default • 86
- default
  - data destination • 86
  - FTP location • 80
- deleting
  - data destination • 86
  - development • 103
  - system registry • 77
- delivery, product acquisition • 13
- deployments
  - confirm • 104
  - create • 92
  - current state • 90
  - delete • 103
  - maintain • 99
  - preview • 96
  - reset status • 102
  - select a product • 106
  - select a system • 133
  - summary • 134
  - validation, failed • 73
  - view • 96
- distribution
  - tape • 13
- download • 28, 39
  - files using ESD • 139
  - installation packages • 28, 39
  - LMP keys • 49
  - maintenance packages • 28, 51, 52
  - options • 146
  - overview • 137
  - to mainframe through a PC • 150
  - using batch JCL • 147
- edit
  - custom data set • 112
  - edit, data destination • 84
  - methodology • 129
- ESD (Electronic Software Delivery) • 13
- external HOLDDATA • 159
- external packages
  - installation • 41, 43
  - migration • 40, 53
- failed validation • 73
- free space • 142
- FTP locations
  - add • 78
  - edit • 79
  - remove • 80
  - set default • 80
- GIMUNZIP utility • 152
- GROUPEXTEND mode • 59
- hash setting • 152
- high-level qualifier • 152
- HOLDDATA • 159
- IEBCOPY • 164
- installation • 28, 43
- installation packages
  - download • 39
  - migration • 40
- installing
  - from Pax-Enhanced ESD • 137
  - from tape • 161
- Integrated Cryptographic Services Facility (ICSF) • 152
- internal HOLDDATA • 159
- investigating failed validation • 73
- Java version support • 152
- LMP keys • 49
- maintain
  - data destinations • 84
  - deployment • 99
  - maintain by list, system register • 76
  - system registry • 70
- maintenance • 157
  - application • 28, 55
  - backout • 63
  - GROUPEXTEND mode • 59
  - USERMODs • 59
- maintenance packages
  - backout • 63
  - download • 28, 51, 52
  - installation • 28, 55, 58
  - migration • 53
  - USERMODs • 59
  - viewing status • 58
- methodology
  - create • 116
  - remove • 131
  - symbolics qualifiers • 119
- migrations
  - installation packages • 40
  - maintenance packages • 53
- monoplex
  - create • 66
- nested packages • 54
- pax ESD procedure
  - copy product files • 146

---

- 
- create product directory • 151
  - download files • 139
  - set up USS directory • 142
  - pax file
    - copy files to USS directory • 146, 147, 150
  - process overview • 137
  - product
    - acquisition • 13
  - product download window • 139
  - product-level directory • 151
  - products
    - acquired externally • 41, 53
    - add • 107
    - download • 28, 39
    - installation • 28, 43
    - maintenance • 28, 55, 63
    - remove from deployment • 107
  - read me • 137, 152
  - remote credentials
    - add • 87
    - delete • 89
    - edit • 88
  - remove
    - custom data sets • 115
    - FTP locations • 80
    - methodologies • 131
    - product • 107
    - system • 134
  - reset status • 102
  - sample JCL • 164
  - sample jobs • 147, 151
    - CAtoMainframe.txt • 147
    - Unpackage.txt • 151
  - scenarios, usage • 28
  - SMP/E
    - GIMUNZIP utility • 152
  - SMP/E environments
    - creation • 46
    - migration • 28
  - software
    - delivery • 13
    - inventory • 38
  - support, contacting • 4
  - symbolic qualifiers • 119
  - system
    - add • 133
    - remove • 134
  - system registry
    - authorization • 69
    - create non-sysplex • 65
    - create, data destination • 82
    - create, shared DASD cluster • 67
    - create, staging • 68
    - create, sysplex • 66
    - delete • 77
    - maintain • 64
    - maintain using list • 76
    - view • 64
  - tape, installing from • 161
  - technical support, contacting • 4
  - UNIX System Services (USS)
    - access requirements • 137, 142
    - directory cleanup • 156
    - directory structure • 142
  - UNZIPJCL • 152
  - USERMODs • 59
  - viewing
    - aggregated package • 54
    - custom data sets • 108
    - deployment • 96
    - maintenance package status • 58
    - product list • 106
    - system list • 133
    - system registry • 64
    - zFS candidate volumes • 76
  - LMP keys • 49
- ## M
- maintain
    - data destinations • 84
    - deployment • 99
    - maintain by list, system register • 76
    - system registry • 70
  - maintenance • 157
    - application • 28, 55
    - backout • 63
    - GROUPEXTEND mode • 59
    - USERMODs • 59
  - maintenance packages
    - backout • 63
    - download • 28, 51, 52
    - installation • 28, 55, 58
    - migration • 53
    - USERMODs • 59
    - viewing status • 58
  - methodology
    - create • 116
-

---

- remove • 131
- symbolics qualifiers • 119
- migrations
  - installation packages • 40
  - maintenance packages • 53
- monoplex
  - create • 66

## N

- nested packages • 54

## P

- pax ESD procedure
  - copy product files • 146
  - create product directory • 151
  - create product-specific directory • 152
  - download files • 139
  - set up USS directory • 142
- pax file
  - copy files to USS directory • 146, 147, 150
- process overview • 137
- product
  - acquisition • 13
- product download window • 139
- product-level directory • 151
- products
  - acquired externally • 41, 53
  - add • 107
  - download • 28, 39
  - installation • 28, 43
  - maintenance • 28, 55, 63
  - remove from deployment • 107

## R

- read me • 137, 152
- remote credentials
  - add • 87
  - delete • 89
  - edit • 88
- remove
  - custom data sets • 115
  - FTP locations • 80
  - methodologies • 131
  - product • 107
  - system • 134
- reset status • 102

## S

- sample JCL • 164
- sample jobs • 147, 151
  - CAtoMainframe.txt • 147
  - Unpackage.txt • 151
- scenarios, usage • 28
- SMP/E
  - GIMUNZIP utility • 152
- SMP/E environments
  - creation • 46
  - migration • 28
- software
  - delivery • 13
  - inventory • 38
- software delivery • 13
- support, contacting • 4
- symbolic qualifiers • 119
- system
  - add • 133
  - remove • 134
- system registry
  - authorization • 69
  - create non-sysplex • 65
  - create, data destination • 82
  - create, shared DASD cluster • 67
  - create, staging • 68
  - create, sysplex • 66
  - delete • 77
  - maintain • 64
  - maintain using list • 76
  - view • 64

## T

- tape, installing from • 161
- technical support, contacting • 4

## U

- UNIX System Services (USS)
  - access requirements • 137, 142
  - directory cleanup • 156
  - directory structure • 142
  - product directory cleanup • 156
- UNZIPJCL • 152
- USERMODs • 59

## V

- viewing

---

aggregated package • 54  
custom data sets • 108  
deployment • 96  
maintenance package status • 58  
product list • 106  
system list • 133  
system registry • 64

## Z

zFS candidate volumes • 76