

CA PMA Chargeback™

Installation Guide

12.5



This documentation and any related computer software help programs (hereinafter referred to as the "Documentation") are for your informational purposes only and are 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 used or disclosed by you except as may be permitted in 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 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 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 THE END USER 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 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 Product References

This document references the following CA products:

- CA Common Services for z/OS
- CA JARS[®] Resource Accounting (CA JARS RA)
- CA Mainframe Software Manager (CA MSM)
- CA Datacom

Contact CA

Contact Technical Support

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

- 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

Provide Feedback

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

If you would like to provide feedback about CA product documentation, complete our short [customer survey](#), which is also available on the CA Support website, found at <http://ca.com/docs>.

Contents

Chapter 1: Overview	9
Audience	9
How the Installation Process Works	10
Chapter 2: Preparing for Installation	11
Hardware Requirments	11
Software Requirements	11
CA Common Services Requirements	11
Security Requirements	13
Storage Requirements	13
TSO Requirements	13
DASD Requirements	13
Concurrent Releases	15
Chapter 3: Installing Your Product Using CA MSM	17
CA MSM Documentation	17
Getting Started Using CA MSM	18
How to Use CA MSM: A Scenario	18
Access CA MSM Using the Web-Based Interface	27
Acquiring Products	28
Update Software Catalog	28
Download Product Installation Package	29
Migrate Installation Packages Downloaded External to CA MSM	30
Download Multiple Product Installation Packages	31
Add a Product	32
Delete a Product	34
Installing Products	34
Install a Product	34
Create a CSI	38
Download LMP Keys	39
Maintaining Products	40
How to Apply Maintenance Packages	40
Download Product Maintenance Packages	41
Download Maintenance Packages for Old Product Releases and Service Packs	41
Manage Maintenance Downloaded External to CA MSM	43
Manage Maintenance	44

GROUPEXTEND Mode	48
Back Out Maintenance	51
Setting System Registry	52
About System Registry	52
Create Non-Sysplex System	53
Create Sysplex or Monoplex	55
Create Staging System	57
Create Shared DASD Cluster	58
Authorization	59
Maintain a System Registry	59
Delete a System Registry	67
Data Destinations	67
FTP Locations	75
Remote Credentials	77
Deploying Products	80
About Deployments	80
Create a Deployment using the Product Wizard	80
View a Deployment	87
Maintain Deployments	88
Delete a Deployment	93
Delete a Completed Deployment	94
Confirm a Deployment	94
Products	96
Custom Data Sets	97
Methodologies	106
Systems	123
Deployment Summary	125

Chapter 4: Installing Your Product From Pax-Enhanced ESD **127**

How to Install a Product Using Pax-Enhanced ESD	127
How the Pax-Enhanced ESD Download Works	129
ESD Product Download Window	129
USS Environment Setup	132
Allocate and Mount a File System	133
Copy the Product Pax Files into Your USS Directory	134
Download Using Batch JCL	135
Download Files to Mainframe through a PC	138
Create a Product Directory from the Pax File	139
Example Job to Execute the Pax Command (Unpackage.txt)	140
Copy Installation Files to z/OS Data Sets	140
Receiving the SMP/E Package	142
How to Install Products Using Native SMP/E JCL	142

Prepare the SMP/E Environment for Pax Installation	143
Run the Installation Jobs for a Pax Installation	144
Clean Up the USS Directory	145
Apply Maintenance	146
HOLDDATA	147

Chapter 5: Installing Your Product From Tape 149

Unload the Sample JCL from Tape	150
How to Install Products Using Native SMP/E JCL	151
Prepare the SMP/E Environment for Tape Installation.....	152
Run the Installation Jobs for a Tape Installation.....	153

Chapter 6: Apply Maintenance 153

HOLDDATA	155
----------------	-----

Chapter 7: Configuring Your Product 157

Step 1. Review System Requirements and Database Installation	157
Step 2. Complete the Worksheet	158
Step 3. Tailor LMP Keys	160
Step 4. Run cBASE Link-Edit	160
Step 5. Run cBASE Data Dictionary Link-Edit for CA Datacom.....	160
Step 6. Run DB2 BIND Procedure	161
Step 7. Allocate CAIKSPAR	161
Step 8. Customize CAIKSPAR.....	161
Step 9. Prepare the Database	162
Step 9A. Prepare CA Datacom/DB.....	162
Step 9B. Prepare CA Datacom/AD Database	162
Step 9C. Prepare DB2 Database	163
Step 10. Create Schema for CA Datacom Users	163
Step 11. Create and Load Tables	164
Step 12. Allocate CAIKRPAR	165
Step 13. Customize CAIKRPAR	166
Step 14. Process DataManager IVP	166
Step 15. Print ORD Data File	166
Step 16. Process CA PMA Chargeback IVP	167
Step 17. Print CA PMA Chargeback Reconciliation File	167
Step 18. Generate CA PMA Chargeback Invoices	167
Step 19. Customize DataManager Online and CA PMA Chargeback Online	168
Step 20. Invoke DataManager Online	169
Step 21. Invoke CA PMA Chargeback Online	170
Step 22. Prepare for Live Data	170

Step 23. Grant Access to Additional Users	171
Step 24. Implement Security	172
Chapter 8: Migration Information	173
Update Database Tables	173
Appendix A: Troubleshooting	175
Verifying the Problem	175
Collecting Diagnostic Data	175
Interpreting Diagnostic Data	177
Index	179

Chapter 1: Overview

This guide describes how to install and implement CA PMA Chargeback.

This section contains the following topics:

[Audience](#) (see page 9)

[How the Installation Process Works](#) (see page 10)

Audience

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

You may need to work with the following personnel:

- Systems programmer for z/OS and VTAM definitions
- Storage administrator, for DASD allocations
- DB2 or CA Datacom database administrator

How the Installation Process Works

The following steps describe the installation process:

1. Prepare for the installation by confirming that your site meets all installation requirements.
2. Acquire the product using one of the following methods:
 - CA MSM
Note: If you do not have CA MSM, you can download it from the Download Center at CA Support Online. Follow the installation instructions in the *CA Mainframe Software Manager Product Guide*, available on the Documentation page of <https://support.ca.com/>.
 - Pax-Enhanced Electronic Software Delivery (ESD)
 - Tape
3. Install your product based on your acquisition method.
4. Apply maintenance, if applicable.
5. Deploy your product.
6. Start your product.
7. Configure the minimum settings for 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 11)

[Software Requirements](#) (see page 11)

[CA Common Services Requirements](#) (see page 11)

[Security Requirements](#) (see page 13)

[Storage Requirements](#) (see page 13)

[Concurrent Releases](#) (see page 15)

Hardware Requirements

CA PMA Chargeback can be run on both nonprogrammable color and monochrome terminals.

Software Requirements

CA PMA Chargeback runs under z/OS.

Either the current release of DB2 or CA Datacom[®] with SQL must be installed. If your site does not have one of these databases, CA provides a current release of CA Datacom/AD on a separate installation tape.

CA Common Services Requirements

CA PMA Chargeback uses the cBASE component of ViewPoint to provide online facilities. Programs are written in C language. We, therefore, provide the CA Common Services for z/OS CA C Runtime routines necessary to execute these programs. Reporting and sorting are accomplished with two CA Common Services components: the Earl Service and CA SRAM.

Before installing CA PMA Chargeback, the following CA Common Services for z/OS *must* be installed:

- CAIRIM (S910 or higher)
- ViewPoint (CAG3000 or higher)
- CA-C Runtime (F330 or higher)

If you plan to use Earl reporting, the following CA Common Services for z/OS *must also* be installed:

- SRAM Service (SR66 or higher)
- Earl Service (XE61)

CAIRIM

Prepares your operating system environment for all CA applications and starts them. It 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 applications.

Two integral parts of CAIRIM are CAISSF and CA LMP.

CAISSF

Provides an external security mechanism for controlling and monitoring access to all system and application resource processes. CAISSF is integrated into many CA enterprise applications and is also used by other CCS for z/OS services. It provides security services for user logon, resource access control, process use control, and recording and monitoring of violation activity.

CA LMP

Provides a standardized and automated approach to the tracking of licensed software and is provided as an integral part of CAIRIM. After CAIRIM is installed, you have access to Technical Support for all CA LMP-supported products.

ViewPoint

Provides an SQL engine for PC-based workstation products. Workstation products can use ViewPoint to query z/OS product databases without knowledge of the underlying database structure.

CA-C Runtime

Provides a C run-time facility that insulates programs from system and release dependencies.

SRAM Service

Allows the activation of several sort processes concurrently, simplifying the data and logic flow. The incoming data to the sort can be manipulated as desired by the user program in a high-level language without the need for special exit routines.

Earl Service

Provides a user-friendly report-definition facility with the power of a comprehensive programming system. Earl Service allows you to modify and print the contents and layout of a pre-defined CA application report using English-like statements.

Security Requirements

One of the CA security solutions or a compatible non-CA security product is required for database access.

Storage Requirements

TSO Requirements

We recommend that TSO users run the DataManager and CA PMA Chargeback online facility using 4 MB. However, online processing can function using 2 MB.

DASD Requirements

This section shows the device independent allocation requirements, in tracks, for this product's SMP/E target and distribution libraries.

CA PMA Chargeback Permanent (Target) Libraries

Library Name	Blksize	Tracks	Dir Blocks	Description
CAJRCLS0	32720	2,1	2	CLIST Library
CAJRLOAD	6144	39,8	6	Load Library
CAJRPROC	32720	3,1	2	Procedure Library
CAJRJCL	32720	6,2	14	Sample JCL Library
CAJRSAMP	32720	2,1	2	Sample Source Library
CAJROPTN	32720	2,1	2	Sample Option Library
CAJRDTV	32760	11,3	2	IVP Data Library
CAJREARL	32720	4,1	9	EARL Library
CAJRXML	32760	3,1	2	XML Library
CAJRSQL	32720	84,17	26	SQL Library
CAJRCPNC	32760	16,4	74	cBASE PMA Chargeback Panel

Library Name	Blksize	Tracks	Dir Blocks	Description
				Library
CAJRCPNS	32760	30,6	137	cBASE Shared Panel Library
CAJRCLST	32760	6,2	41	cBASE List Library
CAJRCMSG	32760	21,5	212	cBASE Message Library
CAJRCDLG	32760	231,47	66	cBASE Dialog Library
CAJRCSQL	32720	24,5	212	cBASE SQL Library
CAJRCTMP	32720	3,1	3	cBASE Template Library

CA PMA Chargeback Distribution Libraries

AAKRSAMP	32720	2,1	2	Sample Library
AAKRSQL	32720	13,3	8	SQL Library
AAKREARL	32720	4,1	9	Earl Library
AAKRJCL	32720	5,1	11	JCL Library
AAKRCLS0	32720	2,1	2	CLIST Library
AAKRPROC	32720	2,1	2	Procedure Library
AAKROPTN	32720	2,1	2	Sample Option Library
AAKRMOD0	27998	19,4	5	Object Module Library
AAKRCLST	32760	5,1	33	cBASE List Library
AAKRCMSG	32760	18,4	161	cBASE Message Library
AAKRCPNS	32760	30,6	137	cBASE Shared Panel Library
AAKRCDLG	32760	209,42	50	cBASE Dialog Library
AAKRCSQL	32760	20,4	168	cBASE SQL Library
AAKRCTMP	32720	2,1	2	cBASE Template Library
AAKRDATV	32760	11,3	2	IVP Data Library
AAKSSQL	32720	73,15	18	SQL Library
AAKSEARL	32720	3,1	2	Earl Library
AAKSJCL	32720	3,1	3	JCL Library
AAKSPROC	32720	3,1	2	Procedure Library
AAKSOPTN	32720	2,1	2	Sample Option Library
AAKSMOD0	27998	15,3	6	Object Module Library
ABE0CDLG	32760	25,5	17	DataManager cBASE Dialog Library

ABE0CLST	32760	3,1	8	DataManager cBASE List Library
ABE0CLS0	32720	2,1	2	DataManager CLIST Library
ABE0CMMSG	32760	9,2	51	DataManager cBASE Message Library
ABE0CPNC	32760	16,4	74	DataManager cBASE Panel Library
ABE0CSQL	32760	9,2	44	DataManager cBASE SQL Library
ABE0CTMP	32720	2,1	2	DataManager cBASE Template Library
ABE0JCL	32720	3,1	2	DataManager JCL Library
ABE0MOD0	27998	4,1	2	DataManager Object Module Library
ABE0XML	32760	3,1	2	XML Library

CA PMA Chargeback Parameter Files

Library Name	Blksize	Blks	Dir	Description
CAI.CAIKRPAR	80	85	N/A	PMA Chargeback runtime parameters
CAI.CAIKSPAR	80	85	N/A	DataManager runtime parameters

Concurrent Releases

You can install this release of CA PMA Chargeback and continue to use an older release for your production environment. However, due to substantial changes in target and distribution libraries, you must install into a new SMP/E environment.

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 CA Support Online. Follow the installation instructions in the *CA Mainframe Software Manager Product Guide*, available on the Documentation page of <https://support.ca.com/>.

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 17)
- [Getting Started Using CA MSM](#) (see page 18)
- [Acquiring Products](#) (see page 28)
- [Installing Products](#) (see page 34)
- [Maintaining Products](#) (see page 40)
- [Setting System Registry](#) (see page 52)
- [Deploying Products](#) (see page 80)

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 guide includes the required procedures to install your product. If you want to learn more about the full functionality of CA MSM, see the *CA Mainframe Software Manager Product Guide* in the Download Center on <https://support.ca.com/>.

Note: To ensure you have the latest version of these procedures, go to your product's documentation page on Customer Support Online and download the latest version of this guide.

Getting Started Using CA MSM

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

How to Use CA MSM: A Scenario

Your organization recently deployed CA MSM to simplify the installation of CA products and unify their management. The organization has also licensed a new CA 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 and install the new product; The second scenario shows how you can use CA MSM to deploy the product to your target systems; and the third scenario shows how you can use CA MSM to maintain products already installed in your environment.

Acquire and Install a New Product

You want to use CA MSM to acquire and install the new CA product.

1. 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 through the CA Support website.
2. To [access CA MSM](#) (see page 27), 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 CA Support Online credentials. This account enables you to download product packages from CA.
3. 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 28). CA MSM refreshes the catalog through CA Support Online using the site IDs associated with your CA Support Online credentials.
4. After you find your product in the catalog, you can [download the product installation packages](#) (see page 29). CA MSM downloads (acquires) the packages (including any maintenance packages) from the CA FTP site.
5. After you acquire the product installation packages, you can find the packages at the product gen level you want. From there, you can [install your product](#) (see page 34). A wizard guides you through the installation process. A CSI is created for the installed product as part of the installation process. You also can install a product to an existing CSI.

Deploy a Product using the Wizard

CA MSM Deployment Services takes installed software in combination with other software and deploys it to systems in your enterprise. That is, deployments copy data on disk from one place to another. It takes the data (the "what") from here (the "source") and moves it to there ("the target"). The CA MSM Deployment Service is the means (the "way").

You can use the following steps to build you first deployment:

1. Find out what systems you have at your enterprise.
2. Add systems to system registry and validate them.
3. [Create remote credentials](#) (see page 78) for those systems in CA MSM.
4. [Add FTP](#) (see page 75) information along with data destination information to each system registry entry.
5. [Create a methodology](#) (see page 106).
6. Use the [deployment wizard](#) (see page 80) to build a deployment.
7. If you need to deploy other products to the systems defined above using the same methodologies, repeat step 6.

System Registration

Each system in the enterprise that you will be deploying products to will need to be added to the CA MSM system registry and then validated. A deployment can only be sent to a validated system. This procedure is called registering your system.

Note: You will need to perform this procedure for each system in your enterprise. For example, if you have five systems at your enterprise, you will need to perform this procedure five times.

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

1. Remote Credentials

Set up your remote credentials. This is the place 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. 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

The *Non-Sysplex* is 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 which 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

The *Sysplex* (SYStem comPLEX) is the IBM mainframe system complex which 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 procedure was created to help customers that 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.

Shared DASD Clusters

A *Shared DASD Clusters* system is a CA MSM deployment services term. It is a set of systems that shared DASD and it can be composed of Sysplex and/or Non-Sysplex systems. A Staging System cannot be part of a Shared DASD Cluster.

Staging Systems

A *Staging system* is a CA MSM deployment services term. It is 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. FTP Location Information

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.

4. Data Destinations

A data destination must be defined 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 two choices are FTP and Shared DASD. 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.

When shared DASD is specified, 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. The remote system, even though the DASD is shared, 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 volsr, CA MSM adds a "volume=" parameter to the GIMUNZIP instructions on the remote system. The list of zFs volsers is only needed if (1) the software you are deploying contains USS parts, and (2) you select a "container" copy option during the deployment process.

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

5. Registered Systems

You need to register each system by validating that it exists. 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 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 set up your products to be deployed.

Deploying Products using the Wizard

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.

The following tabs need to be completed in the deployment wizard before you can deploy.

1. 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 and it is 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.

2. CSI Selection

Select the CSI selection using the wizard. A CSI is created for the installed product as part of the installation process.

3. Product Selection

Displays the products that are installed in the CSI that was selected from the previous step.

4. 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 110) 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 110) 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 97).

5. 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 add a methodology, you need to specify the following:

- Data set name mask (which lets you choose symbolic variables that get resolved during deployment)
- Disposition of the target data sets:
 - If you select *Create*, the target data sets cannot exist, and if they do, the deployment will fail.
 - 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).

Note: 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: 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.

You can [create a methodology](#) (see page 106).

6. System Selection

Select the system for this deployment.

7. 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.

8. Deploy

Deploy combines the snapshot, transmit, and deploy action into one action. Deploy enables a customer to take their CA MSM installed software and copy it onto systems across their enterprise. For example, customers 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.

9. Confirm

Confirms that the deployment is complete. This is the final action by the user. A deployment is not completed until it is confirmed. After it is confirmed, the deployment moves to the Confirmed deployment list.

10. Summary

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

Maintain Existing Products

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

1. To maintain an existing CSI in CA MSM, you first migrate the CSI to CA MSM. During the migration, CA MSM stores information about the CSI in the database.
2. After the CSI is migrated, you can [download the latest maintenance](#) (see page 41) 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 41).
3. After you download the latest maintenance, you can [apply the maintenance](#) (see page 44).

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

Access CA MSM Using the Web-Based Interface

You access CA MSM using the web-based interface. You must have at least *one* of the following web browsers: Microsoft Internet Explorer 6.0, 7.0, or 8.0, or Mozilla Firefox 3.5.

You need the URL of CA MSM from the CA MSM administrator.

To access CA MSM using the web-based interface

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

The login page appears.

Note: If the Notice and Consent Banner appears, read the information provided, and click the link to confirm it.

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 CA Support Online account.

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

3. Click New.

You are prompted for the CA Support Online credentials to use.

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 in to CA Support Online 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 opens that 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 CA Support Online credentials.

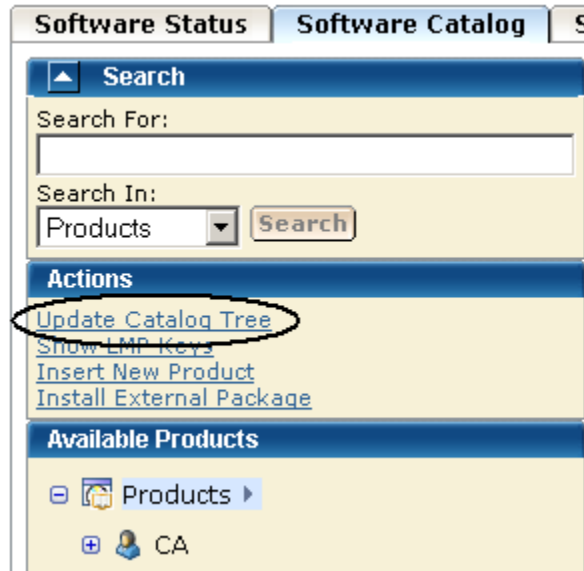
If you update the catalog tree and some changes are missing, check your CA Support Online user settings.

To update your software catalog

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 opens that shows the progress of the task. When the task completes, you can click Show Results on the Progress tab to view the details of the actions. Click Close to return to the previous page.

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 at 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 to which your site is entitled.

To download a product installation package

- Verify that your CA MSM login user name is associated with a registered CA Support Online user for your site on the Software Acquisition Settings page.
CA MSM uses the credentials to access CA Support Online.

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 CA Support Online credentials. If you update the catalog tree and some changes are missing, check your CA Support Online user settings.

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

A dialog opens that shows the progress of the task. When the task completes, you can click Show Results on the Progress tab to view the details of the actions. Click Close to return to the previous page.

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 at the Tasks tab.

The product packages are downloaded.

Note: You can expand the tree in the right panel by selecting a product and clicking the vendor link in the right panel, but if you use this method and select multiple products, be aware that if one of the selected products cannot be downloaded, the remaining products will not be processed. If this happens, remove the checks from the ones 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 enables you to have a complete view of all your product releases. After a package is migrated, you can use CA MSM to [install the product](#) (see page 34).

To migrate information about a product installation package downloaded by other means

1. Click the Software Catalog tab, and select the product gen level (for example, SP0 or 0110) for which the package applies.

The packages for the gen level are listed.

Note: A product not acquired from CA Support Online does not appear in Software Catalog. However, you can use the Insert New Product link to add an entry for the product. You can then select the entry.

2. Click the Add External Package button.
You are prompted to enter a path for the package.
3. 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.

Download Multiple Product Installation Packages

You can download multiple product packages at one time using the Software Catalog tab. The Update Catalog action retrieves information about the products to which your site is entitled.

To download multiple product installation packages

1. Verify that your CA MSM login user name is associated with a registered CA Support Online user for your site on the Software Acquisition Settings page.
CA MSM uses the credentials to access CA Support Online.
2. Click the CA link to expand the tree.

All mainframe CA products that your site is licensed to download appear in the right panel.

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 CA Support Online credentials. If you update the catalog tree and some changes are missing, check your CA Support Online user settings.

3. Click the check boxes in the Select column to select the products you want to download. You can navigate to subsequent pages to select additional products.
4. Click Update Catalog Products.

A dialog opens that shows the progress of the task. When the task completes, you can click Show Results on the Progress tab to view the details of the actions. Click Close to return to the previous page.

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 at the Tasks tab.

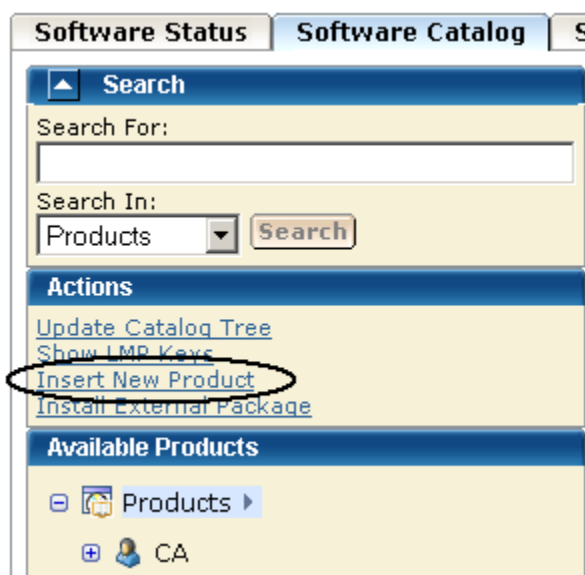
The product packages are downloaded.

Add a Product

Sometimes, a product is not currently available from CA Support Online. 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.

To add a product package to CA MSM

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: If you need to add several packages from the same location, you can use [masking](#) (see page 33).

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 to add more than one package (or set of maintenance files) from the same location based on 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 qualifier of a data set name or any number of characters within a member name or file system name.

**

Match on any number of characters including any number of .qualifier 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. Make sure you review the list and check what files need to be added.

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*)
```

Delete a Product

You can delete a product, product release, or product gen level from CA MSM if you do not need them anymore. You delete them using the Software Catalog tab.

To delete a product, product release, or product gen level

1. Click the Software Catalog tab, and find the product, product release or the product gen level that you want to delete from the tree at the left.
2. Right-click the product, product release or the product gen level and select the applicable action.

You are prompted to confirm the action.

3. Click OK.

A dialog opens showing the progress of the task. When the task completes, you can click Show Results on the Progress tab to view the details of the actions. Click Close to return to the previous page.

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 at the Tasks tab.

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, zFS or HFS only), 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 CSI, the CSI is locked and other CA MSM users cannot perform any action against it. The lock is released when the task is finished, you log out of CA MSM, or your CA MSM session has been inactive for more than ten minutes.

To install a product

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:

Select	Name	Last Modified Date	Type	Download Status	Size	Release/Gen Level	Actions
<input type="checkbox"/>	CA COMMON SERVICES COVER LTR	Nov 20, 2007	PDF	Yes	46 Kb	14.5/SP1	Actions
<input type="checkbox"/>	CA COMMON SERVICES PROD PKG	Nov 11, 2008	Base Install	Yes	407 Mb	14.5/SP1	Actions
<input type="checkbox"/>	CA MSM COVER LETTER	Dec 1, 2009	PDF	Yes	149 Kb	14.5/SP1	Actions
<input type="checkbox"/>	CA MSM COVER LETTER	Mar 18, 2010	PDF	Yes	136 Kb	14.5/SP1	Actions

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 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 is displayed, 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 use the 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 38).

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 with extra parameters.
- If you select a CSI that is being used in CA MSM by another user, a notification message appears, and you are prevented from performing any actions on the CSI. You can either wait until the notification message disappears and the CSI is available, or click Cancel to select another CSI.

After a CSI is selected or a new CSI is specified, 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 a target zone is selected or specified, 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 opens that shows the progress of the task. When the task completes, you can click Show Results on the Progress tab to view the details of the actions. Click Close to return to the previous page.

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 at the Tasks tab.

Create a CSI

You can create a CSI while you are [installing a product](#) (see page 34). During the process, you are asked to specify data set allocation parameters, which you can then customize for each data set, as well as parameters for DDDEF allocation.

To create a CSI

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

You are prompted to define a CSI.

2. Specify a name for the environment represented by the CSI, and the following VSAM and data set allocation parameters. You can leave the other parameters at their defaults.

- Specify the prefix for the name of the CSI VSAM data set.
- Specify the prefix for the names of the SMP/E data sets.
- Select whether to use SMS, and complete the appropriate fields.

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. Click Next.

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

- 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.

- Review the data set names. Click the Override link to change allocation parameters, and then click Next.

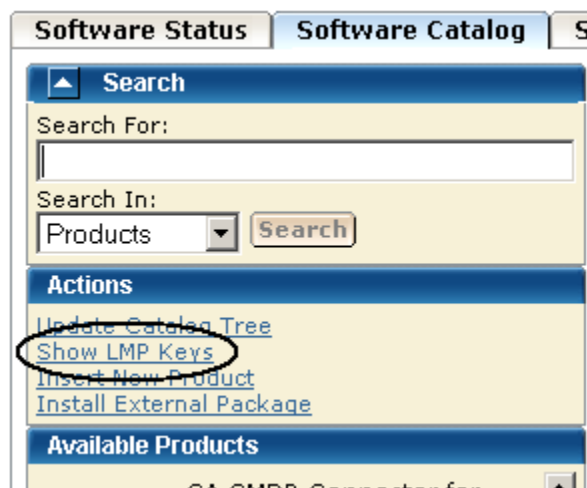
You are prompted to specify any additional parameters. A new CSI is specified.

Download LMP Keys

When you install a CA product on z/OS systems, you enter CA Common Services for z/OS CA License Management Program (LMP) statements to license the product on each system that uses the product. 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.

To retrieve and list the LMP keys for your products

- 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.

- 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 three download methods:
 - Download Product Maintenance Packages
 - Download Product Maintenance Packages for Old Product Releases and Service Packs
 - Manage Maintenance Downloaded External to CA MSM

Contact your system administrator, if necessary.

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

Note: This section also details the procedure 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.

To download product maintenance packages

1. Verify that your CA MSM login user name is associated with a registered CA Support Online user for your site on the Software Acquisition Settings page.

CA MSM uses the credentials to access CA Support Online.

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 opens that shows the progress of the task. When the task completes, you can click Show Results on the Progress tab to view the details of the actions. Click Close to return to the previous page.

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 at the Tasks tab.

The maintenance packages are downloaded.

More information:

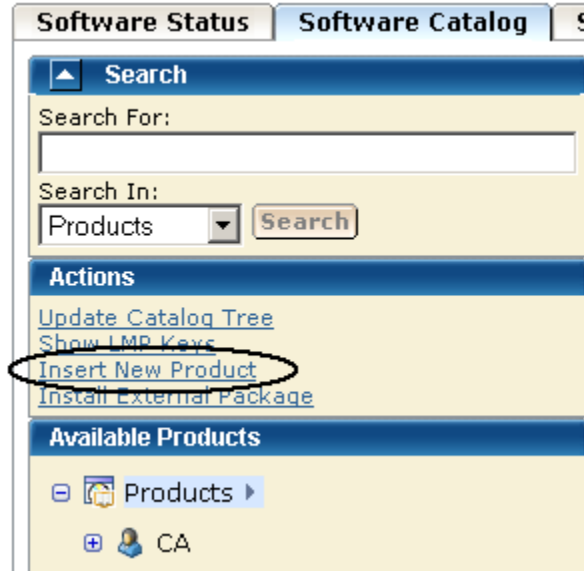
[Download Maintenance Packages for Old Product Releases and Service Packs](#)
(see page 41)

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.

To download maintenance packages for a product release not in the software catalog

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 at CA Support Online.

The product release is added to the software catalog.

3. On 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 opens that shows the progress of the task. When the task completes, you can click Show Results on the Progress tab to view the details of the actions. Click Close to return to the previous page.

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 at 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 44).

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 comprised of 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.

To add a maintenance package acquired externally

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: If you need to add several packages from the same location, you can use [masking](#) (see page 33).

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.

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.

To view aggregated package details

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 CSI, the CSI is locked and other CA MSM users cannot perform any action against it. The lock is released when the task is finished, you log out of CA MSM, or your CA MSM session has been inactive for more than ten minutes.

The following installation modes are available:

- Receive and apply
- Receive and apply check
- Receive, apply check, and apply
- Receive only

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.

To manage maintenance for a product

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.

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

The maintenance packages are listed, for example:

Fix #	Description	Confirmed Date	Type	Installed	Actions
Q185660	* PRODUCT DOCUMENTATION CHANGE	Jan 29, 2007	PEA/PDC	Not installable	Actions
Q089243	* PRODUCT ERROR ALERT *	Jun 20, 2007	PEA/PDC	Not installable	Actions
R012055	0607: MSM INST. ADD SUPPORT FOR SAMPJCL UNDER SMP/E	Oct 7, 2009	PTF	No (0/1)	Actions
Q088256	14.5-SP00 : PANO/PAN#1 INPUT STREAM INVALID COMMAND	May 11, 2007	PTF	No (0/1)	Actions
Q088259	14.5-SP01 : PANO/PAN#1 INPUT STREAM INVALID COMMAND	May 11, 2007	PTF	No (0/1)	Actions
Q086490	14.5-SP00 : DOING ++WRITE, LNG FMT CHANGED AFTER	Mar 6, 2007	PTF	No (0/1)	Actions
Q090975	14.5-SP00/SP01: PAM DIRECTORY AVERAGE BYTES	Sep 4, 2007	PTF	No (0/1)	Actions
Q081764	14.5-SP00: PAN#1 ++CONTROL WITH NO CODE GIVES ERROR	Aug 25, 2006	PTF	No (0/1)	Actions
Q081765	14.5-SP00: PV071 DOING ++SCANS OF ZTYPE1-8 MEMBERS	Aug 25, 2006	PTF	No (0/1)	Actions
Q086868	14.5-SP00: ZTYPE7 NOT FORMATTED CORRECTLY ON TSO	Mar 19, 2007	PTF	No (0/1)	Actions

Red asterisks identify HIPER maintenance packages.

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

The Maintenance Package Details dialog appears, identifying any prerequisites.

Click Close to return to the Maintenance Packages section after you review the information for a package.

5. 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.

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

The packages to install are listed.

7. 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.

8. Select the environments in which you want to install the packages.

9. 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 a CSI that is being used in CA MSM by another user, a notification message appears, and you are prevented from performing any actions on the CSI. You can either wait until the notification message disappears and the CSI is available, or click Cancel to select another CSI.

10. 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 147) entries exist, review and select them, and click Next.

A summary of the task appears.

11. Review the summary, and click Install.

A dialog opens that shows the progress of the task. When the task completes, you can click Show Results on the Progress tab to view the details of the actions. Click Close to return to the previous page.

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 at 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 41)

[Download Maintenance Packages for Old Product Releases and Service Packs](#) (see page 41)

View Installation Status of Maintenance Package

You can view installation status details of each maintenance package, including a list of CSIs where the package is installed, the CSI data sets, and the installation status of the package for each CSI zone. For example, a maintenance package can be received in the global zone, applied in a target zone, and accepted in a distribution zone.

Note: The installation status is not available for aggregated maintenance packages as well as for those maintenance packages that are not installable or do not have available CSIs to be installed to.

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 a CSI zone, the Install action is available.

To view installation status of a maintenance package

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 CSIs with package status per zone appears.

Note: Click the Actions drop-down to start the Installation wizard (for packages that are not yet installed in at least one CSI zone) or the Accept wizard (for packages that are not accepted in at least one CSI zone). Click Install to More Environments to install the maintenance package in one or more CSIs available for the package.

USERMODs

A product USERMOD can be provided as a published maintenance package downloaded by CA MSM during the Update Catalog process. When CA MSM downloads a package that includes a ++USERMOD statement, it is loaded under the CA 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 CA 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 43).

GROUPEXTEND Mode

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

Some maintenance packages require that, before you install them, you must install other maintenance packages (SYSMODs) first.

If a SYSMOD that is defined as a prerequisite for the product maintenance package that you want to install has not been applied or cannot be processed (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), you can install the maintenance package in GROUPEXTEND mode, and the SMP/E environment where the product is installed automatically includes a superseding SYSMOD.

Note: For applying maintenance in GROUPEXTEND mode, the SMP/E environment *must* have all SYSMODs received to be included by the GROUPEXTEND option.

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

- Apply check
- Apply
- Apply check and apply

For the GROUPEXTEND option, CA MSM does not automatically receive and display prerequisites for maintenance or HOLDDATA that needs to 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.

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 SMPDOUT in the task output to check if there are missing (not received) SYSMODs or HOLDDATA that need to be resolved or bypassed.
 - If the task succeeds, review SMPRPT in the task output to check what SYSMODs were found and applied.

- 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 needs to correspond to the version of SMP/E that you use.

When you 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 prepopulated on the wizard dialogs.

Manage Maintenance in GROUPEXTEND Mode

Note: While you are working with a particular CSI, the CSI is locked and other CA MSM users cannot perform any action against it. The lock is released when the task is finished, you log out of CA MSM, or your CA MSM session has been inactive for more than ten minutes.

To manage maintenance for a product in GROUPEXTEND mode

- Click the SMP/E Environments tab, and select the SMP/E environment from the tree at the left.

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

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

- Click the Maintenance link.

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

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

The Introduction tab of the wizard appears.

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

The packages to be applied are listed.

Note: If the Link status for a maintenance package is available, you can click it to review a list of zones 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 prerequisites for maintenance or HOLDDATA to 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. We recommend that you run the maintenance in Apply check mode first.

6. Read the information 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 those 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 should be excluded in the Excluded SYSMODs field. You can enter several SYSMODs separated 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 separated by a comma.

9. Click Next.

A summary of the task appears.

10. Review the summary, and click Apply GROUPEXTEND.

A dialog opens that shows the progress of the task. When the task completes, you can click Show Results on the Progress tab to view the details of the actions. Click Close to return to the previous page.

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 at the Tasks tab.

- If you run the maintenance installation in Apply check mode and the task succeeds, review SMPRPT in the task output to check 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 to check if there are missing (not received) SYSMODs or HOLDDATA that need to be resolved or bypassed.

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

Note: Although you cannot accept USERMODs in GROUPEXTEND mode, you can install them if they are prerequisites for the maintenance package being installed, unless you have enabled the NOUSERMODS option.

Back Out Maintenance

You can back out applied (but not accepted) maintenance packages 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 CSI, the CSI is locked and other CA MSM users cannot perform any action against it. The lock is released when the task is finished, you log out of CA MSM, or your CA MSM session has been inactive for more than ten minutes.

To back out a maintenance package from a product release

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

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: If you want to back out maintenance from all the products in the environment, you can 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 you want to back out, and click the Restore link.

The Introduction tab of the wizard appears.

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

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: Click Select Zones to review and adjust a list of zones from where the maintenance will be restored, and 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.

8. Review the summary, and click Restore.

A dialog opens that shows the progress of the task. When the task completes, you can click Show Results on the Progress tab to view the details of the actions. Click Close to return to the previous page.

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 at 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 all systems that can be selected as a target for a deployment.

About System Registry

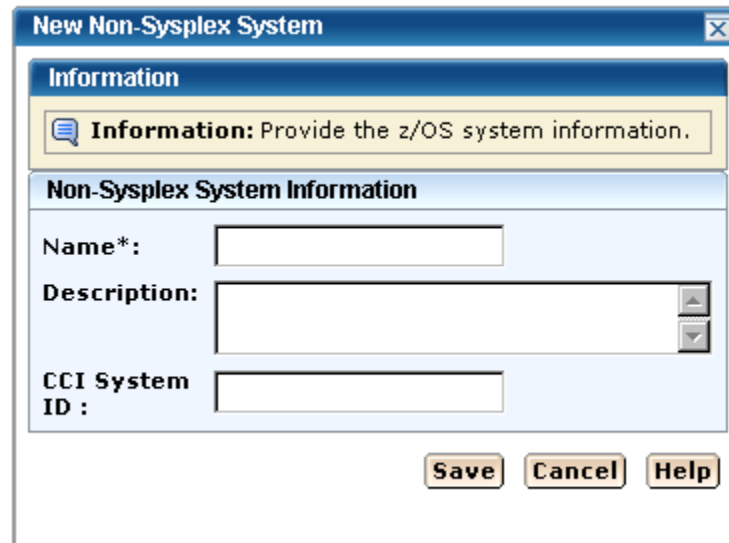
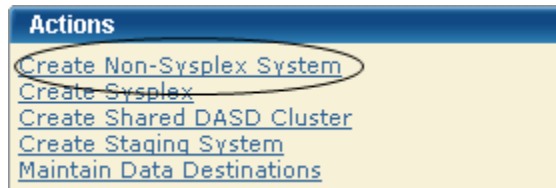
The system registry contains all systems that can be selected as a target for a deployment. You can create Non-SYSPLEX, SYSPLEX, Shared DASD Cluster, and Staging systems as well as maintain, validate, investigate a failed validation, view, and delete a system register.

Create Non-Sysplex System

You can create a Non-Sysplex System Registry.

To create a Non-Sysplex system registry

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

A screenshot of the 'New Non-Sysplex System' dialog box. It has a title bar with a close button. Below the title bar is an 'Information' section with a message icon and the text 'Information: Provide the z/OS system information.' Below that is a section titled 'Non-Sysplex System Information' containing three input fields: 'Name*' (with an asterisk indicating it is mandatory), 'Description' (with a scroll bar), and 'CCI System ID'. At the bottom right are three buttons: 'Save', 'Cancel', and 'Help'.

Note: The asterisk indicates that the field is mandatory.

2. Enter the Non-Sysplex System Name.

Limits: Maximum 8 characters.

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

3. Enter the Description.

Limits: Maximum 255 characters.

4. Enter the CCI System ID:

Limits: Maximum 8 characters.

5. Click Save to save this new Non-Sysplex System.

The New Non-Sysplex System name appears as the last entry in the Non-Sysplex Systems Registry List on the right.

Note: Click Cancel to withdraw this create request.

Note: An MVS System running under VM, it is treated as being in basic mode and not LPAR mode. As result, the LPAR number is null in the MVS control block. When this is the case, the system validation output will show:

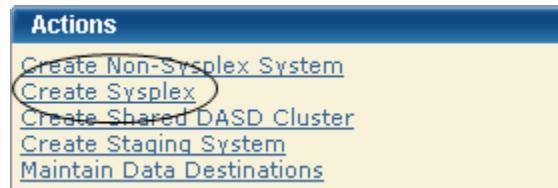
Property Name: z/OS LPAR Name, Value: ** Not Applicable **.

Create Sysplex or Monoplex

You can create a [Sysplex](#) (see page 55) or Monoplex system registry.

To create a Sysplex or Monoplex system registry

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



The Sysplex System window appears.

 A screenshot of a dialog box titled 'New Sysplex'. It has a close button in the top right corner. Below the title bar is an 'Information' section with a speech bubble icon and the text 'Information: Provide the Sysplex information.' Below that is a 'Sysplex Information' section with two input fields: 'Name*' (with an asterisk indicating it is mandatory) and 'Description'. At the bottom of the dialog are three buttons: 'Save', 'Cancel', and 'Help'.

Note: The asterisk indicates that the field is mandatory.

2. Enter the Sysplex System Name.

Limits: Maximum 8 characters.

Note: Sysplex and Non-Sysplex system can have the same name. Use the Description field to differentiate these systems.

Note: Monoplexes are stored in the Sysplex registry tree but with the name of the Sysplex 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 procedure was created to help customers that 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.

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.

3. Enter the Description.

Limits: Maximum 255 characters.

4. Click Save to save this new Sysplex System.

The New Sysplex System name appears as the last entry in the Sysplex Systems Registry List on the right.

Note: Click Cancel to withdraw this create request.

Note: An MVS System running under VM, it is treated as being in basic mode and not LPAR mode. As result, the LPAR number is null in the MVS control block. When this is the case, the system validation output will show:

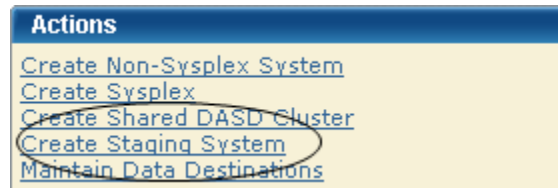
Property Name: z/OS LPAR Name, Value: ** Not Applicable **.

Create Staging System

You can create a Staging System.

To create a Staging System

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



The New Staging System window appears.

 A screenshot of a dialog box titled 'New Staging System'. It has a close button (X) in the top right corner. Below the title bar is an 'Information' section with a speech bubble icon and the text 'Information: Provide the z/OS system information.' Below that is a section titled 'Staging System Information' containing two input fields: 'Name*' (with an asterisk indicating it is mandatory) and 'Description'. At the bottom of the dialog are three buttons: 'Save', 'Cancel', and 'Help'.

Note: The asterisk indicates that the field is mandatory.

2. Enter the Staging System Name.

Limits: Maximum 8 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 may have the same name as a Non-Sysplex, Sysplex, or Shared DASD Cluster.

3. Enter the Description.

Limits: Maximum 255 characters.

4. Click Save to save this new Staging System.

The New Staging System name appears as the last entry in the Staging Systems Registry on the right.

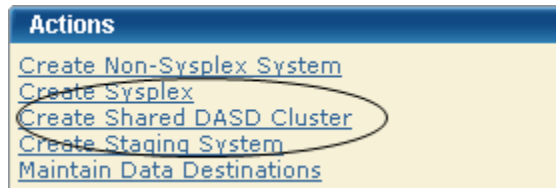
Note: Click Cancel to withdraw this create request.

Create Shared DASD Cluster

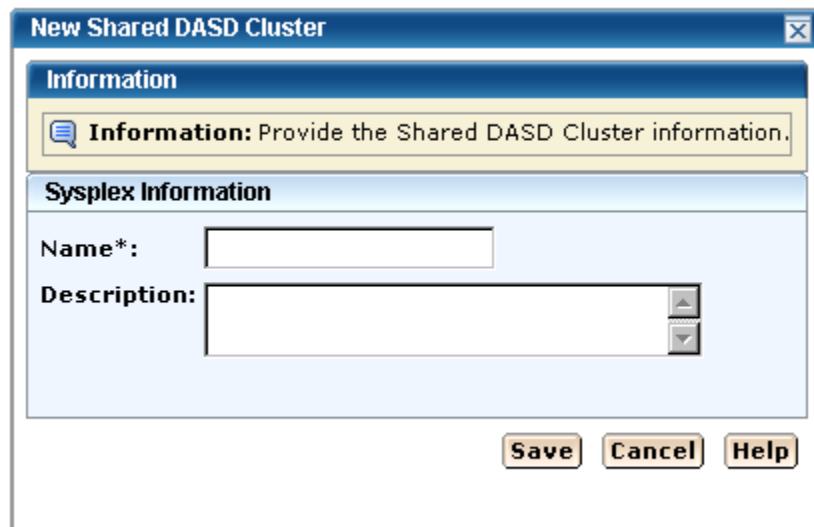
You can create a Shared DASD Cluster.

To create a Shared DASD Cluster

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



The New Shared DASD Cluster window appears.



Note: The asterisk indicates that the field is mandatory.

2. Enter the Shared DASD Cluster Name.

Limits: Maximum 8 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 Staging System may have the same name as a Non-Sysplex, Sysplex, or Shared DASD Cluster.

3. Enter the Description.

Limits: Maximum 255 characters.

4. Click Save to save this new Shared DASD Cluster.

The New Shared DASD Cluster name appears as the last entry in the Systems Registry Cluster List on the right.

Note: Click Cancel to withdraw this create request.

Authorization

There are two authorization modes for the Systems Registry.

- Edit Mode - Allows you to update and change System Registry information.

Note: Once the information is changed you must click save to save the information or cancel to cancel the changed information.

- View Mode - only allows you to see the screen.

Maintain a System Registry

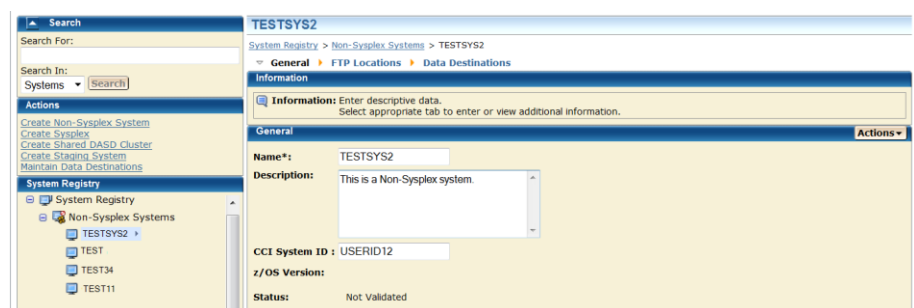
You can maintain the system registry.

To maintain a system registry

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

The detailed information appears at the right.

2. Select the system to maintain.



3. Update the Name as needed.

Limits: Maximum 8 characters.

4. Update the Comments as needed.

Limits: Maximum 255 characters.

- Update the CCI System ID:

Note: CA recommends that the CCI System ID is not updated.

Limits: Maximum 8 characters.

- For Shared DASD or SYSPLEX system only, select the Contact System. This is system where the Shared DASD location or FTP location. The FTP location should be set to the contact system URI. The contact system is used for remote credentials.

For example, assume 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 you set the Contact System to CO11, but you are contacting to XX61 and it will fail because spawn will be started on CO11 but we will look for the output on XX61 because that is where the FTP location was set.

The screenshot shows the 'Data Destinations' configuration window in the CA MSM System Registry. The breadcrumb path is 'General > FTP Locations > Data Destinations'. The window title is 'Information'. Below the title bar, there is an 'Information' message: 'Enter descriptive data. Select appropriate tab to enter or view additional information.' The main area is titled 'General' and contains the following fields:

- Name*:** PLEXC1
- Description:** Test enviornment SYSPLEX
- Contact System:** CO11 (selected from a dropdown menu)
- z/OS Version:** 01.11.00
- Status:** Validated
- Sysplex name:** PLEXC1

Note: z/OS Version is set by CA MSM.

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 procedure was created to help customers that 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.

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.

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.

[System Registry](#) > [Staging Systems](#) > Stage1

▼ **General**

Information

i **Information:** Enter descriptive data.

General Actions ▼

Name*:

Description:

GIMUNZIP Volume:

zFS Candidate Volumes:

- Select the Action from the Actions 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 steps will show how the validation failed. See [How to Investigate a Failed Validation](#) (see page 62).

Validation Rules

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

Note: A Staging system is not validated.

Note: When a system is validated status appears in the Status Field.

This table shows the system validation results and actions.

Result	Action
Validated	System is available, status is updated as valid, and system registry is updated with results from validation.
Validation in Progress	System status is updated to in progress.
Validation Error	System status is updated to error. See How to Investigate a Failed Validation (see page 62).
Not Validated	This system has not been validated yet.
Not Accessible	The system has not been validated because it is no longer available or was not found in the CCI Network.
Validation Conflict	System has been contacted but the information entered then different then the information retrieved.

Error details

When a validation is in error the Error details button appears. Click this button to find the reason for this conflict. See [How to Investigate a Failed Validation](#) (see page 62).

Note: The error reason is kept in local memory. If the "Please validate the system again." message 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. See [How to Investigate a Failed Validation](#) (see page 62).

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.

How to Investigate a Failed Validation

When a validation fails it can be investigated, corrected, and validated again. The following procedures are defined:

- Investigate a validation using the Tasks Page.
- Investigate a validation immediately after a Validation
- Save a message log

Note: This procedure uses a Non-Sysplex system for an example, but the method also works for a Sysplex or a Shared DASD Cluster.

To investigate a failed validation using the Tasks Page

1. On the System Registry Page, in the left hand column find the system with a validation status error.

Note: It is helpful to record the System Name that has failed the validation.

2. Click the Tasks Tab and then click the Task History link.
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.

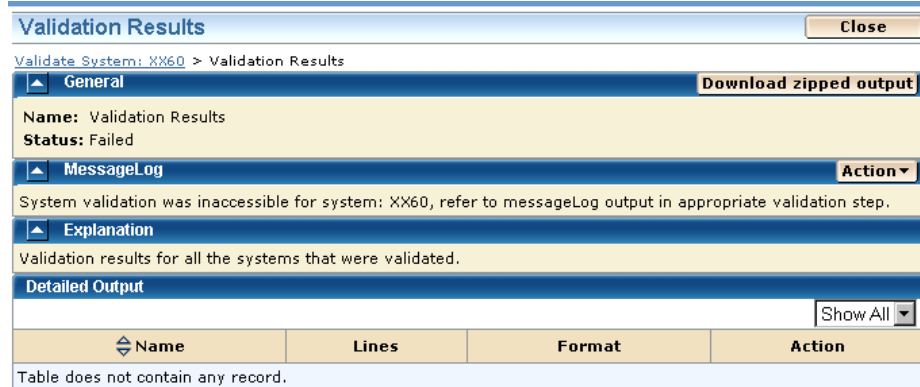
4. Find the Failed validation and click the Name Link.

Task History							Refresh
Current date and time is 1/12/2010 03:41:56PM							
Show:	USER456	All types	All status	<input type="checkbox"/> Start time	<input type="checkbox"/> Stop time	Show All	
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	

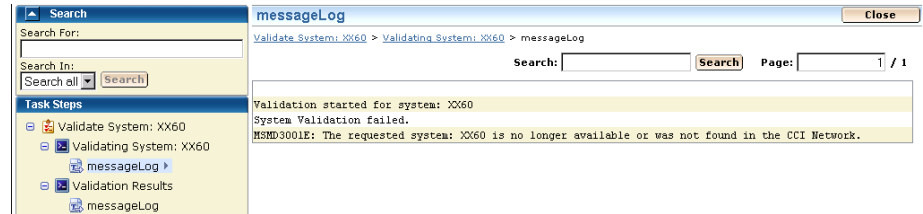
5. The Validate System window appears.

Search		Validate System: XX60		Close
Search For:		General		Download zipped output
Search In:		Name:	Validate System: XX60	
Search all	Search	Task ID:	447	
Task Steps		User ID:	USER456	
<ul style="list-style-type: none"> Validate System: XX60 <ul style="list-style-type: none"> Validating System: XX60 <ul style="list-style-type: none"> messageLog Validation Results <ul style="list-style-type: none"> messageLog 		Status:	Failed	
		Status message:	Failed to undo command	
		Steps		
#	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	

- Click the Validation Results link to view the results and click on the messages logs to review the details for each error. To analyze the error results, see Troubleshooting. Correct the issue and validate again.



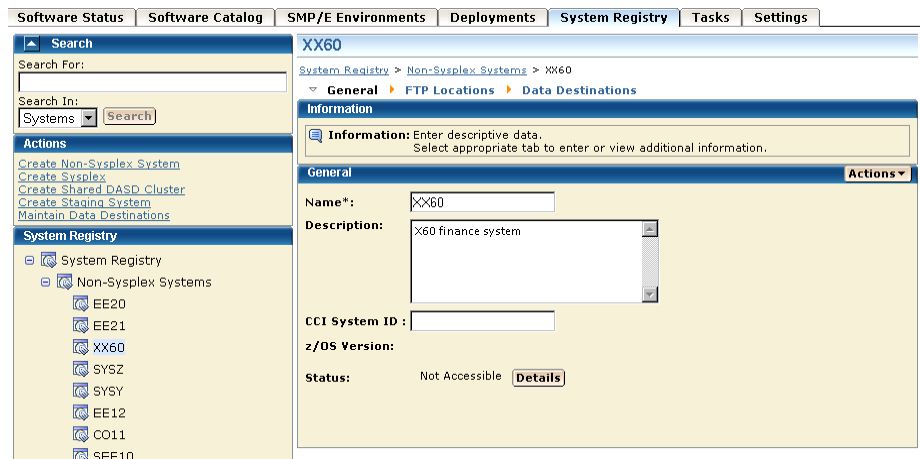
The Message Log.



To investigate a failed validation immediately after Validation

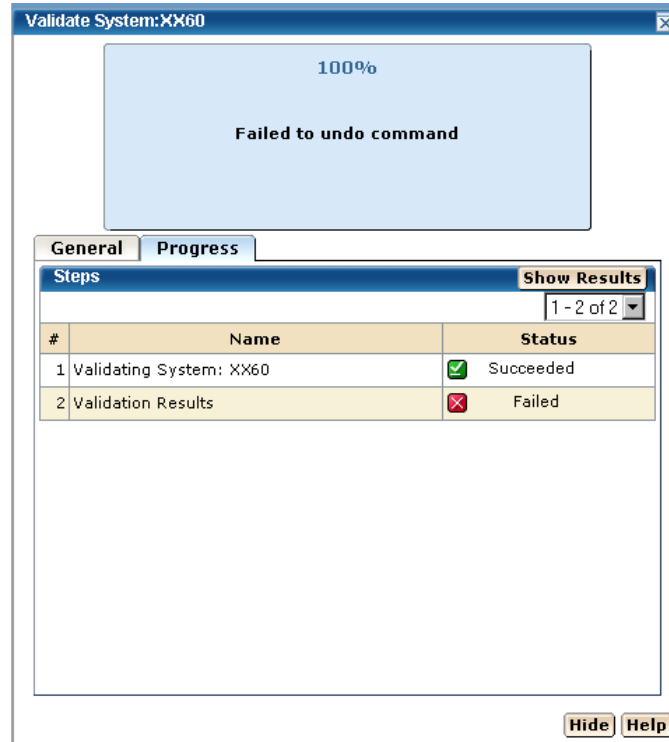
- On the System Registry Page, in the left hand column find the system with a validation status error.

Note: It is helpful to record the System Name that has failed the validation.



- Click the Detail Button to see the Error details.
- If the Message states "Please validate the system again", click the Validate button. The system validates again.

- Click the Progress tab.



- Go to step 5 in the "To investigate a failed validation using the Tasks Page".

Download Message Log

To download a zipped file of all the text messages for this validation

- Click the Deployment Name on the top left tree and click Download zipped out button on the General menu bar. You will be requested to 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 MessageLog bar and click the Download as TXT. You will be requested to 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 MessageLog bar and click the Download as ZIP. You will be requested to save this file.

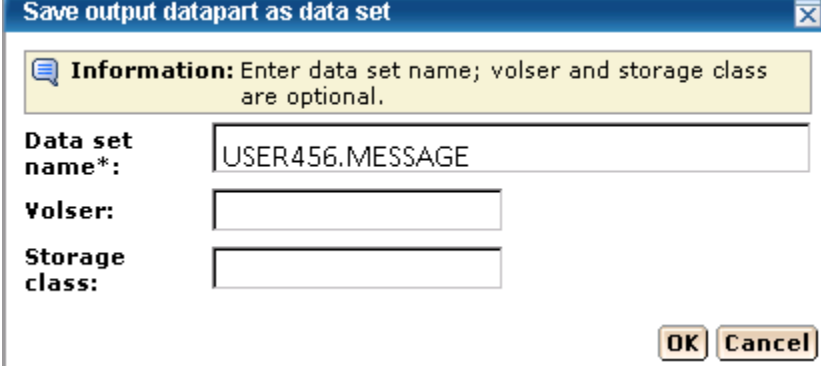
Save a Message Log as a Data Set

To save as a data set

1. Click the Deployment Name or the Deployment Results on the left tree, click the Action button on the MessageLog bar, and click the Save as data set.

The Save output as a data set window appears.

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



Save output datapart as data set

Information: Enter data set name; volser and storage class are optional.

Data set name*: USER456.MESSAGE

Volser:

Storage class:

OK **Cancel**

Note: The asterisk indicates that the field is mandatory.

2. The data set name has been entered by the system.
For Non-SMS data, enter the Volser.

Example:

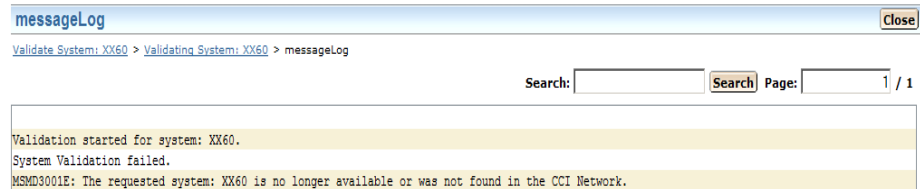
Volsers: SYSP01 and SYSP02

3. For SMS Allocation data, enter the Storage Class.

To Show All

To Show all

1. Click the Show all button and the complete message log appears for this failed validation.



2. Click Close.

To Download as TXT

Save the file.

To Download as ZIP

Save the file.

Delete a System Registry

You can delete a system registry.

To delete a system registry

1. Click the System Registry tab.

The System Registry window appears.
2. On the right, in the System Registry panel, select Non-Sysplex Systems, Sysplexes, Clusters, or Staging Systems link.

The system list appears.
3. Click the Select box for each system registry you want to delete.
4. Click the Delete link and then click OK to the Delete confirmation window.

The system is deleted.

Data Destinations

The Data Destinations page lists the current data destinations for this system.

Create Data Destinations

You can create data destinations.

To create a data destination

1. Click the System Registry tab, and in the Actions section click the Maintain Data destinations link. The Maintains Data Destinations window appears.
2. Click Create. The New Data Destination Window appears.

New Data Destination

Information

Information: Name this data destination then choose transmission method and remote allocation data.

General

Name*:

Description:

Transmission Method: Shared DASD FTP

Mount Point*:

Storage Class:

VOLSER:

Remote Allocation Data

GIMUNZIP Volume:

zFS Candidate Volumes:

Save **Cancel** **Help**

Note: The asterisk indicates that the field is mandatory.

3. 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.

4. Enter the Description.

Limits: Maximum 255 characters.

5. Select the transmission method either Shared DASD (step 6) or FTP (step 11).

Default: Shared DASD.

6. For Shared DASD, enter the Mount point directory path

Mount point 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.

The deployment user must have write permissions for the mount directory. The deployment user ID must have 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.

7. Enter the Storage Class,

Limits: Maximum 8 characters

Example:

Storage Class: SYSPRG

8. Enter the Volser.

Limits: Maximum 6 characters

Example:

Volsers: SYSP01 and SYSP02

9. Enter the GIMUNZIP volume.
Limits: Maximum 6 characters
10. Enter zFS Candidate volumes.
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.

11. Click Save. The new data destination appears as the last entry on the Pick data destination list.
Note: Click Cancel to withdraw this create request.
12. For FTP, select FTP button.

Note: The FTP indicator tells CA MSM that the transmission will be through FTP.

The screenshot shows a dialog box titled "Remote Allocation Data". At the top, it has "Transmission Method:" with two radio buttons: "Shared DASD" (unselected) and "FTP" (selected). Below this is an "Information" section with the text: "Please ensure an FTP location is defined for the system." The main area contains two input fields: "GIMUNZIP Volume:" followed by a single text box, and "zFS Candidate Volumes:" followed by four separate text boxes. At the bottom right, there are three buttons: "Save", "Cancel", and "Help".

13. Enter the GIMUNZIP Volume.
Limits: Maximum 6 characters
14. Enter the zFS Candidate Volumes.
Limits: Maximum 6 characters
15. Click Save. The new data destination appears as the last entry on the Pick data destination list.
Note: Click Cancel to withdraw this create request.

Add a Data Destination

You can add a current data destinations to an existing system.

To add a current data destination to an existing system

1. Click the System Registry tab, and select Non-Sysplex Systems, Sysplexes, or Clusters, from the tree at the left.
The detailed information appears at the right.
2. Select the system you want to add data destinations.

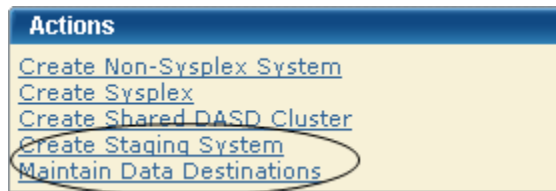
3. Click the Data Destination tab.
The Data Destination window appears.
4. Click Add.
The Pick data destination window appears.
5. Select the data destinations you want to add and click Select.

Maintain Data Destinations

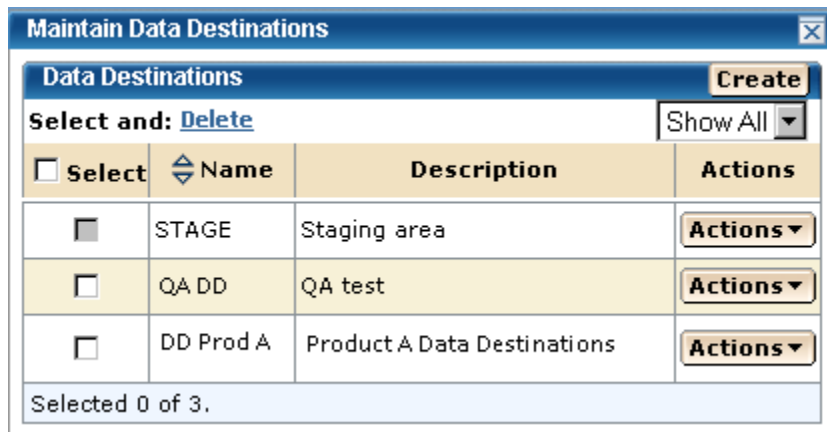
You can maintain, [delete](#) (see page 74), or [create](#) (see page 68) data destinations.

To maintain current data destinations

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



The Maintains Data Destinations window appears.



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

2. Select the data destinations and select Edit on the Actions drop down. The Edit Data Destinations window appears.

Note: The asterisk indicates that the field is mandatory.

Important! The only valid fields in the Data Destination windows are name, comments, Volsers, and the data destination is shared check box.

3. 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.

4. Enter the Description.

Limits: Maximum 255 characters.

5. Select the transmission method either Shared DASD (step 6) or FTP (step 11).

Default: Shared DASD.

6. For Shared DASD, enter the Mount point directory path

Mount point 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.

The deployment user must have write permissions for the mount directory. The deployment user ID must have 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.

7. Enter the Storage Class, and the Volsers.

Example:

Storage Class: SYSPRG

Volsers: SYSP01 and SYSP02

8. Enter the GIMUNZIP volume.
9. Enter zFS Candidate volumes.

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.

10. Click Save.

The new data destination appears as the last entry on the Pick data destination list.

Note: Click Cancel to withdraw this create request.

11. For FTP, select FTP button.

Note: The FTP indicator tells CA MSM that the transmission will be through FTP.

Transmission Method: <input type="radio"/> Shared DASD <input checked="" type="radio"/> FTP	
Information	Please ensure an FTP location is defined for the system.
Remote Allocation Data	
GIMUNZIP Volume:	<input type="text"/>
zFS Candidate Volumes:	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>	

12. Enter the GIMUNZIP Volume.

13. Enter the zFS Candidate Volumes.

14. Click Save.

The new data destination appears as the last entry on the Pick data destination list.

Note: Click Cancel to withdraw this create request.

Set a Default Data Destination

You can set a default for a current data destination.

To set a default for a current data destination

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

The detailed information appears at the right.

2. Click the data destination link.

The data destination window appears.

3. Select the data destination to you want as a default.

4. In the Action box 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 select box indicates that the data destination is assigned and it cannot be deleted. It can be edited.

To delete a data destinations

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

The detailed information appears at the right.

2. Select the system where you want to delete a data destination.

3. Click the Data Destination tab.

The Data Destination window appears.

4. Click the Select box for each data destination you want to remove.

5. Click the Delete link and then click OK to the Delete confirmation window.

The data destination is deleted.

FTP Locations

The FTP Locations lists the current FTP locations for this system.

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.

Add FTP Locations

You can add, [edit](#) (see page 76), [set default](#) (see page 76), or [remove](#) (see page 77) FTP locations.

Note: The asterisk indicates that the field is mandatory.

To add FTP locations

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

The detailed information appears at the right.

2. Click the system name link you want to create FTP locations.
3. Click the FTP Locations tab.

The FTP Locations window appears.

4. Click Add.

The New FTP Location window appears.

5. Enter URI.

Limits: Maximum length is 255.

6. Enter Port.

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

Default: 21

7. Enter Directory Path

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

8. Click Save.

More information:

[Edit FTP Locations](#) (see page 76)

[Set FTP Location Default](#) (see page 76)

[Remove FTP Locations](#) (see page 77)

Edit FTP Locations

You can edit FTP locations.

Note: The asterisk indicates that the field is mandatory.

To edit FTP locations

1. Click the System Registry tab, and select Non-Sysplex Systems, Sysplexes, Shared DASD Clusters, or Staging Systems from the tree at the left.
2. The detailed information appears at the right.
3. Click the system link where you want to create FTP locations.
4. Click the FTP Location tab. The FTP Locations window appears.
5. Select the FTP location and select Edit on the Actions drop down. The Edit FTP Location window appears.

6. Edit the URI.

Limits: Maximum length is 255.

7. Edit the Port.

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

Default: 21

8. Edit the Directory Path

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

9. Click Save.

Set FTP Location Default

You can set an FTP location default.

To set an FTP location default

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

The detailed information appears at the right.

2. Click the system link you want to set the FTP location default to.

3. Click the FTP Locations tab.
The FTP Locations window appears.
4. Select the FTP locations and select Default on the Actions drop down.
The word Default appears in the Default Column.

Remove FTP Locations

You can remove FTP locations.

To remove FTP locations

1. Click the System Registry tab, and select Non-Sysplex Systems, Sysplexes, or Shared DASD Clusters from the tree at the left. The detailed information appears at the right.
2. Select the system where you want to delete FTP locations.
3. Click the FTP Locations tab.
The FTP Locations window appears.
4. Click the Select box for each FTP location you want to remove.
5. Click the Remove link and then click OK to the Remove FTP location confirmation window.
The FTP location is removed.

Remote Credentials

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

Important! Remote Credentials are validated during the deployment process. It is the responsibility of the user to have the correct Owner, Remote User ID, Remote System Name, password, and authenticated authorization before creating a new remote credential.

You can [add](#) (see page 78), [edit](#) (see page 79), or [delete](#) (see page 80) remote credentials.

Add Remote Credentials

You can add remote credentials.

Important! Remote Credentials are validated during the deployment process. It is the responsibility of the user to have the correct Owner, Remote User ID, Remote System Name, password, and authenticated authorization before creating a new remote credential.

Note: The asterisk indicates that the field is mandatory.

To add remote credentials

1. Click the Setting tab, and select Remote Credentials from the tree at the left. The detailed information appears at the right.
2. In the Remote Credentials Account panel, click the New button. The New Remote Credential window appears.
3. Enter a correct Remote User ID.

Limits: Maximum 64 characters.

4. 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.

5. 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.

6. 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.

7. Click OK the remote credential entry appears on Remote Credentials Accounts List.
8. Click Apply to apply and save your changes.

Edit Remote Credentials

You can edit remote credentials.

Important! Remote Credentials are validated during the deployment process. It is the responsibility of the user to have the correct Owner, Remote User ID, Remote System Name, password, and authenticated authorization before creating a new remote credential.

Note: The asterisk indicates that the field is mandatory.

To edit remote credentials

1. Click the Setting tab, and select Remote Credentials from the tree at the left. The detailed information appears at the right.

2. In the Actions drop down list, click Edit for the remote credential you want to edit. The Edit Remote Credential window appears.

3. Enter a correct Remote User ID.

Limits: Maximum 64 characters.

4. 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.

5. Enter a correct password.

This must be entered each time a remote credential is edited.

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.

6. Enter the correct confirm password.

This must be entered each time a remote credential is edited.

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.

7. Click OK.

The remote credential entry appears on Remote Credentials Accounts List.

8. Click Apply to apply and save your changes.

Delete Remote Credentials

You can delete remote credentials.

To delete remote credentials

1. Click the Setting tab, and select Remote Credentials from the tree at the left.
The detailed information appears at the right.
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.

Deploying Products

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

About Deployments

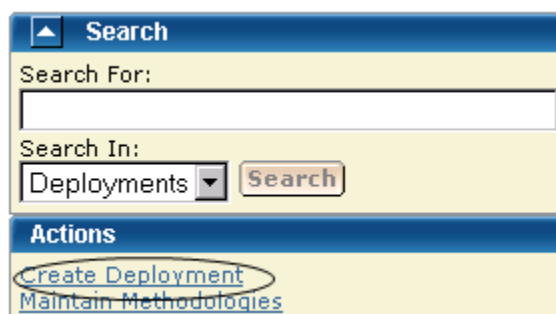
Deployments allow system objects to be deployed across the enterprise. These services enable deployment across both "Shared DASD" environments and networked environments. The objects to be deployed include target libraries defined to SMP/E and user-selected data sets.

Create a Deployment using the Product Wizard

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

To create a deployment

1. Click the Deployments tab, and then in the Actions section, Create Deployment link.



The Deployment of Products wizard appears.

Enter Name and Description

Note: The asterisk indicates that the field is mandatory.

Do the following

1. 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 window 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 88) until a successful snapshot has been created.

CSI Selection

The CSI selections listed were preselected from the SMP/E Environments window. You can select a CSI.

To select a CSI


1. Select a CSI, and click Next.

The Product Selection window 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 88) until a successful snapshot has been created.

Product Selection

To select a product

1. Select a product from the list.
2. 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.
3. 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.

4. Click Next.

Note: If you do not see any products showing up to select that means the appropriate PTF which enables your products deployment through metadata has not been installed.

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 88) until a successful snapshot has been created.

Custom Data Sets Selection window appears.

Custom Data Sets

A *custom data set* contains either an z/OS data set or USS parts paths. For an 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 110) 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 110) and type of copy. Type of copy can be either a container copy or a file-by-file copy.

To select a custom data set

1. Select a custom data set from the list. Click Select and then Next.

Note: To add a new custom data set click the Add Data Set button and [enter the custom data set information](#) (see page 97).

The Methodology Selection window appears.

More information:

[Add a Custom Data Set](#) (see page 97)

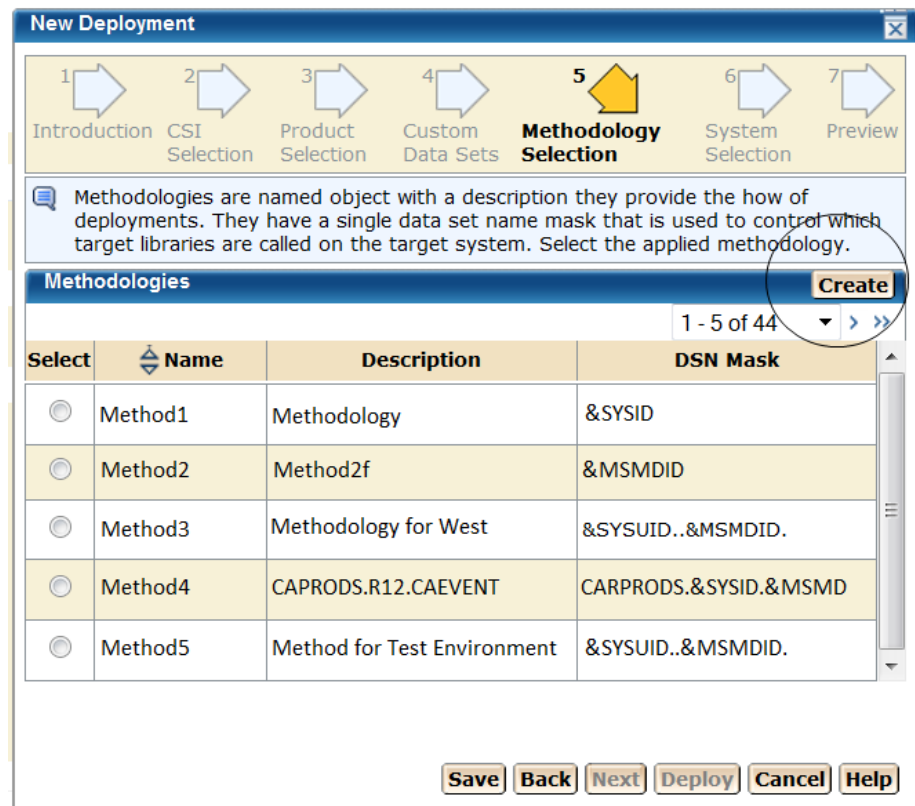
Methodology Selection

The methodology lets you provide a single data set name mask that is used to control the target library names on the target system.

To select a Methodology

1. Select a Methodology from the list and click Next.

Note: To create a new methodology click the Create button and [enter the new methodology information](#) (see page 106).



System Selection window 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 88) until a successful snapshot has been created.

More information:

[Create a Methodology](#) (see page 106)

System Selection

1. Select the systems to be deployed

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

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.

System to deploy			
			Show All
<input type="checkbox"/> Select	Name	Type	Description
<input type="checkbox"/>	XX61	Sysplex	Production System 1
<input type="checkbox"/>	PLEX1	Sysplex	Production System 2
<input type="checkbox"/>	PLEX1:CO1	Sysplex System	Sysplex System West

2. Click Next.

The Preview window 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 88) until a successful snapshot has been created.

Preview

1. Click Save to save the deployment
or
2. Click Deploy to set up this deployment.

Note: Click Cancel to exit this procedure without saving.

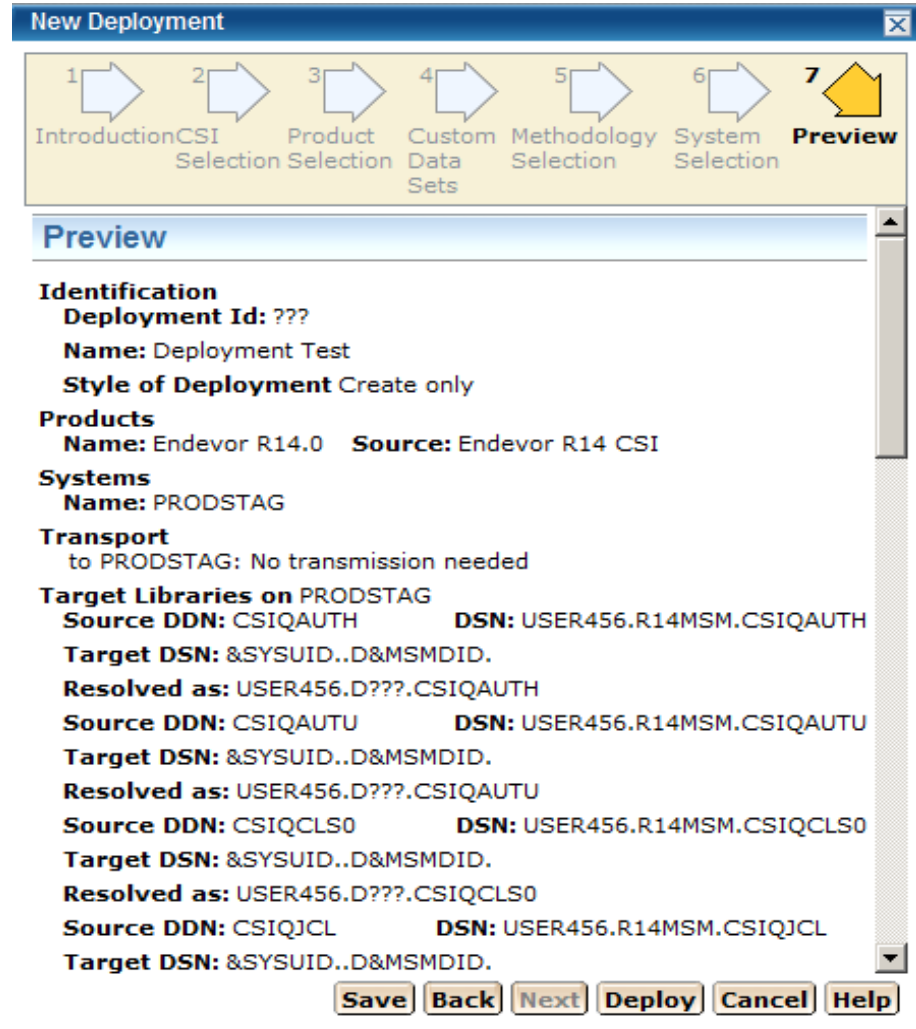
The Preview identifies the deployment by name and briefly states the products, systems, means of transport, target libraries including source, target and resolution, as well as SMP/E environment and snapshot information.

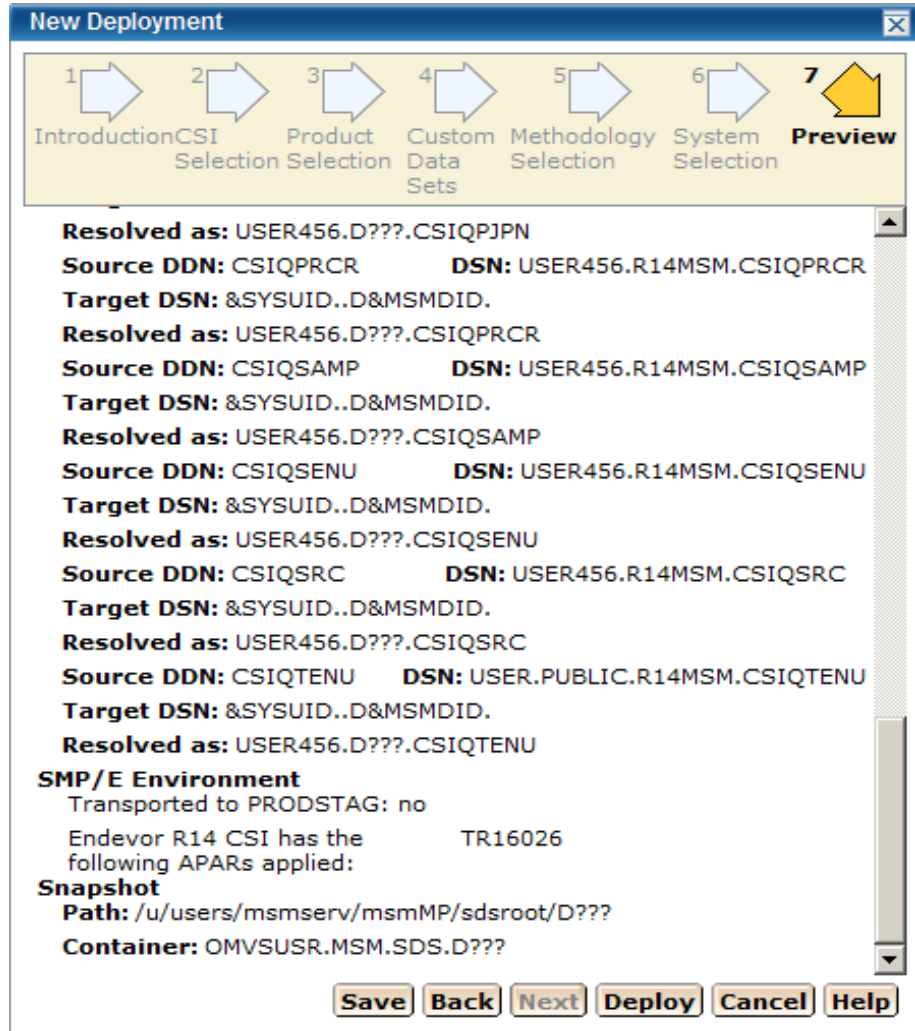
Important! Data sets may need to be APF Authorized and/or added to the Link List and/or Link Pack Area. These data sets are identified in this dialog.

Note: Any ??? in the Preview means that CA MSM has not assigned this value yet. For example, before a Product Deployment is deployed the MSMDID shows as ???. After deployment the Automatic ID is assigned by CA MSM and this is the MSMDID.

Deployment Preview Sample

This sample shows a deployment ready to be deployed.



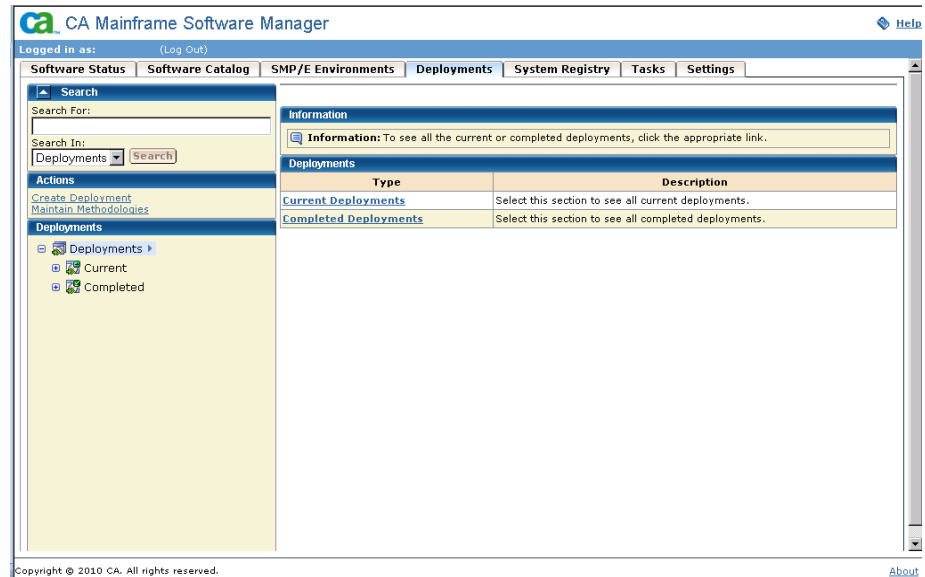


View a Deployment

You can view a deployment by using the CA MSM.

To view a deployment

1. Click the Deployments tab, and select the current or completed deployment from the tree at the left. The detailed deployment information appears at the right.



Maintain Deployments

You can maintain 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.

To maintain deployments

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.

The screenshot shows the 'Deployments' tab selected in the top navigation bar. The left sidebar contains a search bar and a tree view under 'Deployments' with sub-items: 'Current', 'Test Environment', 'QA Environment', and 'Production_A'. The main content area is titled 'Current' and contains an 'Information' section with a message: 'Information: This page contains basic information about current deployments. To see more details, click the appropriate link in the table.' Below this is a table titled 'Current Deployments' with columns 'Name', 'Description', and 'Actions'. The table lists four deployments: 'Test Environment' (Authorized development tester only), 'QA Environment' (Authorized Quality Assurance personnel), 'Production_A' (Production Alpha System), and 'Production_B' (Production Beta System). Each row has an 'Actions' button.

Name	Description	Actions
Test Environment	Authorized development tester only	Actions
QA Environment	Authorized Quality Assurance personnel	Actions
Production_A	Production Alpha System	Actions
Production_B	Production Beta System	Actions

3. Click the Deployment Name link for the Deployment you want to maintain. 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.

Test Environment 768 Actions ▾

Deployments > Current > Test Environment 768

Information

Information: To add products, use the action button on the Product List panel.
To add systems or clusters, use the action button on the System List panel.

▲ **Deployment Details** Save

Deployment Name*: Test Environment 768

Description:

Current State: Under Construction

Methodology*: Edit

Deployment ID: 634

Product List Add Products

Select and: [Remove](#) Show All ▾

<input type="checkbox"/> Select	Product Name	Release/Genlevel	SMP/E Environment	Actions
<input type="checkbox"/>	CA Auditor - MVS	55 58	Auditor Installation	Actions ▾

System List Add Systems

Select and: [Remove](#) Show All ▾

<input type="checkbox"/> Select	System Name	Type	Description	Actions
<input type="checkbox"/>	TestSys2	Non-Sysplex System	test system	Actions ▾
<input type="checkbox"/>	Sysplex2	Sysplex	Sysplex test system	Actions ▾
<input type="checkbox"/>	Clustertestsys2	Shared DASD Cluster	Cluster test system	Actions ▾

Selected 0 of 3.

4. To maintain a methodology, select a methodology from the drop down list. To edit the selected methodology click the edit button and the [Edit Methodology window](#) (see page 119) appears.

Note: The Deployment ID is the value of the MSMID variable.

5. You can select, [add](#) (see page 96), or [remove](#) (see page 97) a product.
6. You can select, [add](#) (see page 123), or [remove](#) (see page 124) a system.
7. You can select, [add](#) (see page 97), or [remove](#) (see page 106) a custom data set.
8. Click Save on the Deployment Details window.

9. Click Actions button 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 94)

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 including 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

You can reset a deployment status when the deployment has a status of *snapshot in progress*, *transmitting*, or *deploying*. See reset status for a list of deleted files.

10. Click Save on the Deployment Details window.

More information:

[Edit a Methodology](#) (see page 119)

[Add a Product](#) (see page 96)

[Remove a Product](#) (see page 97)

[Add a System](#) (see page 123)

[Remove a System](#) (see page 124)

[Confirm a Deployment](#) (see page 94)

How to Investigate a Failed Deployment

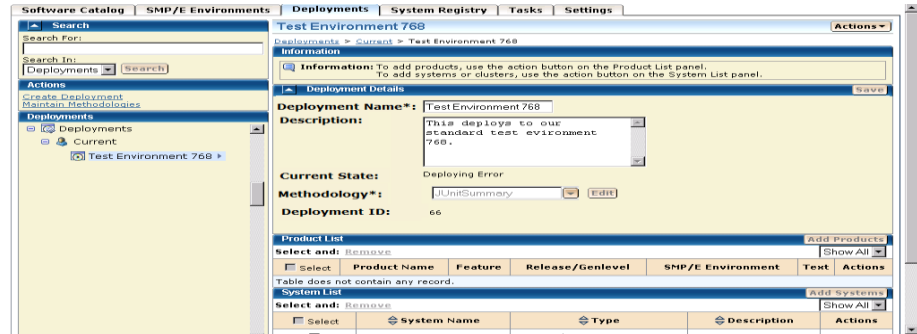
When a deployment fails, it can be investigate, corrected, and deployed again. The following procedures are defined.

- Investigate a deployment using the Tasks Page.
- Save a message log

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.

To investigate a failed deployment using the Tasks page

1. On the Deployments Page, in the left hand column find the deployment with an error and record the Deployment Name that failed.



2. Click the Tasks Tab and then click the Task History link. Click Refresh button on the right hand side of the Task History Bar to refresh the Task History display.
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, and then sort by Task ID.

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

Owner	Name	Type	Status	Start Time	Stop Time	Task ID
USER456	Deploy Test Environment 768	Deployment	Failed	1/26/2010 12:58:09PM	1/26/2010 12:59:14PM	980

4. The Task Manager window 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 “step name” link, in this case Deployment Lock SIS to view the results, and click on the messages logs to review the details for each error. See Troubleshooting for analyzing the error results. Correct the issue and deploy again.

The screenshot shows a window titled "Deployment Lock SIS" with a "Close" button in the top right. Below the title bar is a breadcrumb: "Deploy Test Environment 768 > Deployment Lock SIS". The window is divided into several sections:

- General:** Contains "Name: Deployment Lock SIS" and "Status: Failed". A "Download zipped output" button is in the top right of this section.
- MessageLog:** Contains the text: "SIS Lock command has started. Lock: true", "1 CSI repository is being used. Gathering information for lock.", and "Lock exists by USER null for resource Deployment Bernie1". An "Action" dropdown menu is in the top right.
- Explanation:** Contains the text: "Lock the appropriate SIS database records."
- Detailed Output:** Contains a table with columns: Name, Lines, Format, and Action. A "Show All" dropdown menu is in the top right of this section.

Name	Lines	Format	Action
errorLog	4	U	Action

More information:

- [Download Message Log](#) (see page 65)
- [Save a Message Log as a Data Set](#) (see page 66)
- [To Show All](#) (see page 67)

Delete a Deployment

You can delete deployments.

To delete a deployment

- Click the Deployments tab.
The Deployment window appears.
- On the right, in the Deployments panel click the current deployment link.
The detailed deployment information appears.
- Click the deployment name link.
- Click the Actions drop down list and select delete.
- Click OK to the Delete confirmation window.
The deployment is deleted.
See delete a deployment for a list of deleted files.

Delete a Completed Deployment

You can delete a completed deployment.

To delete a completed deployment

1. Click the Deployments tab. The Deployment window appears.
2. On the right, in the Deployments panel click the Completed Deployments link.

A list of completed deployments appears.

3. Select the completed deployment you want to delete.
4. Click the Delete link and then OK to the Delete confirmation window.

The completed deployment is deleted.

Confirm a Deployment

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 Completed deployment list.

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

To confirm a deployment

1. Click Confirm and Confirmation Dialog window appears.

Review the confirmation.

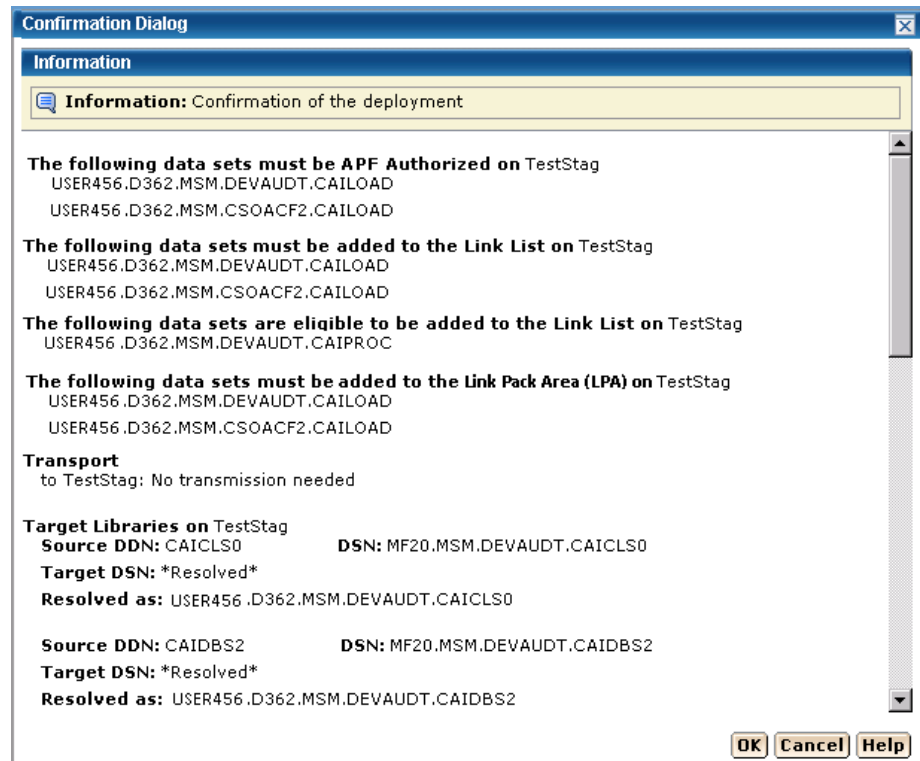
2. Click OK when the deployment is correct.

Note: Click Cancel to exit this procedure without confirming.

The Deployment Summary window contains none or any of 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

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




Products

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

Add a Product

You can add a product to a deployment.

To add a product to a deployment

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 97).
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.

To remove a product from a deployment

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 97), [edit](#) (see page 102), and [remove](#) (see page 106) custom data sets from a deployment.

Add a Custom Data Set

You can add custom data sets to a deployment.

To add custom data sets to deployment

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.

- In the Custom Data Sets List panel click Add Data Sets.

The Add Custom Data Sets window appears.

Note: The asterisk indicates that the field is mandatory.

- Select a Product from the drop down list.

Note: When there is information in the Instructions field they are required directions supplied by CA Support.

- Select the Data Set Type either data set (step 7) or USS (step 10).

Default: data set

- 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 and/or click the file icon and select a [symbolic name](#) (see page 110).

Mask

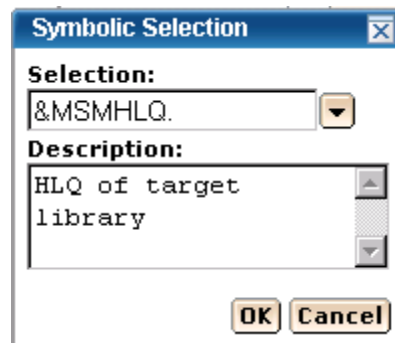
This is the mask that will be used to name the data sets that are being deployed. They can contain [symbolic qualifiers](#) (see page 110). For example, if you enter CAPRODS.&SYSID, the &SYSID is replaced by its values, and if the SYSID that is being deployed to is XX16, the dsn mask will be CAPRODS.XX16

Limits: Maximum 64 characters.

Note: Each deployed target data set will be 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 insures uniqueness of the final data set name.

Note: Two consecutive periods are required to separate the two masks.

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.



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.

The screenshot shows a dialog box with the following fields and options:

- Data Set Type*:** Radio buttons for Data Set and USS.
- Local Path*:** A text input field.
- Remote Path*:** A text input field with a file icon button to its right.
- Type of Copy:** Radio buttons for Container Copy and File-by-file Copy.
- Buttons: **OK**, **Cancel**, and **Help**.

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 110). The remote path is the path were the files are to be copied to.

Limit: Maximum 255 characters.

12. Select Type of Copy container copy (step 14) or File-by-file Copy (step 15).

Note: For file-by-file copy the user must make sure the USS path exists on all of the remote systems of this deployment. And has 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 110).

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 is has a maximum length of 44 characters including the periods.

Note: For container copy the following will occur during the deployment process:

- a. A file system of the requested type will be created
- b. The size of the file system will be computed as follows:
 - The size off 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 will be 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.

The screenshot shows a dialog box with the following fields and controls:

- Type of Copy:** Two radio buttons, with for "Container Copy" and for "File-by-file Copy".
- Container Name*:** A text input field with a file icon on the right.
- Type of Container*:** A dropdown menu.
- Mount Point*:** A text input field with a file icon on the right.
- % Free Space *:** A text input field containing the number "0".
- Buttons:** "OK", "Cancel", and "Help" buttons are located at the bottom right.

Note: The asterisk indicates that the field is mandatory.

- 15. Select the Type of Container from the drop down box. Either zFS or HFS.
- 16. Enter the Mount Point and/or click the file icon and select a [symbolic name](#) (see page 110).

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 any leaf in the USS file system can be a mount point, 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.

To edit a custom data set

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 Actions drop down list and click edit.
The Add Custom Data Sets window appears.

Edit Custom Data Set

Edit a custom data set by selecting the Product, Data Set Name, and the Mask.
Note: The Instructions are required directions supplied by CA Support.

Product*: CA Auditor for z/OS

Instructions:

Data Set Type*: Data Set USS

Data Set Name*:

Mask*:

OK Cancel Help

Note: The asterisk indicates that the field is mandatory.

5. Select a Product from the drop down list.

Note: When there is information in the Instructions field they are required directions 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 MSM to include in the deployment when it is deployed on the target systems.

8. Enter the Data Set Name Mask and/or click the file icon and select a [symbolic name](#) (see page 110).

Mask

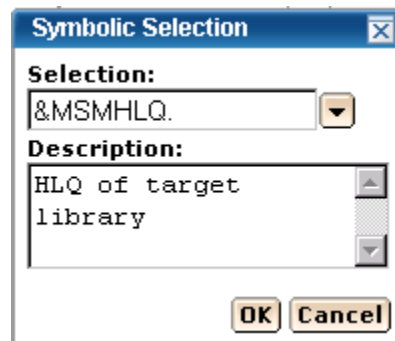
This is the mask that will be used to name the data sets that are being deployed. They can contain [symbolic qualifiers](#) (see page 110). For example, if you enter CAPRODS.&SYSID, the &SYSID is replaced by its values, and if the SYSID that is being deployed to is XX16, the dsn mask will be CAPRODS.XX16

Limits: Maximum 64 characters.

Note: Each deployed target data set will be 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 insures uniqueness of the final data set name.

Note: Two consecutive periods are required to separate the two masks.

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.



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.

The screenshot shows a configuration dialog box with the following fields and options:

- Data Set Type*:** Radio buttons for Data Set and USS.
- Local Path*:** A text input field.
- Remote Path*:** A text input field with a file icon button to its right.
- Type of Copy:** Radio buttons for Container Copy and File-by-file Copy.
- Buttons for **OK**, **Cancel**, and **Help** at the bottom right.

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 110). The remote path is the path where the files are to be copied to.

Limit: Maximum 255 characters.

12. Select Type of Copy container copy (step 14) or File-by-file Copy (step 15).

Note: For file-by-file copy the user must make sure the USS path exists on all of the remote systems of this deployment. And has 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 110).

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 will occur during the deployment process:

- a. A file system of the requested type will be created
- b. The size of the file system will be 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 will be 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.

The dialog box contains the following elements:

- Type of Copy:** Two radio buttons: Container Copy and File-by-file Copy.
- Container Name*:** A text input field with a file icon on the right.
- Type of Container*:** A dropdown menu.
- Mount Point*:** A text input field with a file icon on the right.
- % Free Space *:** A text input field containing the number 0.
- Buttons:** OK, Cancel, and Help buttons located at the bottom right.

Note: The asterisk indicates that the field is mandatory.

15. Select the Type of Container from the drop down box. Either zFS or HFS.
16. Enter the Mount Point and/or click the file icon and select a [symbolic name](#) (see page 110).

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 any leaf in the USS file system can be a mount point, 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.

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.

To remove a custom data set

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.

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 106), maintain, [edit](#) (see page 119), and [delete](#) (see page 122) methodologies from a deployment.

Create a Methodology

You can create a methodology.

Note: The asterisk indicates that the field is mandatory.

To create a methodology

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

New Methodology

Information

Information: Name the methodology, provide data set name mask, and select the style of deployment.

Methodology Information

Name*:

Description:

Data Set Name Mask

*

Style of Deployment

Create only

Create or Replace

Save **Cancel** **Help**

3. Enter the description of this methodology.

Limits: Maximum 255 characters.

4. Enter the data mask name and/or click the file icon and select a [symbolic name](#) (see page 110).

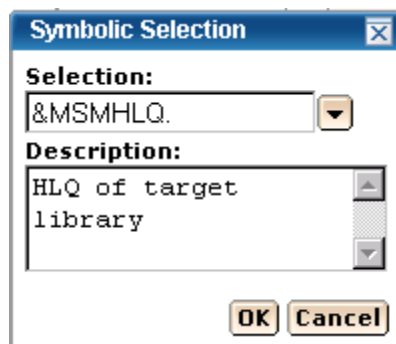
Data Set Name Mask

This is the mask that will be used to name the data sets that are deployed. They can contain [symbolic qualifiers](#) (see page 110). 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 will be 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 help ensures uniqueness of the final data set name.

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.



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.

Replace or Create

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).

Note: 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: 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.

Note: Click Cancel to exit this procedure without saving.

Symbolic Qualifiers

The symbolic qualifiers with description for the Data Set Name Mask and the Directory Path follow.

Data Set Name Mask

Data Set Name Mask 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

Directory Path 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 &LYYMMDD. 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 dataset name segment.

Example: Assume MSMDID is 255.

```
SYSWORK.D&MSMDID..DATASET
```

Note: The double dots are important, since the first dot is part of the symbolic name, it will 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 MVS 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 &LYMMDD. 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&LYMMDD..DATASET, translates to
SYSWORK.D100401.DATASET

An incorrect specification of the mask would be:

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

Directory Paths

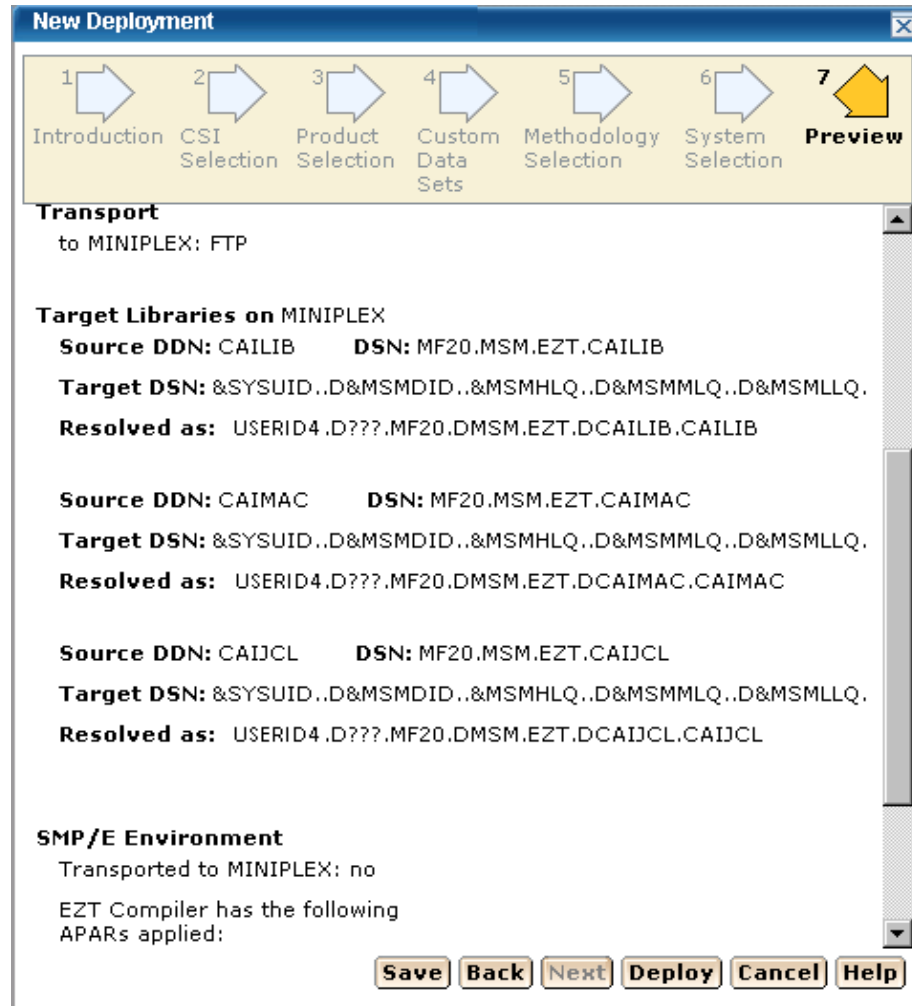
Symbolic substitution works in the same logical way for directory paths. However, directory paths do not typically have periods in them, so you will typically not see the double dots in directory paths.

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 MSM Deployment ID.

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

MSMMPN

This is the MSM Mount Point Name. The value is entered into the mount point name field when [adding a custom data set](#) (see page 97) 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 MSM system object name.

SYSCONE

This is the shorthand name of the system.

Limits: Maximum 2 characters.

SYSNAME

This is the system name entered when a Non-Sysplex System, 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 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.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 last 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**LYYMMDD**

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

LMON

This is the local month.

LMON 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

Edit a Methodology

You can edit a methodology by updating or modifying any of the fields on the Edit Methodology window.

To edit a methodology

1. Click the Deployments tab, and in the Actions section click the Maintain Methodologies link.
2. Select the methodology that you want to edit and click Edit.

The Maintain Methodologies select window 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 and/or click the file icon and select a [symbolic name](#) (see page 110).

Data Set Name Mask

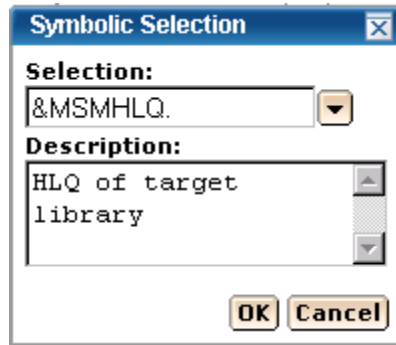
This is the mask that will be used to name the data sets that are deployed. They can contain [symbolic qualifiers](#) (see page 110).

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 will be 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 insures uniqueness of the final data set name.

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 is has a maximum length of 44 characters including the periods.



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.

Replace or Create

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).

Note: 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: 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.

- Click Save.

Note: Click Cancel to exit without saving your changes.

More information:

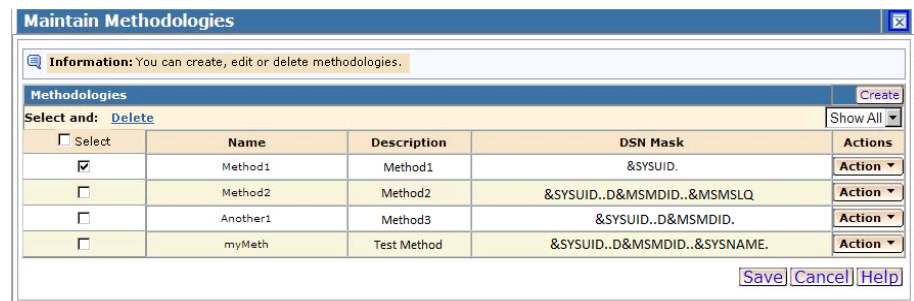
[Symbolic Qualifiers](#) (see page 110)

Delete Methodologies

To delete methodologies

- 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.

Add a System

You can add a system to a deployment.

To add a system

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. 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.

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

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.

System to deploy			
<input type="checkbox"/> Select	<input type="checkbox"/> Name	<input type="checkbox"/> Type	<input type="checkbox"/> Description
<input type="checkbox"/>	XX61	Sysplex	Production System 1
<input type="checkbox"/>	PLEX1	Sysplex	Production System 2
<input type="checkbox"/>	PLEX1:CO1	Sysplex System	Sysplex System West

6. Click OK.
The Preview window appears.
The system is added.

Remove a System

You can remove a system from a deployment.

To remove a system

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 wish to remove the product 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

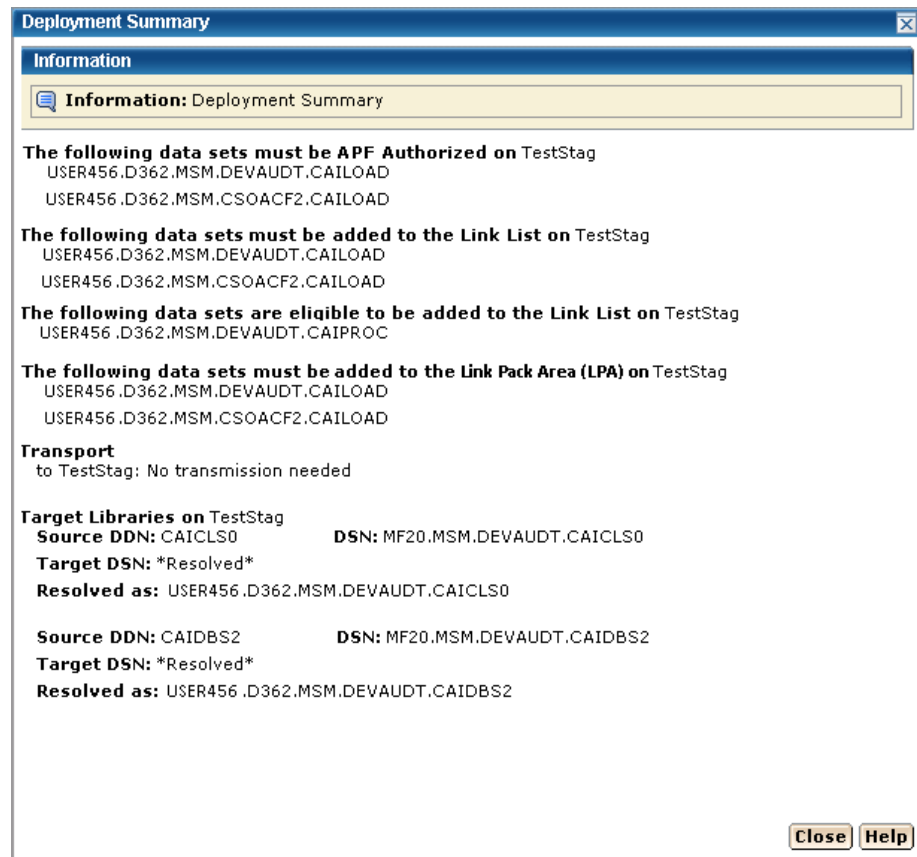
This Action button is available after a successful deployment.

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

The Deployment Summary window contains none or any of 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

This 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

Use the procedures in this section to acquire and install your product using Pax-Enhanced Electronic Software Delivery (ESD).

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

This section contains the following topics:

- [How to Install a Product Using Pax-Enhanced ESD](#) (see page 127)
- [Allocate and Mount a File System](#) (see page 133)
- [Copy the Product Pax Files into Your USS Directory](#) (see page 134)
- [Create a Product Directory from the Pax File](#) (see page 139)
- [Copy Installation Files to z/OS Data Sets](#) (see page 140)
- [Receiving the SMP/E Package](#) (see page 142)
- [Clean Up the USS Directory](#) (see page 145)
- [Apply Maintenance](#) (see page 146)

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. Experienced UNIX users may find the Pax-Enhanced ESD Quick Reference Guide or this overview sufficient 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 used for the ESD process.

Important! If you prefer not to involve all CA 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 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 new directory in your USS directory by entering the following command:

```
pax -rvf pax-file-name
```

4. Use the SMP/E GIMUNZIP utility to create z/OS installation data sets. The file UNZIPJCL in the directory created by the pax command in Step 3 contains a sample job to GIMUNZIP the installation package. Edit and submit the UNZIPJCL job.
5. Receive the SMP/E package. For this step, use the data sets created by GIMUNZIP 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 created by the pax command, all of the files in it, and the SMP/E RELFILEs, SMPMCS, and HOLDDATA data sets.

More Information:

[USS Environment Setup](#) (see page 132)

[Allocate and Mount a File System](#) (see page 133)

[Copy the Product Pax Files into Your USS Directory](#) (see page 134)

[Create a Product Directory from the Pax File](#) (see page 139)

[Copy Installation Files to z/OS Data Sets](#) (see page 140)

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. For additional ESD information, go to <http://www.ca.com/mainframe>. Under Events, we offer an ESD webcast to further explain the Pax-Enhanced ESD process.

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 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 129) 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

CA product ESD packages can be downloaded multiple ways. Your choices depend on the size of the individual files and the number of files 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. It lists all components of the product. You can use the Download Cart by checking one or more components that you need or check the 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](#)

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

[View Download Cart](#)

Add All to cart

Product Components				Add to cart	Download
CA COMMON SERVICES PROD PKG 11SP08AW000.pax.Z	11.0 /SP08	03/31/2010	407MB	<input type="checkbox"/>	Download
CA EARL PRODUCT PACKAGE 610106AEO00.pax.Z	6.1 /0106	03/31/2010	1MB	<input type="checkbox"/>	Download
EARL PIPPACK AEO61010600.pdf	6.1 /0106	03/31/2010	93KB	<input type="checkbox"/>	Download
EARL INSTALL GUIDE MANUAL I2J2ED610NE.pdf	6.1 /0000	03/31/2010	361KB	<input type="checkbox"/>	Download
CA COMMON SERVICES COVER LTR QI92742.pdf	11.0 /SP08	03/31/2010	46KB	<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 product files ordered, 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 methods let 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, New York-based FTP servers.

The Create a Zip File option first creates the zip and when ready, offers the options shown by the Zip Download Request examples in the next screen.

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 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 set up. You need to complete the USS setup only one time. You reuse the same directory for subsequent downloads. Alternatively, you can create a new 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 used for the ESD process. In the file system that contains the ESD directories, you also need free space approximately 3.5 times the pax file size 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 Pax-Enhanced ESD downloads.

This procedure details how to perform the following tasks:

- Allocate an HFS file system
- Create a new mount point in an existing maintenance directory
- Mount the file system on the newly created mount point
- Optionally permit write access to anyone in the same group as the person who created the directory

Important! USS commands are case-sensitive.

To allocate and mount the file system

1. Allocate the HFS. For example:

```
//ALCHFS EXEC PGM=IEFBRI4
//CAESD DD DSN=yourHFS dataset name,
// DISP=(NEW,CATLG,DELETE),UNIT=3390,
// DSNTYPE=HFS,SPACE=(CYL,(primary,secondary,1))
```

The HFS is allocated.

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. For example, from TSO, enter the following command:

```
MOUNT      FILESYSTEM('yourHFS dataset name')  
           MOUNTPPOINT('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 *z/OS UNIX System Services User Guide (SA22-7802)*.

Copy the Product Pax Files into Your USS Directory

To begin the CA product installation procedure, copy the product's pax file into the USS directory 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 PC, and upload it to your z/OS system.
- Download the product file from CA Support Online to your PC. 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 PC to a USS directory on your z/OS system.

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

Important! Ensure that sufficient free space is available in the USS file system 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 should match the value in the Size column for the corresponding pax file on the CA Products Download window.

More Information:

[How the Pax-Enhanced ESD Download Works](#) (see page 129)
[ESD Product Download Window](#) (see page 129)

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 in the lower left corner of the PDF reader. This opens a window displaying attachments. 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.

To download files using batch JCL

1. Supply a valid JOB statement.
2. Replace *yourTCPIP.PROFILE.dataset* with the name of the TCPIP 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: You may also add files to a cart for multiple downloads.

The Download Method window opens.

7. Click FTP Request.

The Review Download Requests window opens and 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's world-wide content delivery network (CDN). If you are not able to download using the Preferred FTP method, your company may have security restrictions that require knowledge of and configuration for all servers that company employees can download from that are outside of your corporate network.

Host Name: ftp://ftpddownloads.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: For details regarding FTP, see 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, this job may fail and still return a zero condition code. You must read the messages in the job DDNAME SYSPRINT to verify the FTP succeeded.

After running the JCL, 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.      *
//*                                                                *
//* This job must be customized as follows:                        *
//* 1. Supply a valid JOB statement.                               *
//* 2. Replace "yourTCPIP.PROFILE.dataset" with the name of the TCPIP *
//*    profile data set for your system.                           *
//* 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,REGION=0K
//SYSTCPD DD DSN=yourTCPIP.PROFILE.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.

To upload files to the mainframe through a PC

1. Follow the procedures in [How the Pax-Enhanced ESD Download Works](#) (see page 10) 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's 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 sample a JCL job that you can copy directly to the mainframe. To access this job, click the paper clip icon in the lower left corner of the PDF reader. This opens a window displaying attachments. Double-click the file to view the sample JCL.

To create a product installation directory using the `Unpackage.txt` sample job

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: After making the changes noted in the job, 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.

Example 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.

To copy the Pax-Enhanced ESD installation files to z/OS data sets

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 product-specific details you need to complete the installation procedure.

You have identified 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.
 - b. Perform one of the following steps:
 - Change the SMPCPATH DD PATH to your SMP/E Java application classes directory, usually `/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 for z/OS data sets used by the installation process. We suggest that you use a unique HLQ for each expanded pax file to uniquely identify the package. Do not use the same value for *yourHLQ* as you will 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 should complete 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 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 at this point.

Note: For more information, see the IBM Reference Manual, *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 CA PMA Chargeback. 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 BL5SEEDIT 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 BL5SEEDIT 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 BL5SEEDIT macro each time you open a new SAMPJCL member. To edit all SAMPJCL members simultaneously, read and follow the instructions in the BL5EDALL member.

2. Open the SAMPJCL member BL51ALL in an edit session and execute the BL5SEEDIT macro from the command line.

BL51ALL is customized.

3. Submit BL51ALL.

This job produces the following results:

- The target and distribution data sets for CA PMA Chargeback are created.
- Unique SMPLTS, SMPMTS, SMPSCDS, and SMPSTS data sets for this target zone are created.

4. Open the SAMPJCL member BL52CSI in an edit session and execute the BL5SEEDIT macro from the command line.

BL52CSI is customized.

5. Submit BL52CSI.

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 BL53RECD in an edit session and execute the BL5SEEDIT macro from the command line.

BL53RECD is customized.

2. Submit the *yourhlq*.SAMPJCL member BL53RECD to receive SMP/E base functions.

CA PMA Chargeback is received and now resides in the global zone.

3. Open the SAMPJCL member BL54APP in an edit session and execute the BL5SEEDIT macro from the command line.

BL54APP is customized.

4. Submit the *yourhlq*.SAMPJCL member BL54APP to APPLY SMP/E base functions.

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

5. Open the SAMPJCL member BL55ACC in an edit session and execute the BL5SEEDIT macro from the command line.

BL55ACC is customized.

6. Submit the *yourhlq*.SAMPJCL member BL55ACC 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 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 created by the pax command 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.

To delete the pax files and product-specific directories

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 Product 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 created by the pax command.

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 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 BL5SEEDIT macro was customized in the installation steps. Verify that you still have the values from the base install.

4. Open the SAMPJCL member BL56RECP in an edit session and execute the BL5SEEDIT macro from the command line.

BL56RECP is customized with your jobcard, CSI location, and zone names.

5. Customize the BL56RECP SMPPTFIN and SMPHOLD DD statements to reference the FB 80 data sets for the PTFs and HOLDDATA.

6. Submit BL56RECP.

The PTFs and HOLDDATA are received.

7. Open the SAMPJCL member BL57APYP in an edit session and execute the BL5SEEDIT macro from the command line.

BL57APYP is customized.

8. Submit BL57APYP.

The PTFs are applied.

9. (Optional) Open the SAMPJCL member BL58ACCP in an edit session and execute the BL5SEEDIT macro from the command line.

BL58ACCP is customized.

10. (Optional) Submit *yourhlq.SAMPJCL* member BL58ACCP.

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.

Note: We recommend that you check for available maintenance; however, you may find that none is available. If maintenance is not available, go to Deploying Your Product.

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 two types of HOLDDATA:

System HOLDDATA

Indicates data that is an in-stream part of the SYSMOD instructing you of special conditions. Examples of system HOLDDATA are as follows:

ACTION

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

DEP

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

DELETE

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

DOC

Indicates a documentation change with this SYSMOD.

EC

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

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

External HOLDDATA

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

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

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

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

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

To reliably manage external HOLDDATA, allow SMP/E to manage it automatically. The only manual task is running a REPORT ERRSYSMODS. This report identifies any held SYSMODs already applied to your system. If the resolving SYSMOD is in receive status, SMP/E identifies the SYSMOD to apply to correct the situation.

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:

[Unload the Sample JCL from Tape](#) (see page 150)

[How to Install Products Using Native SMP/E JCL](#) (see page 151)

Unload the Sample JCL from Tape

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

To unload the sample JCL from tape

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 the SMP/E environment set up, go to Run the Installation Jobs for a Tape Installation.
 - If you *do not* have the SMP/E environment set up, go to Prepare the SMP/E Environment for Tape Installation.

How to Install Products Using Native SMP/E JCL

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

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

Prepare the SMP/E Environment for Tape Installation

The members in this procedure prepare the data sets, initialize the zones, and create the DDDEFs for CA PMA Chargeback. 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 BL5SEEDIT 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 BL5SEEDIT on the TSO command line, and press Enter to replace the defaults with your specifications.

The macro is ready to customize your BL5.SAMPJCL members.

Note: The following steps include instructions to execute the BL5SEEDIT macro each time you open a new SAMPJCL member. To edit all SAMPJCL members simultaneously, read and follow the instructions in the BL5EDALL member.

2. Open the SAMPJCL member BL51ALL in an edit session and execute the BL5SEEDIT macro from the command line.

BL51ALL is customized.

3. Submit BL51ALL.

This job produces the following results:

- The target and distribution data sets for CA PMA Chargeback are created.
- Unique SMPLTS, SMPMTS, SMPSCDS, and SMPSTS data sets for this target zone are created.

4. Open the SAMPJCL member BL52CSI in an edit session and execute the BL5SEEDIT macro from the command line.

BL52CSI is customized.

5. Submit BL52CSI.

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 BL53RECT in an edit session and execute the BL5SEEDIT macro from the command line.

BL53RECT is customized.

2. Submit the *yourhlq*.SAMPJCL member BL53RECT to receive SMP/E base functions.

CA PMA Chargeback is received and now resides in the global zone.

3. Open the SAMPJCL member BL54APP in an edit session and execute the BL5SEEDIT macro from the command line.

BL54APP is customized.

4. Submit the *yourhlq*.SAMPJCL member BL54APP to APPLY SMP/E base functions.

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

5. Open the SAMPJCL member BL55ACC in an edit session and execute the BL5SEEDIT macro from the command line.

BL55ACC is customized.

6. Submit the *yourhlq*.SAMPJCL member BL55ACC to ACCEPT SMP/E base functions.

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

Chapter 6: 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 BL5SEEDIT macro was customized in the installation steps. Verify that you still have the values from the base install.
4. Open the SAMPJCL member BL56RECP in an edit session and execute the BL5SEEDIT macro from the command line.

BL56RECP is customized with your jobcard, CSI location, and zone names.

5. Customize the BL56RECP SMPPTFIN and SMPHOLD DD statements to reference the FB 80 data sets for the PTFs and HOLDDATA.
6. Submit BL56RECP.

The PTFs and HOLDDATA are received.

7. Open the SAMPJCL member BL57APYP in an edit session and execute the BL5SEEDIT macro from the command line.

BL57APYP is customized.

8. Submit BL57APYP.

The PTFs are applied.

9. (Optional) Open the SAMPJCL member BL58ACCP in an edit session and execute the BL5SEEDIT macro from the command line.

BL58ACCP is customized.

10. (Optional) Submit *yourhlq.SAMPJCL* member BL58ACCP.

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.

Note: We recommend that you check for available maintenance; however, you may find that none is available. If maintenance is not available, go to Deploying Your Product.

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 two types of HOLDDATA:

System HOLDDATA

Indicates data that is an in-stream part of the SYSMOD instructing you of special conditions. Examples of system HOLDDATA are as follows:

ACTION

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

DEP

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

DELETE

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

DOC

Indicates a documentation change with this SYSMOD.

EC

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

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

External HOLDDATA

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

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

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

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

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

To reliably manage external HOLDDATA, allow SMP/E to manage it automatically. The only manual task is running a REPORT ERRSYSMODS. This report identifies any held SYSMODs already applied to your system. If the resolving SYSMOD is in receive status, SMP/E identifies the SYSMOD to apply to correct the situation.

Note: When you have completed the procedures in this section, go to *Configuring Your Product*.

Chapter 7: Configuring Your Product

This chapter describes the minimum configuration tasks needed before CA PMA Chargeback can be started, customized, and used in your environment.

This section contains the following topics:

[Step 1. Review System Requirements and Database Installation](#) (see page 157)

[Step 2. Complete the Worksheet](#) (see page 158)

[Step 3. Tailor LMP Keys](#) (see page 160)

[Step 4. Run cBASE Link-Edit](#) (see page 160)

[Step 5. Run cBASE Data Dictionary Link-Edit for CA Datacom](#) (see page 160)

[Step 6. Run DB2 BIND Procedure](#) (see page 161)

[Step 7. Allocate CAIKSPAR](#) (see page 161)

[Step 8. Customize CAIKSPAR](#) (see page 161)

[Step 9. Prepare the Database](#) (see page 162)

[Step 10. Create Schema for CA Datacom Users](#) (see page 163)

[Step 11. Create and Load Tables](#) (see page 164)

[Step 12. Allocate CAIKRPAR](#) (see page 165)

[Step 13. Customize CAIKRPAR](#) (see page 166)

[Step 14. Process DataManager IVP](#) (see page 166)

[Step 15. Print ORD Data File](#) (see page 166)

[Step 16. Process CA PMA Chargeback IVP](#) (see page 167)

[Step 17. Print CA PMA Chargeback Reconciliation File](#) (see page 167)

[Step 18. Generate CA PMA Chargeback Invoices](#) (see page 167)

[Step 19. Customize DataManager Online and CA PMA Chargeback Online](#) (see page 168)

[Step 20. Invoke DataManager Online](#) (see page 169)

[Step 21. Invoke CA PMA Chargeback Online](#) (see page 170)

[Step 22. Prepare for Live Data](#) (see page 170)

[Step 23. Grant Access to Additional Users](#) (see page 171)

[Step 24. Implement Security](#) (see page 172)

Step 1. Review System Requirements and Database Installation

Review the system requirements in the "Preparing for Installation" chapter. Pay special attention to the requirement for one of two databases: DB2 or CA Datacom. If you do not already have one, now is the time to install CA Datacom/AD. See the CA Datacom/AD installation and maintenance documentation for instructions on how to install the database.

Step 2. Complete the Worksheet

Complete the worksheet before going any further. The keywords on the worksheet are the same as the symbolic parameters used in the supplied installation JCL. If a default has been assigned in the supplied JCL, it is indicated under the associated item description of the worksheet.

1. What high-level qualifier has been defined for the CA Common Services libraries?

Default: CSIND='CAI' 1. CSIND=_____

2. If using CA Datacom, what high-level qualifier has been defined for those libraries?

Default: DCIND='CAI' 2. DCIND=_____

3. If using DB2, what is the name of your DB2 load library?

No default 3. DSNLOAD=_____

4. If using DB2, what is the subsystem ID?

No default 4. SUBSYSTEM_ID=_____

5. Which DASD volume do you plan to use for the JARS/OLF parameter files?

No default

5. PARMVOL=_____

6. What high-level qualifier do you plan to assign to the parameter files?

Default: PINDEX='CAI'

6. PINDEX=_____

7. What values do you plan to use for the following parameters?

7. DATABASE_NAME=_____

DB2 PLAN_ID=_____

SQL_TYPE=_____

SUBSYSTEM_ID=_____

CUSTOMER_NAME=_____

BASE_VERSION=_____

CHARGE_PREC=_____

RATE_PREC=_____

UNIT_PREC=_____

EURODB2=_____

CBLOAD_VERSION=_____

RECONCILIATION_FILE=____

Note: See the "Batch Processing & Reporting" chapter in the *User Guide* for information on these parameters.

Step 3. Tailor LMP Keys

The CA License Management Program (LMP) is one of the components of CA TCC: Total Client Care. LMP is comprised of three components: the CA product, the LMP product key certificate, and the common LMP enforcement software.

The key certificate contains an execution key for each CPU licensed at your site. These keys must be entered into the PPOPTION data set LMP product keys member, which has a default name of KEYS.

The LMP common enforcement software is distributed as part of the CAIRIM CA Common Services for z/OS.

Define the LMP execution key at this time. See the *CA Common Services for z/OS Getting Started* for detailed instructions.

Step 4. Run cBASE Link-Edit

Members IF23LKDC and IF23LKD2 link-edit the CA Datacom service routines or the DB2 plan database, respectively. Choose the appropriate member, depending on which database you are using.

Edit the JCL to conform to your data center's standards and the previously completed worksheet. Submit the job and review the output. Processing should complete with a return code of 0 or 4.

Note: Members IF23LKDC and IF23LKD2 are in the CA Common Services for z/OS sample JCL library.

Step 5. Run cBASE Data Dictionary Link-Edit for CA Datacom

If you are using CA Datacom, you must process member SP23DDLK to link-edit the Data Dictionary.

Edit the JCL to conform to your data center's standards and the previously completed worksheet. Submit the job and review the output. Processing should complete with a return code of 0.

Note: Member SP23DDLK is in the CA Common Services for z/OS sample JCL library.

Step 6. Run DB2 BIND Procedure

If you are using DB2 as your database access method, member SP23BIND runs the BIND procedure for the CA SDBS modules just installed by SYSMOD CSP2300. If you are not using DB2, proceed to the next step.

Edit the JCL to conform to your data center's standards and the previously completed worksheet. Submit the job and review the output. Processing should complete with a return code of 0.

Note: Member SP23BIND is in the CA Common Services for z/OS sample JCL library.

Important! The userid used in subsequent steps (referred to as the owner's ID or ownerid) *must* be authorized for the database by your database administrator. This userid *must* be used to complete the configuration.

Step 7. Allocate CAIKSPAR

Member CAKSPALL in CAJRJCL allocates the CAIKSPAR file. Edit this JCL to conform to your data center's standards using the previously completed worksheet. Submit the job and review the output to verify that processing completed with a return code of 0.

Step 8. Customize CAIKSPAR

Customize the CAIKSPAR data set to define your database environment. See the "Batch Processing & Reporting" chapter in the *User Guide* for information on customization. In order to process the IVPs, the Base_Version must be set to **TEST**.

Important! All the batch JCL STEPLIB statements must be reviewed and customized prior to processing.

- If CA Datacom is being used, ensure that the data set name matches the data set names used during CA Datacom installation. Also delete references to the DB2 library.
- If DB2 is being used, ensure that the data set name of the DB2 library is correct. Also delete the references to the CA Datacom libraries and remove the DCIND symbolic from all JCL members and PROCs.

Step 9. Prepare the Database

If the database system to be used by CA PMA Chargeback is:

- CA Datacom/DB, then complete task 9A.
- CA Datacom/AD, then complete task 9B.
- DB2, then complete task 9C.

Step 9A. Prepare CA Datacom/DB

Before running the schema (Step 10) for CA Datacom/DB, the PMA490 database must be set up. JCL to set up the database can be found in the CAJRJCL as member name CADBDATA. The JCL contains five steps:

- DDUPDATE - Adds the PMA490 database definitions to the dictionary.
- CPYPRD - Copies the PMA490 definitions to PROD status.
- CATALOG - Catalogs the PMA490 definitions to the CXX.
- IEFBR14 - Allocates the dataspace for index and data areas.
- INITLD - Initializes and NULL LOADs the PMA490 areas.

After completing the above steps successfully, continue with Step 10.

Note: If you are using Datacom r12 or later, the DBUTLTY program (see step INITLD) must be authorized.

Step 9B. Prepare CA Datacom/AD Database

The following jobs, provided in CAJRJCL, must be executed in the order listed below to prepare the CA Datacom/AD database.

- CADBDEF - Adds the PMA490 database definitions.
- CADDRTV - Verifies, copies to PROD, catalogs, and enables.
- CADBALLC - Allocates the dataspace for index and data areas.
- CADBUTIL - Initializes and NULL LOADs the database.

After completing the above steps successfully, continue with Step 10.

Note: If you are using Datacom r12 or later, the DBUTLTY program (see step INITLD in the CADBUTIL job) must be authorized.

Step 9C. Prepare DB2 Database

- Have the DB2 database administrator authorize the ID being used to install CA PMA Chargeback for DATABASE CREATE, TABLE CREATE, and GRANT authority.
- Create a database, buffer pool, and storage group to be used by CA PMA Chargeback.
- Grant access to the database and buffer pool to the ID being used to install CA PMA Chargeback.
- The following SQL commands can be used as a guide for setting up DB2 to prepare for CA PMA Chargeback.

```
CREATE DATABASE PMA490
STOGROUP SGPMA490
BUFFERPOOL BP0;
```

The above SQL statements will create and identify the PMACB database to DB2 using storage group CAI001 and buffer pool zero.

```
GRANT DBADM ON DATABASE PMA490 TO userid;
GRANT USE OF BUFFERPOOL BP0 TO userid;
GRANT USE OF STOGROUP SGPMA490 TO userid;
```

The SQL statements above grant database administrator authority and use of the buffer pool and storage group to the userid specified.

- Continue with Step 11.

Step 10. Create Schema for CA Datacom Users

CAJRJCL member CAKRSCH creates a schema authorizing an owner ID to allow access to the database. Be sure to customize the CAKRTAB PROC contained in CAJRPROC and CAKRSCMA contained in CAJRSQL.

- In CAKRSCMA, the default owner ID of DUMMY must be changed to the ID that is to be authorized (the installer's ID).
- In CAKRTAB, the PARM statement must be set as follows:

```
EXEC PGM=CAKRINST,PARM='CAIKSPCB,SYSADM'
```

The second parameter of the PARM statement indicates to the database installation program how to connect to the database. The SYSADM AUTH ID is a pre-authorized ID that can be used to authorize the first new userid (usually the installer's). Use SYSADM to perform the CREATE SCHEMA task authorizing the new owner ID (installer's ID). After successful completion of this step, change SYSADM in the CAKRTAB PROC to the userid just authorized in the CREATE SCHEMA step.

Step 11. Create and Load Tables

This is a two-step process where JCL members CAKRTBLI and CAKRTBLP are executed. Both members invoke the CAKRTAB procedure found in the CAJRPROC library. Before executing CAKRTBLI and CAKRTBLP, update CAKRTAB according to directions found in the member.

1. Member CAKRTBLI allocates and loads the required tables for both CA PMA Chargeback and DataManager. This member also creates indexes and synonyms for the owner's ID, and loads and commits the DataManager startup definitions, as well as the CA PMA Chargeback definitions needed for IVP processing.

This jobstream consists of four steps. Each of these steps utilizes input from additional CAJRSQL members. An overview of the steps and the input statements is provided in the table below. The last two columns of the table indicate whether customization is required for DB2 or Datacom.

Step	Description	Input	DB2	CA Datacom
STEP010	Creates Tables	CAKRDC8 CAKRDB8	N/A Y	Y N/A
STEP020	Create Synonyms	CAKRRCR84	Y	Y
STEP030	Load Dispatch Tables	CAKSCR81	N	N
STEP040	Load CA PMA Chargeback Tables — IVP	CAKRRCR88	N	N

For CA Datacom, input members that must be customized are CAKRDC8 and CAKRRCR84. In member CAKRDC8, change PMA490 to reflect the correct database name. In member CAKRRCR84, change *ownerid* to the DB owner's ID.

For DB2, input members CAKRDB8 and CAKRRCR84 must be customized. For member CAKRDB8, change DSNDB04 to reflect the correct database name. For member CAKRRCR84, change *ownerid* to the DB owner ID.

After completing this, customize CAJRJCL library member CAKRTBLI. The STEP010 step must be reviewed to ensure that the INPUT symbolic reflects the appropriate input, either CAKRDC8 or CAKRDB8. Submit the job and review the output to verify that processing completed with a return code of 0.

Note: Input members are from CAJRSQL.

2. Member CAKRTBLP will load CA PMA Chargeback IRD/ORD tables. Edit this member and select only the tables that you want to load. See Appendix B in the *DataManager User Guide* for a list of the predefined input and output records.

CAJRSQL members distributed with the product that are used as input to the CAKRINST program, include SQL "COMMIT" statements after every one-hundred inserts. The COMMIT statement commits all work to the database and held storage is freed.

Important! This removes the "ROLLBACK" capability if the job fails for any reason. It will be necessary for users to create backups for tables that are modified after initial installation before using CAKRINST.

Step 12. Allocate CAIKRPAR

Member CAKRCALL allocates CAIKRPAR. Customize the JCL to conform to your data center's standards using the previously completed worksheet. Submit the job and review the output to verify that processing has completed with a return code of 0.

Step 13. Customize CAIKRPAR

Customize the CAIKRPAR data set. For IVPs to run successfully, set the following:

- BASE = TEST
- CBLOAD = TEST
- RECON = YES

Note: For more information, see the "Batch Processing and Reporting" chapter in the *User Guide*.

Step 14. Process DataManager IVP

Member CAKSIVP processes IVP data using the startup definitions loaded in Step 11. Edit this JCL to conform to your data center's standards using the previously defined worksheet. Submit the job and review the output to verify that processing has completed with a return code of 0.

Validate that IVP processing completed successfully by reviewing the condition codes and the DataManager Load Processing Report. This report should show the following:

Input Statistics: JARS Record Read	544
IRDID Records Generated	213
Output Statistics: CAIKSOP MBJ	213

Step 15. Print ORD Data File

Customize the EARL PROC (CAKSEARL) located in CAJRPROC. Copy the CAKSEARL PROC to your user PROCLIB or use instream in CAJRJCL library member CAKSORDS.

Edit member CAKSORDS to conform to your data center's standards using the previously completed worksheet. Submit the job and review the output to verify processing completed with a return code of 0.

Step 16. Process CA PMA Chargeback IVP

This step uses the **committed** CA PMA Chargeback startup definitions loaded into the database during install Step 11, along with the ORD data file generated from Step 14 to apply charges to the CCCTAB and to generate a detailed reconciliation file.

Edit member CAKRIVP to conform to your data center's standards using the previously completed worksheet.

Submit the job and review the output to verify processing completed with a return code of 0. Review the CA PMA Chargeback Load Processing Summary Report. The records read should be equal to the total output records written to the ORD data file.

Validate that the IVP processing completed successfully by reviewing the condition codes and the CA PMA Chargeback Summary Control Report. The control report should show the following:

Records Read	213
Original Records Created	419
Records Inserted into CCCTAB	61

Step 17. Print CA PMA Chargeback Reconciliation File

The CA PMA Chargeback IVP process includes generation of the reconciliation file. Member CAKRECON uses Earl Service to print the reconciliation file. See Chapter 11 of the *User Guide* for detailed information.

Edit this member according to your data center's standards and the previously completed worksheet. Submit the job and review the output to verify that processing completed successfully. The record count of the SYSEARL should show the following:

Hitfile Records Written	419
Grand Total	2931.6712

Step 18. Generate CA PMA Chargeback Invoices

This step generates an invoice from the IVP data processed in Step 16. Member CAKRINVC uses Earl Service to generate an invoice.

Edit this member according to your data center's standards and the previously completed worksheet. Submit the job and review the output to verify that processing completed successfully.


```

ISPEXEC LIBDEF ISPLLIB LIBRARY ID(PMALIB)
CBASEX NEWCB
ISPEXEC LIBDEF ISPLLIB LIBRARY

```

Updating your CLISTs as shown in this section (instead of adding a STEPLIB statement to your TSOPROC) will reduce system overhead. When STEPLIBs are added to TSO LOGON PROCs, they are searched every time TSO commands are entered. By allocating as a TASKLIB within the CLIST and removing the TASKLIB on exiting the CLIST, no additional overhead is incurred.

4. **Set European DB2 (optional):**

Customize the CAIKSPAR data set to set EURODB2 = YES if you plan to use European DB2 with a comma as a decimal point separator. In addition, update CAJRCTMP library members NEWDM and NEWCB and uncomment the following three)*SET statements:

```

)*SET &&XXDECPNT = ,      ->  )SET &&XXDECPNT = ,
)*SET &&XXNTYPE = EUR     ->  )SET &&XXNTYPE = EUR
)*SET &&NTYPE = EUR       ->  )*SET &&NTYPE = EUR

```

Note: See step 8 for information on how to customize CAIKSPAR.

Step 20. Invoke DataManager Online

1. Log on executing the TSOPROC.
2. Execute CAI.CAJRCLS0(PMADMC) either through TSO or the ISPF TSO command processor.

Step 21. Invoke CA PMA Chargeback Online

1. Log on executing the TSOPROC.
2. Execute the CAI.CAJRCLS0(PMACBC) either through TSO or the ISPF TSO command processor.
3. Verify IVP results. Perform the following:
 - Select the online Query function.
 - Select Charge query.
 - On the Charge Query Primary panel (CBQQRYP) define the Query name and description. Press F2 to create.
 - On the Charge Query Specifications panel (CBQQRYS):
 - Ensure that the Version field is set to TEST.
 - Press F2 to execute the query.
 - The Charge Query Results panel (CBQQRYD) displays where you can verify IVP results.

Step 22. Prepare for Live Data

To complete the IVP process, the DataManager tables were committed to a TEST version and the CA PMA Chargeback tables were committed to TESTTEST. Processing of the CA PMA Chargeback IVP resulted in updating of the CCCTAB. The following steps are required to remove IVP data:

1. Delete the CCCTAB:

CAJRJCL member CAKRDEL1 deletes the IVP data records from the CCCTAB.

Edit this member to conform to your data center's standards using the previously completed worksheet. Submit the job and review the output to verify processing completed with a return code of 0.

Note: Processing of this member will result in the deletion of the CA PMA Chargeback IVP data.
2. Delete IVP CA PMA Chargeback Definitions (Optional):

CAJRJCL member CAKRDEL2 deletes the CBdefs that were utilized in processing of the CA PMA Chargeback IVP.

Edit this member to conform to your data center's standards using the previously completed worksheet. Submit the job and review the output to verify processing completed with a return code of 0.

Step 23. Grant Access to Additional Users

This step outlines the tasks necessary to grant additional users access to the CA PMA Chargeback tables

1. Authorize userid:

If you have installed the system using DB2, the new user must be granted EXECUTE access on the plans created when the bind procedure was run for DB2. The plan names are CAISSQL2, CAISSQL3 and CAISSQL9. The following SQL statement grants EXECUTE access to userid B0001:

```
GRANT EXECUTE ON PLAN CAISSQL2, CAISSQL3, CAISSQL9 TO B0001;
```

If you installed the system using CA Datacom, you must create a schema for the new user. Member CAKRSCM can be used. Be sure to customize CAKRSCMA. The userid must be changed to the new userid.

2. Grant access to userid:

Customize CAJRSQ member CAKRCR87 to reflect the userid requiring GRANT access. Edit CAJRSQ member CAKRGRNT to conform to your data center's standards. Submit the job and review the output to ensure that the job completed with a condition code of 0.

Note: If database security is not turned on, SQL error -559 will be returned when attempting to grant other users access to CA PMA Chargeback tables. You can proceed to the next step if you get this error.

3. Establish synonyms:

Note: This step must be executed by the userid requiring the synonyms.

Member CAKRSYN will establish synonyms. This member uses input member CAKRCR84 to complete this process. Edit CAKRSYN to conform to your data center's standards and make sure the owner ID of the tables you are creating synonyms for is reflected in CAKRCR84. The last SQL statement in member CAKRCR84 performs an insert into the options table to set up the default options for the new user. Change the first variable in the statement to the name of the new userid. This variable appears in the statement directly after the word "VALUES" as illustrated in the following example:

```
INSERT INTO XXXXXXXX.OPTTAB VALUES ('YYYYYYYY', 'BOTH', 'NOREV', ...
```

The XXXXXXXX in the above statement should be replaced with the userid (OWNER) that was originally used to create the tables. The YYYYYYYY should be replaced with the new userid.

- If the database system being used is DB2, run the CAKRSYN step from the userid that requires the synonyms.
- If the database system is CA Datacom, be sure to update the CAKRTAB PROC as follows:

```
EXEC PGM=CAKRINST, PARM='CAIKSPCB, YYYYYYYY'
```

Replace the YYYYYYYY parameter of the PARM statement with the name of the userid for which you are creating synonyms.

Step 24. Implement Security

Security of CA PMA Chargeback tables is implemented by protection of dialogs.

See the *User Guide* or the *DataManager User Guide* chapters on security and audit.

Chapter 8: Migration Information

This section contains the following topics:

[Update Database Tables](#) (see page 173)

Update Database Tables

After applying CA PMA Chargeback maintenance or installing a new version of CA PMA Chargeback, there is an optional step to perform database table updates. Member CAKRTBLM contained in CAJRJCL contains the JCL and instructions on how to perform table updates. Note that it uses the CAKRTAB procedure, customized during installation.

Before running the update job, review member CAKRTBLZ in CAJRSQL to determine if table updates are required. Member CAKRTBLZ contains a list of all modified IRD/ORD data sets by release and the SQL statements to delete IRD/ORD sets that may need to be refreshed. Update job CAKRTBLM is required only if IRD/ORD data sets that are in use by the current chargeback algorithm are listed in CAKRTBLZ and new metrics provided by the updated IRD/ORD data sets are needed in a chargeback algorithm.

Appendix A: Troubleshooting

This section contains the following topics:

[Verifying the Problem](#) (see page 175)

[Collecting Diagnostic Data](#) (see page 175)

[Interpreting Diagnostic Data](#) (see page 177)

Verifying the Problem

Before contacting Technical Support, attempt to resolve the problem using the following steps.

1. Examine the procedure that you used and compare it to the documented procedure for performing the required activity.
2. If you find no discrepancies between your procedures and the documented procedures, repeat the activity under conditions similar to those that existed when the problem first appeared. (If you no longer get unsatisfactory results, an inadvertent error may have caused the problem.)
3. If the same error occurs when you repeat a given activity, and you can find nothing in the documentation to suggest that your procedure is flawed, check with others at your site to determine if they have had the same or similar problem and how they handled it.

Collecting Diagnostic Data

Use the information below to see how to resolve various problems.

CA PMA Chargeback Online Facility

Unable to bring up the online facility

- Verify that member NEWCB in CAJRCTMP is correctly customized as outlined in the step Customize DataManager Online and CA PMA Chargeback Online in the chapter "Configuring Your Product."
- Verify that member PMACBC in CAJRCLS0 has been changed to reflect the appropriate high-level qualifiers.
- Verify that the CAJRLOAD library is allocated and available to the TSO session.
- Verify that the user CAIKRPAR (CAIKRPAR DD statement) correctly defines your database environment.
- Verify that the step Grant Access to Additional Users in the chapter "Configuring Your Product" has been completed.

Error in definition

If you attempt to define accounting sources for an ORD Type and receive a message that says the ORD Type does not exist, do the following:

- Verify that the DataManager version specified using the Option facility reflects the DataManager version with which the ORD Type was committed.
- If the ORD Types definition exists in the development version of DataManager, you must process the DataManager commit before these ORD Types can be used by CA PMA Chargeback for definition.

Period Functions — Forecasting

If you receive a message stating the Forecast version does not match the version specified in Options, perform the following steps.

- Exit the Forecasting panel.
- Select Options, then select item 2 (Versions) from the Options pull-down.
- Change the DataManager and CA PMA Chargeback version to match the CA PMA Chargeback version specified during generation of the forecast.

CA PMA Chargeback

Batch Processing Error

See the *Messages and Codes Guide* to determine appropriate reasons and actions for the error messages received.

DataManager

Batch Processing Error

See the *Messages and Codes Guide* to determine appropriate reasons and actions for the error messages received.

DataManager Online Facility

Unable to bring up the online facility

- Verify that member NEWDM in CAJRCTMP is correctly customized as outlined in the step Customize DataManager Online and CA PMA Chargeback Online in the chapter "Configuring Your Product."
- Verify that member PMADMC in CAJRCLS0 has been changed to reflect the appropriate high-level qualifiers.
- Verify that the CAJRLOAD library is allocated and available to the TSO session.
- Ensure that the user CAIKSPAR (CAIKSPAR DD statement) correctly defines your database environment.

Interpreting Diagnostic Data

When you have collected the specified diagnostic data, write down your answers to the following questions.

- What was the sequence of events prior to the error condition?
- What circumstances existed when the problem occurred and what action did you take?
- Has this situation occurred before? What was different then?
- Did the problem occur after a particular PTF was applied or after a new release of the software was installed?
- Have you recently installed a new release of the operating system?
- Has the hardware configuration (tape drives, disk drives, and so forth) changed?

From your response to these questions and the diagnostic data, try to identify the cause and resolve the problem.

If you determine that the problem is a result of an error in a CA product, you can make use of the CA online support system to see if a fix (APAR or PTF) or other solution to your problem has been published. Otherwise, contact [Technical Support](#).

Index

A

access
 login • 27
acquiring the product • 10, 28
acquisition
 download • 18, 29
add
 custom data set • 97
 data destination • 70
 FTP locations • 75
 product • 96
 system • 123
aggregated package, viewing • 44
allocate and mount • 133
allocating
 CAIKRPAR • 165
 CAIKSPAR • 161
authorization
 modes • 59

C

CA Datacom
 database preparation • 162
 schema creation • 163
CA LMP • 11
CA-C Runtime • 11
CAI.SAMPJCL
 library • 150
 sample jobs • 150
CAIKRPAR • 165, 166
CAIKSPAR • 161
CAIRIM • 11
CAISSF • 11
catalog, update • 28
cBASE data dictionary link-edit • 160
checklist for installation • 157
Common Services requirements • 11
completed deployment, remove • 94
confirming deployment • 94
contacting technical support • iii
copy files to USS directory • 134, 135, 138
create
 data destination • 68
 deployment • 80
 methodology • 106

 monoplex • 55
 shared DASD cluster • 58
 staging • 57
 sysplex • 55
creating tables • 164
CSIs (consolidated software inventories)
 creation • 38
 migration • 18
custom data sets
 add • 97
 edit • 102
 remove • 106
customer support, contacting • iii
customizing
 CA PMA Chargeback online • 168
 CAIKRPAR • 166
 CAIKSPAR • 161

D

data destinations
 add • 70
 create • 68
 delete • 74
 maintain • 71
 set default • 74
data set name mask • 110
database installation • 157
DataManager
 invoking online facility • 169
 process IVP • 166
DB2
 bind procedure • 161
 database • 163
 European • 168
 user access to • 171
default
 data destination • 74
 FTP location • 76
defining database environment • 161
delete
 completed deployment • 94
 data destination • 74
 development • 93
 product • 34
 product gen level • 34
 product release • 34

- system registry • 67
- delivery, product acquisition • 10
- deployment
 - about • 80
 - confirm • 94
 - create • 80
 - delete • 93
 - preview • 84
 - summary • 125
 - validation, failed • 62
 - view • 87
- diagnostic data • 175
- distribution
 - tape • 10
- distribution libraries • 14
- download • 18, 29
 - files using ESD • 129
 - installation packages • 18, 29
 - LMP keys • 39
 - maintenance packages • 18, 41
 - multiple installation packages • 31
 - options • 134
 - overview • 127
 - to mainframe through a PC • 138
 - using batch JCL • 135

E

- Earl Service • 11
- edit
 - custom data set • 102
 - methodology • 119
- ESD (Electronic Software Delivery) • 10
- European DB2 • 168
- external HOLDDATA • 147
- external packages
 - installation • 32, 34
 - migration • 30, 43

F

- failed validation • 62
- free space • 132
- FTP locations
 - add • 75
 - edit • 76
 - remove • 77
 - set default • 76

G

- generating invoices • 167

- GIMUNZIP utility • 140
- granting access to additional users • 171
- GROUPEXTEND mode • 48

H

- hardware requirements • 11
- hash setting • 140
- high-level qualifier • 140
- HOLDDATA • 147

I

- IEBCOPY • 150
- implementing security • 172
- installation • 18, 34
 - checklist • 157
 - tables • 164
 - worksheet • 158
- installation packages
 - download • 29
 - download multiple • 31
 - migration • 30
- installing
 - from Pax-Enhanced ESD • 127
 - from tape • 149
- Integrated Cryptographic Services Facility (ICSF) • 140
- internal HOLDDATA • 147
- investigating failed validation • 62
- invoices • 167
- invoking
 - CA PMA Chargeback online • 170
 - DataManager online • 169

J

- Java version support • 140

L

- libraries • 13
- LMP keys • 39
- LMP keys, tailoring • 160

M

- maintain
 - data destinations • 71
 - system registry • 59
- maintenance • 146
 - application • 18, 44
 - backout • 51

- GROUPEXTEND mode • 48
- USERMODs • 47
- maintenance packages
 - backout • 51
 - download • 18, 41
 - installation • 18, 44, 47
 - migration • 43
 - USERMODs • 47
 - viewing status • 47
- methodology
 - create • 106
 - remove • 122
 - symbolics qualifiers • 110
- migrations
 - installation packages • 30
 - maintenance packages • 43
- monoplex
 - create • 55
- multiple product installation packages,
 - download • 31

N

- nested packages • 44

O

- online facility • 169
- ORD data file, print • 166

P

- parameter libraries • 15
- pax ESD procedure
 - copy product files • 134
 - create product directory • 139
 - download files • 129
 - set up USS directory • 132
- pax file
 - copy files to USS directory • 134, 135, 138
- permanent (target) libraries • 13
- preparing for live data • 170
- printing
 - ORD data file • 166
 - reconciliation file • 167
- process overview • 127
- processing
 - CA PMA Chargeback IVP • 167
 - DataManager IVP • 166
- product
 - acquisition • 10
- product download window • 129

- product-level directory • 139
- products
 - acquired externally • 32, 43
 - add • 96
 - download • 18, 29
 - download multiple • 31
 - installation • 18, 34
 - maintenance • 18, 44, 51
 - remove from CA MSM • 34
 - remove from deployment • 97

R

- read me • 127, 140
- reconciliation file, print • 167
- remote credentials
 - add • 78
 - delete • 80
 - edit • 79
- remove
 - custom data sets • 106
 - FTP locations • 77
 - methodologies • 122
 - product • 97
 - system • 124
- requirements • 157
- running
 - cBASE data dictionary link-edit • 160
 - DB2 BIND procedure • 161

S

- sample JCL • 150
- sample jobs • 135, 139
 - CAtoMainframe.txt • 135
 - Unpackage.txt • 139
- scenarios, usage • 18
- security
 - implementation • 172
 - requirements • 13
- SMP/E
 - GIMUNZIP utility • 140
- software
 - delivery • 10
 - inventory • 28
- software requirements • 11
- SRAM Service • 11
- support, contacting • iii
- symbolic qualifiers • 110
- system • 11
 - add • 123

- remove • 124
- system registry
 - about • 52
 - authorization • 59
 - create non-sysplex • 53
 - create, data destination • 68
 - create, shared DASD cluster • 58
 - create, staging • 57
 - create, sysplex • 55
 - delete • 67

T

- tables loaded • 164
- tailoring LMP keys • 160
- tape, installing from • 149
- target libraries • 13
- technical support, contacting • iii
- troubleshooting • 175
- TSO requirements • 13

U

- UNIX System Services (USS)
 - access requirements • 127, 132
 - directory cleanup • 145
 - directory structure • 132
- UNZIPJCL • 140
- usage • 18
- USERMODs • 47

V

- viewing
 - aggregated package • 44
 - deployment • 87
 - maintenance package status • 47
- ViewPoint • 11

W

- worksheet, installation • 158