

CA PanAPT®

Installation Guide

r3.2



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

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

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

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

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

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

The manufacturer of this Documentation is CA.

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

Copyright © 2010 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

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

Documentation Changes

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

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

CA Technologies Product References

This document references the following CA Technologies products:

- CA Common Services for z/OS
- CA Mainframe Software Manager (CA MSM)
- CA Panvalet®

Contents

Chapter 1: Overview 13

Audience	13
How the Installation Process Works	14
CA PanAPT Options	15

Chapter 2: Preparing for Installation 17

System Requirements	17
Software Requirements	17
CA Common Services for z/OS	18
Security Requirements	18
Data Set Authorization	18
External Security Setup	19
Storage Requirements	20

Chapter 3: Installing Your Product Using CA MSM 21

CA MSM Documentation	21
Getting Started Using CA MSM	22
How to Use CA MSM: Scenarios	22
Access CA MSM Using the Web-Based Interface	31
Acquiring Products	32
Update Software Catalog	32
Download Product Installation Package	33
Migrate Installation Packages Downloaded External to CA MSM	34
Add a Product	35
Installing Products	37
Install a Product	37
Create a CSI	40
Download LMP Keys	43
Maintaining Products	44
How to Apply Maintenance Packages	44
Download Product Maintenance Packages	45
Download Maintenance Packages for Old Product Releases and Service Packs	46
Manage Maintenance Downloaded External to CA MSM	47
Manage Maintenance	49
GROUPEXTEND Mode	53
Back Out Maintenance	57

Setting System Registry	58
View a System Registry	58
Create a Non-sysplex System	59
Create a Sysplex or Monoplex.....	60
Create a Shared DASD Cluster	61
Create a Staging System.....	62
Authorization	63
Change a System Registry	64
Maintain a System Registry using the List Option.....	70
Delete a System Registry.....	71
FTP Locations	71
Data Destinations.....	75
Remote Credentials.....	81
Deploying Products	83
Deployment Status.....	84
Creating Deployments.....	85
View a Deployment	90
Change Deployments	91
Delete a Deployment	97
Confirm a Deployment.....	98
Products	100
Custom Data Sets	102
Methodologies	109
Systems	126
Deployment Summary	128

Chapter 4: Installing Your Product from Pax-Enhanced ESD 131

How to Install a Product Using Pax-Enhanced ESD	131
How the Pax-Enhanced ESD Download Works	133
ESD Product Download Window	133
USS Environment Setup	136
Allocate and Mount a File System.....	137
Copy the Product Pax Files into Your USS Directory	140
Download Using Batch JCL	141
Download Files to Mainframe through a PC	144
Create a Product Directory from the Pax File	145
Sample Job to Execute the Pax Command (Unpackage.txt)	146
Copy Installation Files to z/OS Data Sets.....	146
Receiving the SMP/E Package	147
How to Install Products Using Native SMP/E JCL	148
Prepare the SMP/E Environment for Pax Installation	148

Run the Installation Jobs for a Pax Installation	149
Clean Up the USS Directory	150
Apply Maintenance	151
HOLDDATA	151
Copy Modules to Authorized Link List Library (Optional)	152
Update Your Security System	152
Data Set Authorization	153
Define or Convert the VSAM CA PanAPT Database	156
Define or Convert the VSAM CA PanAPT History Database	156
Update the Model Exchange PDS (Optional)	157

Chapter 5: Installing Your Product from Tape 159

Unload the Sample JCL from Tape	160
How to Install Products Using Native SMP/E JCL	161
Prepare the SMP/E Environment for Tape Installation	161
Run the Installation Jobs for a Tape Installation	162
Apply Maintenance	163
Hold Data	164
Copy Modules to Authorized Link List Library (Optional)	165
Update Your Security System	165
Data Set Authorization	166
Define or Convert the VSAM CA PanAPT Database	169
Define or Convert the VSAM CA PanAPT History Database	169
Update the Model Exchange PDS (Optional)	170

Chapter 6: Preparing to Start Your Product 171

Verify Installation Checklist	171
Create TSO Logon Procedure	172
How the Modifying the ISPF Primary Option Menu Works	173
Create Test PDS Libraries	176
Set Up PF Keys	177
Edit Members in the CABYCLS0	177
Verify Online System	177
Edit Members in CAI.CABYDATA	179
Edit Members in CAI.CABYJCL	179
Verify Batch System	181
Complete Installation Checklist	181
Complete Editing Members in CABYJCL	182
Edit Members in CABYJCL (Optional)	182
Edit Members in CABYSKLO	182
Edit Members in CABYPARM (CA Panvalet Users Only)	183

Back Up CA PanAPT Files	183
Test Complete CA PanAPT System	184
Implement Move Cycles.....	185
Chapter 7: Deploying Your Product	187
Improve Initial Entry Performance	187
Chapter 8: Configuring Your Product	189
Implement Purge Move Request	189
Implement Security Event Exit	189
Implement MSL Exits.....	190
Implement External Security Rules	190
CA PanAPT Activity Access	190
CA PanAPT/UIF Security	196
Chapter 9: Conversion	197
Conversion Procedures	198
Conversion Checklist	198
Determine CA PanAPT Customizations	200
Install CA PanAPT	200
Reimplement Customization Into CA PanAPT	201
Make Source Changes	201
Update User Exits	202
Update Security Package.....	202
Update Scheduling Package	203
Complete System Modifications	203
Symbolic Parameters	203
Convert Database.....	203
Tailor CABYJCL Member #PJCNDDB	204
Tailor CABYJCL Member #PJJBLDB	204
Verify Conversion	204
Complete Conversion	205
Shut Down the Current CAPanAPT System	205
Convert History	206
Tailor CABYJCL Member #PJJCHS1	206
Tailor CABYJCL Member #PJJCHS2	206
Verify Conversion	207
Complete Testing with Test Move Requests	207
Conversion Cleanup	207
Clean Up Test Data	208

Back Up New CA PanAPT VSAM File to GDGs	208
Back Up New CA PanAPT VSAM File to GDGs	208
Clean Up Scheduling and Security Packages	208
Clean Up Old System	209
Appendix A: CA PanAPT DB2 Option	211
Receiving the SMP/E Package	211
How to Install Products Using Native SMP/E JCL	211
Prepare the SMP/E Environment for Pax Installation	212
Run the Installation Jobs for a Pax Installation	213
Clean Up the USS Directory	213
Apply Maintenance	215
Hold Data	216
Review DB2 Setup JCL	217
Grant Authority	218
Create VIEWLIB(VIEWS)	219
Modify DB2 Setup JCL	222
Review Setup Job Results	222
Update Your Security System	222
Run the CA PanAPT DB2 Option Enable Program	222
Index	223

Chapter 1: Overview

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

This section contains the following topics:

[Audience](#) (see page 13)

[How the Installation Process Works](#) (see page 14)

[CA PanAPT Options](#) (see page 15)

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

How the Installation Process Works

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

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

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

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

To install your product, do the following tasks:

1. Prepare for the installation by [confirming that your site meets all installation requirements](#) (see page 17).
2. Acquire the product using one of the following methods:
 - CA MSM
 - Pax-Enhanced Electronic Software Delivery (ESD)
 - Order a DVD.
3. Install the product based on your acquisition method.
4. Install the CA Common Services using the pax files that contain the CA Common Services you need at your site.

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

CA PanAPT Options

The DB2 option of CA PanAPT automates the DB2 production turnover process. This option shows DBRM and plan associations, eliminates time stamp errors, preserves DBA changes, and shows invalid plans and packages. The DB2 option decreases errors, which saves database administrators' and programmers' time.

The following guides are useful for related concepts or assumed terminology:

- *CA Panvalet Reference Guide*—Operating instructions for this library system product.
- *CA ACF2 Administrator Guide*—Command reference guide.
- *CA Telon Programming Concepts Guide*—Programming instructions for this application development tool.
- *CA Top Secret Command Functions Guide*—Command reference guide, including security administration panels.
- *CA PanExec Reference Guide*—Operating instructions for this program management product.

The IBM *z/OS JCL Reference Guide* is not produced by CA but is referenced in this publication or is recommend reading.

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:

[System Requirements](#) (see page 17)

[Software Requirements](#) (see page 17)

[CA Common Services for z/OS](#) (see page 18)

[Security Requirements](#) (see page 18)

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

System Requirements

The following is a description of the system requirements for installing and operating the CA PanAPT product:

- z/OS Version 1, or higher, and the corresponding version of:
 - Data Facility Product (DFP)
 - SMP/E
 - LE/390 COBOL Compiler
- IBM TSO/ISPF Version 2.3 (or higher) (V2R3M0, 2.3.0).
- Standard VSAM KSDS and standard PDS system files. Use VSAM share options (4,3).
- Printers able to print uppercase and lowercase or able to FOLD lowercase to uppercase. If your printer prints only uppercase, your systems programmer can specify that the printer replace lowercase letters with the uppercase equivalent. Your job entry subsystem controls FOLD processing when it loads the printer Universal Character Set (UCS) buffer. See the discussion of UCS images on SYS1.IMAGELIB in IBM publications.

Software Requirements

The following are the system requirements for installing and operating the CA PanAPT product:

- CA Panvalet r14.5 (or higher) is required for CA Panvalet moves.
- CA Librarian r4.3 or higher is required for CA Librarian moves.
- CA Panexec 5.3 PTF 1005604 is required for the APAS0223 member existence exit.

- CA PFF r1.1 or higher for CA PFF support.
- TSOE r2.1 for the REXX CA Panvalet Move Procedures (APJP5423).

CA Common Services for z/OS

CA PanAPT uses the CAIRIM component of CA Common Services for z/OS. This component must be installed for CA PanAPT to function. CA Common Services for z/OS is part of a separate installation and is not included with this installation procedure.

CA PanAPT uses the CAIRIM component (CS91000) for z/OS. CAIRIM is the common driver for a collection of dynamic initialization routines that eliminate the need for user SVCs, SMF exits, and other installation requirements commonly encountered when installing systems software. These routines are grouped under the Computer Associate z/OS Dynamic Initialization component, S910.

Security Requirements

This section describes requirements for updating your security system to authorize data set access to CA PanAPT users. In addition, if you plan to use an external security system, this section includes steps on how to update your security system to allow access for standard CA PanAPT security checks.

Data Set Authorization

All data sets created so far should be regarded as protected production data sets with the exception of the database and history files. Update your security system to the appropriate access for your site.

Because the CA PanAPT built-in security protects data in the database and the history files, set your security system to grant update authority to these files for anyone who needs to use CA PanAPT. CA PanAPT users must be able to read from and write to these data sets.

Give system administrators update authority for the following data sets:

Data Set Name	Description
<i>prefix</i> .APTDB	Database
<i>prefix</i> .APTHIST	History file
<i>prefix</i> .CABYDATA	Model library

The prefix is the prefix specified at your site by the individual who installed CA PanAPT.

External Security Setup

CA PanAPT issues external security calls for just about every function and action related to CA PanAPT functionality. CA PanAPT uses the CA Standard Security Facility (CAISSF), which is a standardized security interface to CA ACF2, CA Top Secret for z/OS, and RACF. The CA PanAPT User Identification Facility (UIF) also interfaces with external security.

All security rules are in DSN format so that the rules built by CA PanAPT are the same regardless of the security package you are running.

To use the external security interface

1. Define PANAPT as a resource class to your security system.
2. Use the high-level ownership for CA Top Secret or the key for CA ACF2 as follows:
 - PANAPTF for CA PanAPT functionality
 - PANAPTU for CA PanAPT/UIF functionality

If your security package requires access rules, you must update your security system to allow access for the following security checks:

- Require a CA PanAPT/UIF logon system ID to access CA PanAPT. The CAISSF rule is:

PANAPTU.PANAPT

- Authorize the system ID entered or that was selected from an MSL. The CAISSF rule is:

PANAPTU.PANSYSID.*system-id*

- Authorize CA PanAPT/UIF usage to create or change logon system IDs. The CAISSF rule is:

PANAPTU.PANUIF

- Allow CA PanAPT activities for authorized system ID. The CAISSF rule is:

PANAPTF.*system-id*.xxxxxxx.xxxxxxx.xxxxxxx

See CA ACF2 Example, which allows access to all users and all activities.

Storage Requirements

The following table shows a list of the storage requirements for the various components of the CA PanAPT product:

Product Component	Storage Requirements
Delivered software libraries	60 cylinders of 3380 space
Control and processing files	15 cylinders of 3380 space
TSO address space	2048 KB
Maximum batch region	4096 KB

The installation job creates two CA PanAPT VSAM files in addition to the three CA PanAPT VSAM files that are on the installation tape. They are:

- The Startup Inventory File, with a space requirement of CYL, (3,3).
- The Startup Pending File Alternate Index with a space requirement of TRK, (14,3).

The installation job can optionally create another CA PanAPT VSAM file (the Startup History File) that has a space requirement of CYL,(3,1).

Chapter 3: Installing Your Product Using CA MSM

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

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

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

This section contains the following topics:

[CA MSM Documentation](#) (see page 21)

[Getting Started Using CA MSM](#) (see page 22)

[Acquiring Products](#) (see page 32)

[Installing Products](#) (see page 37)

[Maintaining Products](#) (see page 44)

[Setting System Registry](#) (see page 58)

[Deploying Products](#) (see page 83)

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

CA MSM Documentation

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

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

Getting Started Using CA MSM

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

How to Use CA MSM: Scenarios

In the scenarios that follow, imagine that your organization recently deployed CA MSM to simplify the installation of CA Technologies products and unify their management. You have also licensed a new CA Technologies product. In addition, you have a number of existing CSIs from previously installed products.

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

How to Acquire a Product

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

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

Follow these steps:

1. Set up a CA Support Online account.

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

2. Determine the CA MSM URL for your site.

To [access CA MSM](#) (see page 31), you require its URL. You can get the URL from your site's CA MSM administrator and log in using your z/OS credentials. When you log in for the first time, you are prompted to create a CA MSM account with your credentials for [the CA Support Online website](#). This account enables you to download product packages.

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

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

If you cannot find the product you want to acquire, [update the catalog](#) (see page 32). CA MSM refreshes the catalog through [the CA Support Online website](#) using the site IDs associated with your credentials for [the CA Support Online website](#).

4. [Download the product installation packages](#) (see page 33).

After you find your product in the catalog, you can [download the product installation packages](#) (see page 33).

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

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

How to Deploy a Product

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

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

Follow these steps:

1. Set up the system registry:
 - a. Determine the systems you have at your enterprise.
 - b. Set up [remote credentials](#) (see page 81) for those systems.
 - c. Set up the target systems ([Non-Sysplex](#) (see page 59), [Sysplex or Monoplex](#) (see page 60), [Shared DASD Cluster](#) (see page 61), and [Staging](#) (see page 62)), and validate them.
 - d. [Add FTP](#) (see page 71) information, including data destination information, to each system registry entry.
2. Set up [methodologies](#) (see page 109).

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

After creating the deployment, you can save it and change it later by adding and editing [systems](#) (see page 126), [products](#) (see page 100), [custom data sets](#) (see page 102), and [methodologies](#) (see page 109), or you can deploy directly from the wizard.

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

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

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

System Registration

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

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

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

1. Set up your remote credentials.

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

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

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

2. Set up your system registry.

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

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

Non-Sysplex Systems

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

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

Sysplex or Monoplex Systems

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

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

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

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

Shared DASD Clusters

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

Staging Systems

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

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

3. Define the FTP location information for every system.

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

To define the FTP location, provide the following:

URI

Specifies the host system name.

Port Number

Specifies the port number.

Default: 21.

Directory Path

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

4. Define a data destination for every system.

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

FTP

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

Shared DASD

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

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

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

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

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

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

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

5. Register each system by validating that it exists.

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

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

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

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

You are now ready to deploy your products.

Deploying Products

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

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

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

Deployment Name and Description

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

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

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

CSI Selection

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

Product Selection

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

Custom Data Set

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

- For a z/OS data set, you need to provide a data set name that is the actual existing z/OS data set and a mask that names the data set on the target system. This mask may be set up using [symbolic qualifiers](#) (see page 113) 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 113) 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 103).

Methodology

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

To [create a methodology](#) (see page 110), specify the following:

Data set name mask

Lets you choose symbolic variables that get resolved during deployment.

Disposition of the target data sets

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

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

Partitioned data set

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

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

Directory in a UNIX file system

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

Sequential data set or a file in the UNIX file system

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

For a VSAM data set (cluster)

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

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

System Selection

Select the system for this deployment.

Preview

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

Use this option to review your deployment before deploying.

Deploy

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

Summary

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

Confirm

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

How to Maintain Existing Products

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

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

Follow these steps:

1. Migrate the CSI to CA MSM to maintain an existing CSI in CA MSM.
During the migration, CA MSM stores information about the CSI in the database.
2. [Download the latest maintenance](#) (see page 45) 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 46).
3. [Apply the maintenance](#) (see page 49).

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

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

Access CA MSM Using the Web-Based Interface

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

Follow these steps:

1. Start your web browser, and enter the access URL.
The login page appears.
Note: If the Notice and Consent Banner appears, read and confirm the provided information.
2. Enter your z/OS login user name and password, and click the Log in button.
The initial page appears. If you log in for the first time, you are prompted to define your account on [the CA Support Online website](#).
Note: For more information about the interface, click the online help link at the top right corner of the page.

3. Click New.

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

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

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

You are prompted to review your user settings.

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

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

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

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

Acquiring Products

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

Update Software Catalog

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

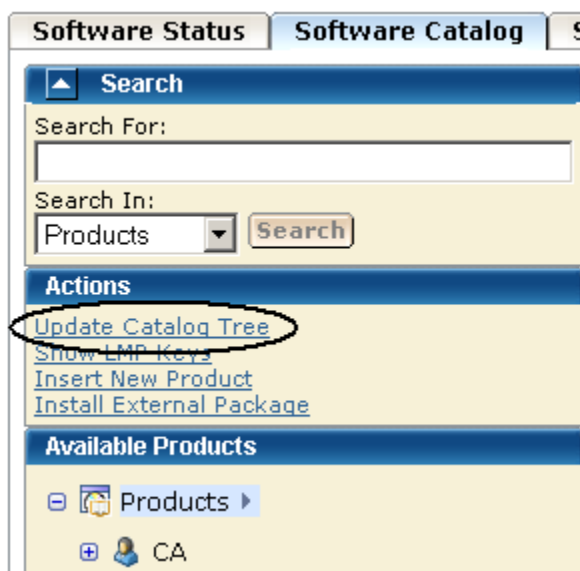
If you update the catalog tree and some changes are missing, check your user settings on [the CA Support Online website](#).

Follow these steps:

1. Click the Software Catalog tab.

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

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



You are prompted to confirm the update.

3. Click OK.

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

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

Download Product Installation Package

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

Follow these steps:

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

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

The product releases are listed.

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

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

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

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

The product packages are downloaded.

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

Migrate Installation Packages Downloaded External to CA MSM

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

Migrating these packages to CA MSM provides a complete view of all your product releases. After a package is migrated, you can use CA MSM to [install the product](#) (see page 37).

Follow these steps:

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

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

An entry is added for the product.

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

The packages for the gen level are listed.

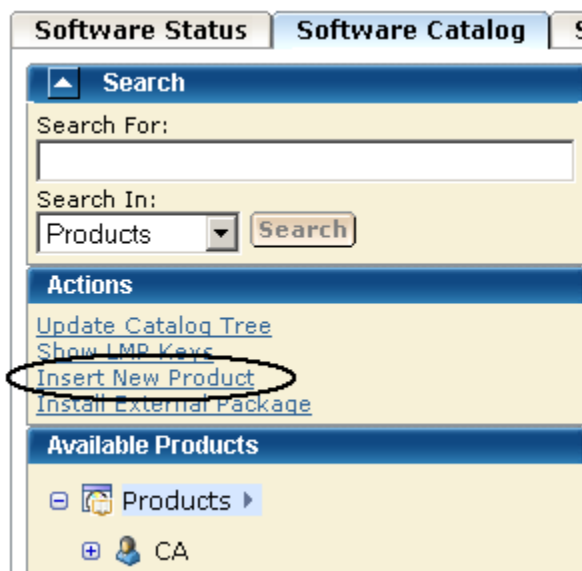
3. Click the Add External Package button.
You are prompted to enter a path for the package.
4. Specify the USS path to the package you want to migrate, and click OK.
Information about the package is saved in the CA MSM database.
Note: To see the added package, refresh the page.

Add a Product

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

Follow these steps:

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



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

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

Note: To add several packages from the same location, use [masking](#) (see page 36).

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

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

Masking for External Packages

Masking lets you add more than one [package](#) (see page 35) (or set of [maintenance files](#) (see page 47)) from the same location using a pattern (mask). You can use masking for components, maintenance in USS, and maintenance in data sets. You can use masking for files only, not for directories.

Masking: Use the asterisk symbol (*).

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

- For sequential data sets, use the following characters:

?

Match on a single character.

*

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

**

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

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

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

Example 1

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

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

Example 2

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

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

Example 3

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

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

Example 4

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

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

Installing Products

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

Install a Product

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

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

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

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

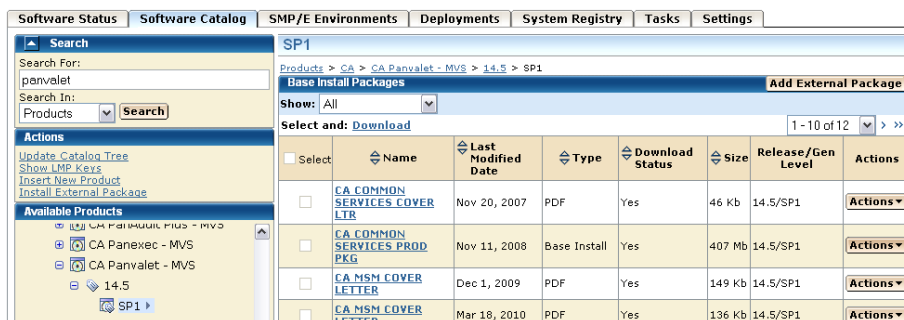
During installation, you select the CSI where the product is to be installed, and specify its zones. You can either specify target and distribution zones to be in the existing CSI data sets, or create new data sets for each zone.

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

Follow these steps:

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

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



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

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

The Introduction tab of the wizard appears.

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

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

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

You are prompted to select the type of installation.

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

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

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

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

- If no prerequisites exist, click Next.

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

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

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

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

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

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

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

If you select Create a New SMP/E CSI, you are prompted to [specify the CSI parameters](#) (see page 40).

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

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

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

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

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

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

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

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

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

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

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

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

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

9. Review the summary, and click Install.

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

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

Create a CSI

You can create a CSI while you are [installing a product](#) (see page 37). During the process, you are asked to specify the following:

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

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

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

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

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

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

Follow these steps:

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

You are prompted to define a CSI.
2. Specify the following, and click Next:

Name

Defines the name for the environment represented by the CSI.

Data Set Name Prefix

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

Catalog

Defines the name of the SMP/E CSI catalog.

Cross-Region

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

Cross-System

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

High-Level Qualifier

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

DSN Type

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

SMS Parameters / Data Set Parameters

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

Storage Class (SMS Parameters only)

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

Management Class (SMS Parameters only)

Defines the management class for SMP/E data sets.

Data Class (SMS Parameters only)

Defines the data class for SMP/E data sets.

VOLSER (Data Set Parameters only)

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

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

Unit (Data Set Parameters only)

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

Catalog (Data Set Parameters only)

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

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

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

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

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

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

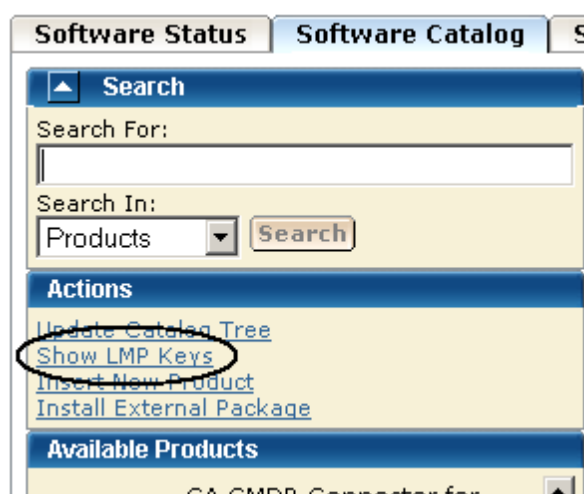
You are prompted to specify any additional parameters. A new CSI is specified.

Download LMP Keys

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

Follow these steps:

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



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

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

The list is refreshed for the selected site ID.

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

3. Click Update Keys.

You are prompted to confirm the update.

4. Click OK.

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

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

Maintaining Products

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

How to Apply Maintenance Packages

Use this process to download and apply product maintenance packages.

1. Identify your download method. This section details the steps to use the following download methods:
 - [Download Product Maintenance Packages](#) (see page 45)
 - [Download Product Maintenance Packages for Old Product Releases and Service Packs](#) (see page 46)
 - [Manage Maintenance Downloaded External to CA MSM](#) (see page 47)

Contact your system administrator, if necessary.

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

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

Download Product Maintenance Packages

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

Follow these steps:

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

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

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

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

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

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

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

The maintenance packages are downloaded.

More information:

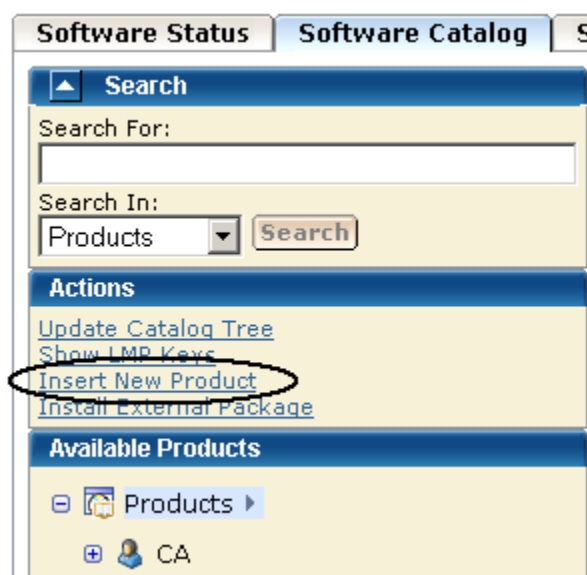
[Download Maintenance Packages for Old Product Releases and Service Packs](#) (see page 46)

Download Maintenance Packages for Old Product Releases and Service Packs

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

Follow these steps:

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



You are prompted to supply information about the product release.

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

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

The product release is added to the software catalog.

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

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

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

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

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

Manage Maintenance Downloaded External to CA MSM

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

Adding these maintenance packages to CA MSM provides you with a complete view of all the maintenance for a product release. After a package is migrated, you can use CA MSM to [apply the maintenance](#) (see page 49).

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

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

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

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

Follow these steps:

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

The maintenance packages for the release are listed.

2. Click the Add External Maintenance button.

You are prompted to specify the package type and location.

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

Note: To add several packages from the same location, use [masking](#) (see page 36).

4. Click OK.

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

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

More information:

[Manage Maintenance](#) (see page 49)

View Aggregated Package Details

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

Follow these steps:

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

The maintenance packages for the release are listed.

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

The Maintenance Package Details dialog opens.

3. Click the Nested Packages tab.

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

Manage Maintenance

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

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

The following installation modes are available:

Receive and Apply

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

Receive and Apply Check

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

Receive, Apply Check, and Apply

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

Receive Only

Receives the maintenance.

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

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

Follow these steps:

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

The maintenance information is updated.

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

The maintenance packages are listed, for example:

Software Status

Software Catalog

SMP/E Environments

Deployments

System Registry

Tasks

Settings

Search

Search For:

Search In:

Products

Search

Actions

Update Catalog Tree

Show LMP Keys

Insert New Product

Install External Package

Available Products

CA Panvalet - MVS

14.4

14.5

SP1

CA Panvalet Option for ISPF - MVS

CA Panvalet Option for TSO - MVS

CA Partition Expert for DB2 for z/OS - MVS

CA PDSMAN PDS Library Management ALL 5 COMPONENTS - MVS

CA PDSMAN PDS Library Management All Extensions and Performance - MVS

14.5

Products > CA > CA Panvalet - MVS > 14.5

Maintenance Packages

Add External Maintenance

Refresh

Show: All

All for current release

All source IDs

Select and: Install

1 - 10 of 70

>

>>

Select	Fix #	Description	Confirmed Date	Type	Installed	Actions
<input type="checkbox"/>	Q085668	* PRODUCT DOCUMENTATION CHANGE	Jan 29, 2007	PEA/PDC	Not installable	Actions
<input type="checkbox"/>	Q089243	* PRODUCT ERROR ALERT *	Jun 20, 2007	PEA/PDC	Not installable	Actions
<input type="checkbox"/>	R012055	0607: MSM INST. ADD SUPPORT FOR SAMPJCL UNDER SMP/E	Oct 7, 2009	PTF	No (0/1)	Actions
<input type="checkbox"/>	Q088250	14.5 SP00 : PAN0/PAN#1 INPUT STREAM INVALID COMMAND	May 11, 2007	PTF	No (0/1)	Actions
<input type="checkbox"/>	Q088259	14.5 SP01 : PAN0/PAN#1 INPUT STREAM INVALID COMMAND	May 11, 2007	PTF	No (0/1)	Actions
<input type="checkbox"/>	Q086490	14.5-SP00 : DOING ++WRITE, LNG FMT CHANGED AFTER	Mar 6, 2007	PTF	No (0/1)	Actions
<input type="checkbox"/>	Q090975	14.5-SP00/SP01: PAM DIRECTORY AVERAGE BYTES	Sep 4, 2007	PTF	No (0/1)	Actions
<input type="checkbox"/>	Q081764	14.5-SP00: PAN#1 ++CONTROL WITH NO CODE GIVES ERROR	Aug 25, 2006	PTF	No (0/1)	Actions
<input type="checkbox"/>	Q081765	14.5-SP00: PV071 DOING ++SCANS OF ZTYPE1-8 MEMBERS	Aug 25, 2006	PTF	No (0/1)	Actions
<input type="checkbox"/>	Q086868	14.5-SP00: ZTYPE7 NOT FORMATTED CORRECTLY ON TSO	Mar 19, 2007	PTF	No (0/1)	Actions

Red asterisks identify HIPER maintenance packages.

- Click the Fix # link for each maintenance package you want to install.
The Maintenance Package Details dialog appears, identifying any prerequisites.
- Review the information on this dialog, and click Close to return to the Maintenance Packages section.
- Select the maintenance packages you want to install, and click the Install link.
Note: The Installed column indicates whether a package is installed.
The Introduction tab of the wizard appears.
- Review the information about the maintenance, and click Next.
The packages to install are listed.
- Review and adjust the list selections as required, and click Next.
The SMP/E environments that contain the product to maintain are listed. Only environments in your working set are listed.
- Select the environments in which you want to install the packages.
- Click Select Zones to review and adjust the zones where the maintenance will be installed, click OK to confirm the selection and return to the wizard, and click Next.

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

11. Select the installation mode for the selected maintenance, and click Next.

- If prerequisites exist and are available, review them and click Next. CA MSM installs these prerequisites as part of the process. If a prerequisite is *not* available, the wizard cannot continue. You must acquire the prerequisite and restart the process.
- If [HOLDDATA](#) (see page 151) entries exist, review and select them, and click Next.

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

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

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

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

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

A pop-up window opens.

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

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

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

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

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

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

14. Click Next.

A summary of the task appears.

15. Review the summary, and click Install.

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

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

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

More information:

[Download Product Maintenance Packages](#) (see page 45)

[Download Maintenance Packages for Old Product Releases and Service Packs](#) (see page 46)

View Installation Status of Maintenance Package

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

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

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

Follow these steps:

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

The maintenance packages for the release are listed.

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

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

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

USERMODs

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

You can create a USERMOD manually, or we can provide an unpublished maintenance package as a USERMOD. In this case, the USERMOD file, which contains the ++USERMOD statement and the body of the USERMOD, must be [managed as an externally downloaded package](#) (see page 47).

GROUPEXTEND Mode

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

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

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

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

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

Apply Check

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

Apply

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

Apply Check and Apply

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

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

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

- Accept Check
- Accept
- Accept Check and Accept

How Maintenance in GROUPEXTEND Mode Works

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

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

The followings options are available for bypassing HOLDDATA:

- HOLDSYSTEM
- HOLDCLASS
- HOLDERROR
- HOLDUSER

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

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

Manage Maintenance in GROUPEXTEND Mode

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

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

Follow these steps:

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

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

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

2. Click the Maintenance link.

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

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

The Introduction tab of the wizard appears.

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

The packages that you want to apply are listed.

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

5. Review the packages, and click Next.

The Prerequisites tab of the wizard appears.

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

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

Installation options appear.

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

NOAPARS

Excludes APARs that resolve error reason ID.

NOUSERMODS

Exclude USERMODs that resolve error user ID.

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

The Bypass HOLDDATA tab of the wizard appears.

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

9. Click Next.

A summary of the task appears.

10. Review the summary, and click Apply GROUPEXTEND.

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

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

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

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

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

Back Out Maintenance

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

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

Follow these steps:

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

Products installed in the environment are listed.

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

The features in the component are listed.

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

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

The maintenance packages for the feature are listed.

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

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

The maintenance wizard opens to the Introduction step.

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

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

The packages to back out are listed.

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

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

The Prerequisite tab of the wizard appears.

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

A summary of the task appears.

8. Review the summary, and click Restore.

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

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

Setting System Registry

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

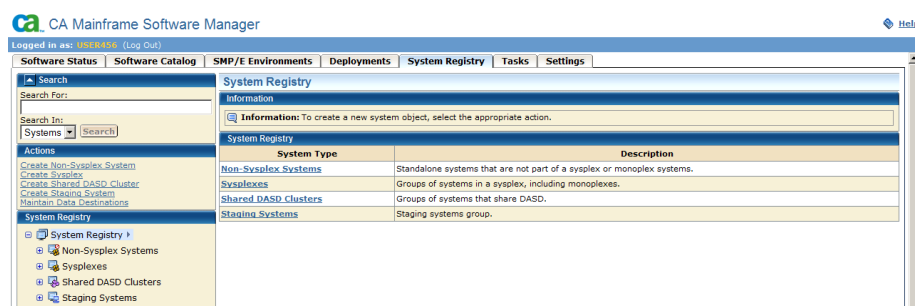
View a System Registry

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

Follow these steps:

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

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

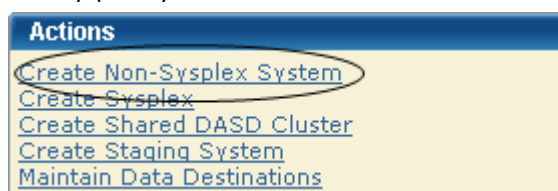


Create a Non-sysplex System

You can create a non-sysplex system registry.

Follow these steps:

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



The New Non-Sysplex System dialog appears.

Note: The asterisk indicates that the field is mandatory.

2. Enter the following information, and click Save:

Name

Enter the non-sysplex system name.

Limits: Eight characters

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

Description

Enter the description.

Limits: 255 characters

CCI System ID

(Optional) Enter the CAICCI system ID.

Limits: Eight characters

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

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

Note: To withdraw this create request, click Cancel.

3. Detail the nonstaging system.

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

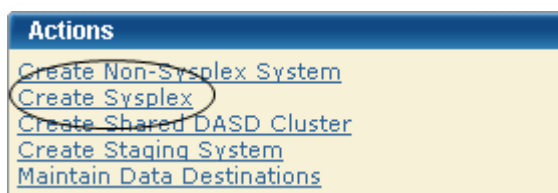
Property Name: z/OS LPAR Name, Value: ** Not Applicable **.

Create a Sysplex or Monoplex

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

Follow these steps:

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



The New Sysplex dialog appears.

Note: The asterisk indicates that the field is mandatory.

2. Enter the following and click Save.

Name

Enter the sysplex system name.

Limits: Eight characters

Description

Enter the description.

Limits: 255 characters

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

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

Note: Click Cancel to withdraw this create request.

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

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

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

- Enter the following data items for each system:

Name

Enter the sysplex system name.

Limits: Eight characters

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

Description

Enter the description.

Limits: 255 characters

CCI System ID

(Optional) Enter the CAICCI system ID.

Limits: Eight characters

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

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

Note: To withdraw this create request, click Cancel.

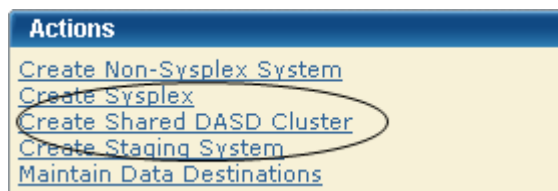
- Detail the nonstaging system.

Create a Shared DASD Cluster

You can create a shared DASD cluster.

Follow these steps:

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



The New Shared DASD Cluster dialog appears.

Note: The asterisk indicates that the field is mandatory.

2. Enter the following information, and click Save:

Name

Enter the shared DASD cluster name.

Limits: Eight characters

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

Description

Enter the description.

Limits: 255 characters

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

Note: Click Cancel to withdraw this create request.

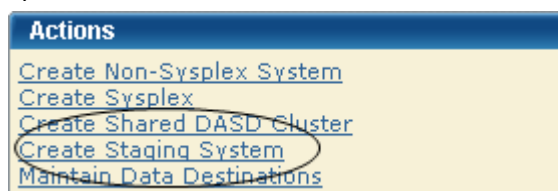
3. Right-click the newly added DASD cluster name and select Add System or Sysplex to this Shared DASD Cluster. Select the systems or sysplexes that you want to add to the DASD cluster.

Create a Staging System

You can create a staging system.

Follow these steps:

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



The New Staging System dialog appears.

Note: The asterisk indicates that the field is mandatory.

2. Enter the following information, and click Save:

Name

Enter the staging system name.

Limits: Eight characters

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

Description

Enter the description.

Limits: 255 characters

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

Note: Click Cancel to withdraw this create request.

Authorization

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

Edit Mode

Lets you update and change system registry information.

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

View Mode

Lets you view system registry information.

Note: You cannot edit information in this mode.

Change a System Registry

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

Follow these steps:

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

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

2. Select the system to change.

Detailed information about the system appears on the right side.

3. Update the following information as needed. The information that you update is dependent on whether you are changing a [Non-Sysplex System](#) (see page 59), [Sysplex](#) (see page 60), [Shared DASD Cluster](#) (see page 61), or [Staging System](#) (see page 62).

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

- For Shared DASD or sysplex system only, select the [contact system](#) (see page 69), which is the system where the Shared DASD or FTP is located. The FTP location should be set to the contact system URI. The contact system is used for remote credentials.

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

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

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

- For Staging systems, enter the GIMUNZIP volume and/or [zFS candidate volumes](#) (see page 70).

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

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

Cancel

Cancel this maintenance.

Save

Save the changes to this maintenance.

Validate

Validate authenticates this entry.

Note: The validation process is done in steps; each system in this request is validated with the last step summarizing, verifying, and confirming the validation. If the validation fails this step shows how the validation failed. You can [investigate the failed validation](#) (see page 67).

Validation Rules

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

Note: A Staging system is not validated.

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

The following are the system validation results:

Validated

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

Validation in Progress

Indicates that the system status is updated to in progress.

Validation Error

Indicates that the system status is updated to error, and you can [investigate the failed validation](#) (see page 67).

Not Validated

Indicates that this system has not been validated yet.

Not Accessible

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

Validation Conflict

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

Error Details

When there is a validation conflict, the Error details button appears. Click this button to find the reason for this conflict. You can [investigate the failed validation](#) (see page 67).

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

Conflict Details

When a validation is in conflict, the Error details button appears. Click this button to find the reason for this conflict. You can [investigate the failed validation](#) (see page 67).

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

Failed Validations

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

- [Investigate a Failed Validation using the Tasks Page](#) (see page 67)
- [Investigate a Failed Validation Immediately After a Validation](#) (see page 68)
- [Download a Message Log](#) (see page 68)
- [Save a Message Log as a Data Set](#) (see page 69)
- [View Complete Message Log](#) (see page 69)

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

Investigate a Failed Validation Using Task Output Browser

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

Follow these steps:

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

The screenshot shows the 'Task History' window with a search bar at the top. Below the search bar, there are filters for 'Show: USER456', 'All types', and 'All status'. A table lists tasks with columns: Owner, Name, Type, Status, Start Time, Stop Time, and Task ID. One task is highlighted: Owner: USER456, Name: [Validating System: XX60](#), Type: System Registry, Status: Failed (indicated by a red X icon), Start Time: 1/12/2010 02:26:01PM, Stop Time: 1/12/2010 02:26:09PM, Task ID: 432.

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

The Validate System Task Output Browser appears.

The screenshot shows the 'Validate System: XX60' window. It has a 'Search' section on the left and a main area with 'General' and 'Steps' tabs. The 'General' tab shows details: Name: Validate System: XX60, Task ID: 447, User ID: USER456, Status: Failed, Status Message: Failed to undo command. The 'Steps' tab shows a list of steps with columns: #, Name, Description, and Status.

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

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

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

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

7. Correct the issue and validate again.

Investigate a Failed Validation After Validation

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

Follow these steps:

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

The validation results appear.

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

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

7. Correct the issue and validate again.

Download a Message Log

You can save the message log in the following ways:

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

Save a Message Log as a Data Set

You can save a message log as a data set.

Follow these steps:

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

The Save Output as Data Set dialog appears.

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

Note: The asterisk indicates that the field is mandatory.

2. Enter the following information and click OK:

Data Set Name

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

VOLSER

For non-SMS data, enter the Volser.

Example:

Volser: SYSP01 and SYSP02

Storage Class

For SMS Allocation data, enter the Storage Class.

The message log is saved as a data set.

View Complete Message Log

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

Note: To close the message log, click Close.

Contact System

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

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

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

zFS Candidate Volumes

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

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

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

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

Note: Remote system requirement is customer defined.

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

CA Allocate

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

CA Disk Backup and Restore

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

You can also use the following standard IBM techniques:

- Allocation exits
- ACS routines

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

Maintain a System Registry using the List Option

Follow these steps:

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

Delete a System Registry

Follow these steps:

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

The system list appears.

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

The system is deleted.

FTP Locations

The [FTP](#) (see page 71) Locations lists the current FTP locations for this system. You can [add](#) (see page 71), [edit](#) (see page 73), [set default](#) (see page 74), or [remove](#) (see page 74) [FTP](#) (see page 71) locations.

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

Deployment FTP Locations

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

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

Add FTP Locations

You can add [FTP](#) (see page 71) locations.

Follow these steps:

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

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

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

Detailed information about the system appears on the right side.

3. Click the FTP Locations tab.

The FTP Locations window appears.

4. Click Add.

The New FTP Location dialog appears.

Note: The asterisk indicates that the field is mandatory.

5. Enter the following information, and click Save:

URI

Enter the URI.

Limits: Maximum length is 255.

Port

Enter the Port.

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

Default: 21

Directory Path

Enter the Directory Path.

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

The new FTP location appears on the list.

Note: Click Cancel to withdraw this create request.

More information:

[Edit FTP Locations](#) (see page 73)

[Delete FTP Locations](#) (see page 74)

[Set FTP Location Default](#) (see page 74)

Edit FTP Locations

You can edit [FTP](#) (see page 71) locations.

Note: The asterisk indicates that the field is mandatory.

Follow these steps:

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

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

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

Detailed information about the system appears on the right side.

3. Click the FTP Location tab.

The FTP Locations window appears.

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

The Edit FTP Location dialog appears.

5. Update the following and click Save:

URI

Enter the URI.

Limits: Maximum length is 255.

Port

Enter the Port.

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

Default: 21

Directory Path

Enter the Directory Path.

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

Your changes are saved.

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

Set FTP Location Default

You can set an [FTP](#) (see page 71) location default.

Follow these steps:

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

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

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

Detailed information about the system appears on the right side.

3. Click the FTP Locations tab.

The FTP Locations window appears.

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

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

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

Delete FTP Locations

You can delete [FTP](#) (see page 71) locations.

Follow these steps:

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

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

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

Detailed information about the system appears on the right side.

3. Click the FTP Locations tab.

The FTP Locations window appears.

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

The FTP location is deleted from this system.

Data Destinations

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

FTP

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

Shared DASD

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

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

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

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

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

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

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

Create Data Destinations

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

Follow these steps:

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

The Maintains Data Destinations dialog appears.

2. Click Create.

The New Data Destination dialog appears.

Note: The asterisk indicates that the field is mandatory.

3. Enter the following information, and click Save:

Name

Enter a meaningful name.

Limits: Maximum 64 characters.

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

Description

Enter the description.

Limits: Maximum 255 characters.

Transmission Method

Select the transmission method.

Default: Shared DASD.

Mount Point

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

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

Limits: Maximum 120 characters

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

Storage Class

(Shared DASD only) Enter the Storage Class.

Limits: Maximum 8 characters

Example: SYSPRG

VOLSER

(Shared DASD only) Enter the Volser.

Limits: Maximum 6 characters

Example: SYSP01 and SYSP02

GIMUNZIP Volume

Enter the GIMUNZIP volume.

Limits: Maximum 6 characters

zFS Candidate Volumes

Enter [zFS Candidate volumes](#) (see page 70).

Limits: Maximum 6 characters

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

The new data destination appears on the Data Destination list.

Note: Click Cancel to withdraw this create request.

Add a Data Destination

You can add current data destinations to an existing system.

Follow these steps:

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

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

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

Detailed information about the system appears on the right side.

3. Click the Data Destination tab.

The Data Destination window appears.

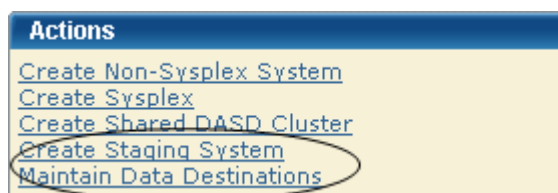
4. Click Add.
The Pick Data Destination dialog appears.
5. Select the data destinations you want to add and click Select.
The data destinations are added to the system.

Maintain Data Destinations

You can maintain, [delete](#) (see page 80), or [create](#) (see page 76) data destinations.

Follow these steps:

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



The Maintains Data Destinations dialog appears.

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

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

The Edit Data Destinations dialog appears.

Note: The asterisk indicates that the field is mandatory.

3. Update the following and click Save:

Name

Enter a meaningful Name.

Limits: Maximum 64 characters.

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

Description

Enter the description.

Limits: Maximum 255 characters.

Transmission Method

Select the transmission method.

Default: Shared DASD.

Mount Point

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

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

Limits: Maximum 120 characters

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

Storage Class

(Shared DASD only) Enter the Storage Class.

Limits: Maximum 8 characters

Example: SYSPRG

VOLSER

(Shared DASD only) Enter the Volser.

Limits: Maximum 6 characters

Example: SYSP01 and SYSP02

GIMUNZIP Volume

Enter the GIMUNZIP volume.

Limits: Maximum 6 characters

zFS Candidate Volumes

Enter [zFS Candidate volumes](#) (see page 70).

Limits: Maximum 6 characters

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

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

Note: Click Cancel to withdraw this change request.

Set a Default Data Destination

You can set a default for a current data destination.

Follow these steps:

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

Delete Data Destinations

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

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

Follow these steps:

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

Remote Credentials

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

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

You can [add](#) (see page 81), [edit](#) (see page 82), or [delete](#) (see page 83) remote credentials.

Add Remote Credentials

Follow these steps:

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

Note: The asterisk indicates that the field is mandatory.

Remote User ID

Enter a correct remote user ID.

Limits: 64 characters

Remote System Name

Enter a remote system name.

Limits: Eight characters

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

Password

Enter a correct password.

Limits: 2 to 63 characters

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

Confirm Password

Enter the correct confirm password.

Limits: 2 to 63 characters

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

The remote credential entry appears on the Remote Credentials list.

4. Click Apply.

Your changes are applied.

Edit Remote Credentials

You can edit remote credentials.

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

Follow these steps:

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

Note: The asterisk indicates that the field is mandatory.

Remote User ID

Enter a correct remote user ID.

Limits: Maximum 64 characters.

Remote System Name

Enter a correct remote system name.

Limits: Maximum 8 characters.

Example: RMinPlex

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

Password

Enter a correct password.

Limits: Minimum 2 characters and Maximum 63 characters.

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

Confirm Password

Enter the correct confirm password.

Limits: Minimum 2 characters and Maximum 63 characters.

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

The remote credential entry appears on Remote Credentials list.

4. Click Apply

Your changes are applied.

Delete Remote Credentials

You can delete remote credentials.

Follow these steps:

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

Deploying Products

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

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

Deployment Status

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

Under Construction

The user is constructing the deployment.

Available Actions: All but Confirm

Snapshot in Progress

Snapshot is in Progress

Available Actions: Reset Status

Snapshot in Error

Snapshot failed

Available Actions: All but Confirm

Snapshot Completed

Snapshot Succeeded

Available Actions: Delete, Preview, Transmit, Deploy

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

Transmitting

The deployment archives are being transmitted using the FTP procedure.

Available Actions: Reset Status

Transmission Error

Transmission Failed

Available Actions: Delete, Preview, Transmit, Deploy

Transmitted

The deployment archives have been transmitted.

Available Actions: Delete, Preview, Deploy

Deploying

The deployment archives are being deployed.

Available Actions: Reset Status

Deploying Error

Deployment failed

Available Actions: Delete, Preview, Deploy

Deployed

The target libraries were deployed.

Available Actions: Delete, Summary, Confirm

Complete

The deployment is complete.

Available Actions: Delete, Summary

Creating Deployments

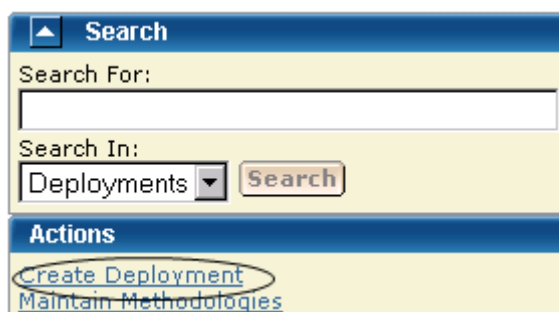
The deployment creation process consists of the following steps:

1. [Initiate deployment creation](#) (see page 86).
2. [Define a name and description](#) (see page 86).
3. [Select an SMP/E environment](#) (see page 87).
4. [Select a product](#) (see page 87).
5. [Select a custom data set](#) (see page 88).
6. [Select a methodology](#) (see page 88).
7. [Select a system](#) (see page 90).
8. [Preview and save](#) (see page 90).

Initiate Deployment Creation

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

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



The New Deployment wizard opens to the Introduction step.

Note: When creating a deployment, you can save this deployment at any step in this wizard. This "under construction" deployment is added to the current deployments list. You can [maintain this deployment](#) (see page 91) until a successful snapshot has been created.

Define Name and Description

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

Note: The asterisk indicates that the field is mandatory.

Follow these steps:

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

Limits: Maximum 64 characters.

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

2. Enter the description of this deployment.

Limits: Maximum 255 characters.

3. Click Next.

The CSI Selection step appears.

Note: When creating a deployment, you can save this deployment at any step in this wizard. This "under construction" deployment is added to the current deployments list. You can [maintain this deployment](#) (see page 91) until a successful snapshot has been created.

Select a CSI

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

Follow these steps:


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

Note: When creating a deployment, you can save this deployment at any step in this wizard. This "under construction" deployment is added to the current deployments list. You can [maintain this deployment](#) (see page 91) until a successful snapshot has been created.

Select a Product

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

Follow these steps:

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

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

The Custom Data Sets step appears.

Note: When creating a deployment, you can save this deployment at any step in this wizard. This "under construction" deployment is added to the current deployments list. You can [maintain this deployment](#) (see page 91) until a successful snapshot has been created.

Select a Custom Data Set

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

Follow these steps:

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

Note: To add a new custom data set, click Add Data Set and [enter the custom data set information](#) (see page 103).

2. Click Next.

The Methodology Selection step appears.

Note: When creating a deployment, you can save this deployment at any step in this wizard. This "under construction" deployment is added to the current deployments list. You can [maintain this deployment](#) (see page 91) until a successful snapshot has been created.

More information:

[Add a Custom Data Set](#) (see page 103)

Select a Methodology

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

Follow these steps:

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

2. (Optional) Click the Create button and [enter the new methodology information](#) (see page 110).

New Deployment

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

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

Methodologies

1 - 5 of 44

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

Create

Save Back Next Deploy Cancel Help

3. Click Next.

The System Selection step appears.

Note: When creating a deployment, you can save this deployment at any step in this wizard. This "under construction" deployment is added to the current deployments list. You can [maintain this deployment](#) (see page 91) until a successful snapshot has been created.

More information:

[Create a Methodology](#) (see page 110)

Select a System

After you select a methodology, you select a system.

Follow these steps:

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

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

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

2. Click Next.

The Preview step appears.

Note: When creating a deployment, you can save this deployment at any step in this wizard. This "under construction" deployment is added to the current deployments list. You can [maintain this deployment](#) (see page 91) until a successful snapshot has been created.

Preview and Save the Deployment

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

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

Note: Click Cancel to exit the wizard without saving.

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

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

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

View a Deployment

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

Change Deployments

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

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

Follow these steps:

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

This deployment's window appears.

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

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

[There are actions that you can perform based on Deployment State](#) (see page 84).

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

The [Edit Methodology window](#) (see page 123) appears. The Deployment ID is the value of the MSMID variable.

Note: You can perform the following actions:

- You can [select](#) (see page 100), [add](#) (see page 101), or [remove](#) (see page 101) a product.
 - You can [select](#) (see page 127), [add](#) (see page 127), or [remove](#) (see page 128) a system.
 - You can [select](#) (see page 102), [add](#) (see page 103), or [remove](#) (see page 109) a custom data set.
5. Click Save on the Deployment Details window.

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

Preview (Summary)

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

Generates a list of the following current information:

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

Snapshot

Takes a snapshot of the current deployment.

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

Transmit

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

Deploy

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

Confirm (see page 98)

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

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

Delete

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

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

[Reset Status](#) (see page 96)

You can reset a deployment status when the deployment has a status of *snapshot in progress*, *transmitting*, or *deploying*. See [reset status](#) (see page 96) for a list of deleted files.

7. Click Save on the Deployment Details window.

Your changes are saved.

More information:

[Add a Product](#) (see page 101)
[Add a System](#) (see page 127)
[Remove a Product](#) (see page 101)
[Remove a System](#) (see page 128)
[View the Product List](#) (see page 100)
[View a System List](#) (see page 127)
[Edit a Methodology](#) (see page 123)
[Confirm a Deployment](#) (see page 98)

Deployment Maintenance

You can maintain a deployment in the following ways:

- Adding
 - [System](#) (see page 127)
 - [Product](#) (see page 101)
 - [Custom data sets](#) (see page 103)
- Delete
 - Deployment
- Removing
 - [System](#) (see page 128)
 - [Product](#) (see page 101)
 - [Custom data sets](#) (see page 109)

- Editing
 - [Maintain deployments](#) (see page 91)
 - [Edit a custom data set](#) (see page 106)
 - [Edit a methodology](#) (see page 123)
- Viewing
 - [System](#) (see page 127)
 - [Product](#) (see page 100)
 - [Custom data sets](#) (see page 102)

Failed Deployments

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

- [Investigate a Failed Deployment Using the Tasks Page](#) (see page 94)
- [Download a Message Log](#) (see page 68)
- [Save a Message Log as a Data Set](#) (see page 69)
- [View Complete Message Log](#) (see page 69)

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

More information:

[Download a Message Log](#) (see page 68)

[Save a Message Log as a Data Set](#) (see page 69)

[View Complete Message Log](#) (see page 69)

Investigate a Failed Deployment

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

Follow these steps:

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

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

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

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

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

The Task Output Browser appears.

Deploy: Deployment Test Close			
<div>General Download Zipped Output</div> <div> Name: Deploy: Deployment Test Task ID: 3172 User ID: USER456 Status: Failed Status Message: Failed </div>			
Steps			
#	Name	Description	Status
1	Validate deployable state	Validate that the deployment is in a state that can be deployed	Succeeded
2	Deployment Update Status: Snapshot In Progress	Update the deployment status of the deployment	Succeeded
3	Validate remote systems	Validate that the remote systems are valid, including contact systems	Succeeded
4	Lock CSIs in deployment	Serialize access to the CSIs in this deployment	Failed
5	Validate deployment	Validate the deployment settings	Not Started
6	Archive creation	Creating archives for products	Not Started
7	SYSMODS Extraction	Extracting SYSMODS from CSIs	Not Started
8	Freeze deployment	Creating a permanent location for this deployment	Not Started
9	Record target library names	Record the target libraries used by the deployment	Not Started
10	Unlock CSIs in this deployment	Release the serialization of CSIs in this deployment	Not Started
11	Deployment Update Status: Snapshot Completed	Update the deployment status of the deployment	Not Started
12	Deployment Update Status: Deploying	Update the deployment status of the deployment	Not Started
13	Deploy Products	Deploy the product libraries on the target systems	Not Started
14	Deployment Update Status: Deployed	Update the deployment status of the deployment	Not Started

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

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

- Correct the issue and deploy again.

More information:

[Download a Message Log](#) (see page 68)

[Save a Message Log as a Data Set](#) (see page 69)

[View Complete Message Log](#) (see page 69)

Download a Message Log

You can save the message log in the following ways:

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

- To download as ZIP, click the Deployment Name or the Deployment Results on the left tree. Click the Action button on the Message Log bar and click the Download as ZIP. Save this file.

Save a Message Log as a Data Set

You can save a message log as a data set.

Follow these steps:

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

The Save Output as Data Set dialog appears.

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

Note: The asterisk indicates that the field is mandatory.

2. Enter the following information and click OK:

Data Set Name

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

VOLSER

For non-SMS data, enter the Volser.

Example:

Volser: SYSP01 and SYSP02

Storage Class

For SMS Allocation data, enter the Storage Class.

The message log is saved as a data set.

View Complete Message Log

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

Note: To close the message log, click Close.

Reset Deployment Status

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

You can also [investigate a failed deployment](#) (see page 67) to see additional details in the message log.

The following statuses may be reset.

Snapshot in progress

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

Transmitting

Transmitting is reset to *transmit in error*.

Deploying

Deploying is reset to *deploy in error*.

The following artifacts are reset by status.

Snapshot in Progress

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

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

Transmit in Progress

Nothing is reset.

Deploy in Progress

Nothing is reset.

Delete a Deployment

You can delete deployments.

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

A deployment deletion must be confirmed before a deletion starts.

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

The message log explains which containers, folders, and files were deleted during processing and which ones were not deleted. See how to [investigate a failed deployment](#) (see page 67) for details on finding the message log.

Note: Target libraries are never deleted.

The following artifacts are deleted by status:

Under Construction

All applicable database records

Snapshot in Error

All applicable database records

Snapshot Completed

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

All applicable database records.

Transmit in Error

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

Transmitted

Same as Transmit in Error.

Deploy in Error

Same as Transmitted.

Deployed

Same as Snapshot Completed.

Complete

Same as Snapshot Completed.

Follow these steps:

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

Confirm a Deployment

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

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

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

Follow these steps:

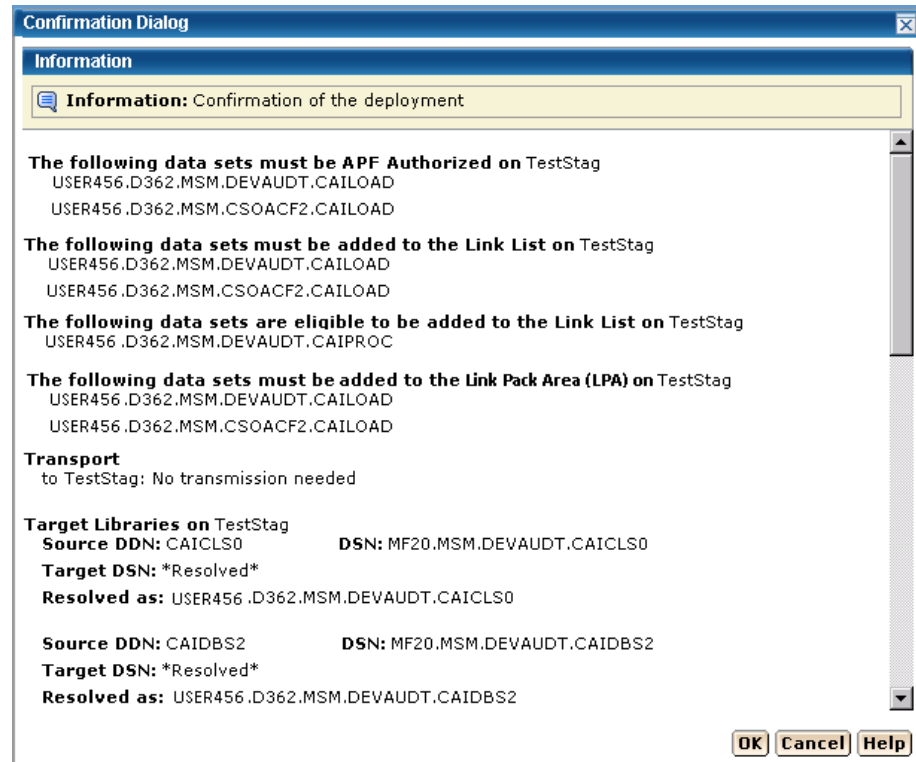
1. Click the Deployments tab.
The Deployment page appears.
2. Click Confirm.
The Confirmation dialog appears.
3. Review the confirmation.
4. Click OK when the deployment is correct.

Note: Click Cancel to exit this procedure without confirming.

The Deployment Summary window may contain the following:

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

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



Products

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

View the Product List

You can view a product.


Follow these steps:

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

Add a Product

You can add a product to a deployment.

Follow these steps:

1. Click the Deployments tab. The Deployments window appears.
2. On the right, in the Deployments panel click the Current Deployment link.
A list of current deployments appears.
3. Click the deployment name link.
4. In the Product List panel click Add Products.
The Add Products wizard appears.
5. Select a CSI and click Next.
The Product Selection appears.
6. Select a product.
7. If there is a  text icon in Text column, click the text icon to read the instructions supplied by CA Support for product, data sets, and other necessary information.
8. Click the "I have read the associated text by selecting the text icon from the list about" box. This box appears only if there is a text icon.
Note: You will not be able to click Next until you click this box.
9. Click Next.
The Custom Data Set Selection appears
10. If needed, select or [add a custom data set](#) (see page 103).
11. Click Add Products.
The Product is added.

Remove a Product

You can remove a product from a deployment.

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

Follow these steps:

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

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

The product is removed.

Custom Data Sets

You can view, [add](#) (see page 103), [edit](#) (see page 106), and [remove](#) (see page 109) custom data sets from a deployment.

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

- For a z/OS data set, you need to provide a data set name that is the actual existing z/OS data set and a mask that names the data set on the target system. This mask may be set up using [symbolic qualifiers](#) (see page 113) 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 113)), and a type of copy. The type of copy can be either a container copy or a file-by-file copy.

View Custom Data Sets

You can view custom data sets.

Follow these steps:

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

The detailed deployment information appears on the right side.

Product Name Sort Arrows

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

Add a Custom Data Set

You can add custom data sets to a deployment.

Follow these steps:

1. Click the Deployments tab.
The Deployments window appears.
2. On the right, in the Deployments panel, click the Current Deployment link.
A list of current deployments appears.
3. Click the deployment name link.
4. In the Custom Data Sets List panel, click Add Data Sets.
The Add Custom Data Sets dialog appears.
Note: The asterisk indicates that the field is mandatory.
5. Select a Product from the drop-down list.
Note: When there are instructions, they are required and supplied by CA Support.
6. Select the Data Set Type, either data set (step 7) or USS (step 10).
Default: data set
7. For data set, enter the data set name.
Limits: Maximum 44 characters.
Note: This is the existing z/OS data set name that you want CA MSM to include in the deployment when it is deployed on the target systems.
8. Enter the data set name mask, click the file icon, and select a [symbolic name](#) (see page 113).

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 113). For example, if you enter CAPRODS.&SYSID, the &SYSID is replaced by its values, and if the SYSID that is being deployed to is XX16, the DSN mask will be CAPRODS.XX16

Limits: Maximum 64 characters.

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

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

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

■

Two consecutive periods are required to separate the two masks.

9. Enter the Mask and click OK.

10. For USS data set type, enter the Local Path. The local path is the directory are where files are to be copied from.

Limit: Maximum 255 characters.

Note: The asterisk indicates that the field is mandatory.

11. Enter the Remote Path and/or click the file icon and select a [symbolic name](#) (see page 113). The remote path is the path where the files are to be copied to.

Limit: Maximum 255 characters.

12. Select the Type of Copy:

- If you select Container Copy, proceed to step 14.
- If you select File-by-file Copy, proceed to step 15, and ensure that the USS path exists on all of the remote systems of this deployment, and that there is sufficient space to hold these target libraries.

Default: Container Copy

13. Click OK.

14. For Container Copy, enter the container name and/or click the file icon and select a [symbolic name](#) (see page 113).

Limit: Maximum 64 characters.

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

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

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

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

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

Note: The asterisk indicates that the field is mandatory.

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

16. Enter the Mount Point and/or click the file icon and select a [symbolic name](#) (see page 113).

Limit: Maximum 255 characters.

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

17. Enter the percentage of Free Space needed.

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

Limit: 0 to 1000.

18. Click OK.

The custom data set is added.

Edit a Custom Data Set

You can edit a custom data set.

Follow these steps:

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

Note: The asterisk indicates that the field is mandatory.

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

Default: data set

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

Limits: Maximum 44 characters.

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

8. Enter the data set name mask, click the file icon, and select a [symbolic name](#) (see page 113).

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 113). For example, if you enter CAPRODS.&SYSID, the &SYSID is replaced by its values, and if the SYSID that is being deployed to is XX16, the dsn mask will be CAPRODS.XX16

Limits: Maximum 64 characters.

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

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

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

-

Two consecutive periods are required to separate the two masks.

9. Enter the Mask and click OK.
10. For USS data set type, enter the Local Path. The local path is the directory where files are to be copied from.
Limit: Maximum 255 characters.
Note: The asterisk indicates that the field is mandatory.
11. Enter the Remote Path and/or click the file icon and select a [symbolic name](#) (see page 113). The remote path is the path where the files are to be copied to.
Limit: Maximum 255 characters.
12. Select the Type of Copy:
 - If you select Container Copy, proceed to step 14.
 - If you select File-by-file Copy, proceed to step 15, and ensure that the USS path exists on all of the remote systems of this deployment, and that there is sufficient space to hold these target libraries.

Default: File-by-file Copy

13. Click OK.
14. For Container Copy, enter the container name and/or click the file icon and select a [symbolic name](#) (see page 113).
Limit: Maximum 64 characters.

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

For container copy the following occurs during the deployment process:

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

Note: The mount is not permanent. You will need to update your BPXPARMS to make this mount point permanent.
- e. The content from the local path will be copied into the newly created and mounted file system.

Note: The asterisk indicates that the field is mandatory.

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

16. Enter the Mount Point and/or click the file icon and select a [symbolic name](#) (see page 113).

Limit: Maximum 255 characters.

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

17. Enter the percentage of Free Space needed.

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

Limit: 0 to 1000.

18. Click OK.

The custom data set is changed.

Remove a Custom Data Set

You can remove a custom data set from a deployment.

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

Follow these steps:

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

Product Name Sort Arrows

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

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

Methodologies

You can [create](#) (see page 110), maintain, [edit](#) (see page 123), and [delete](#) (see page 125) methodologies from a deployment.

A methodology has the following attributes:

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

z/OS data sets

z/OS data sets use a data set name mask. The data set name mask is a valid data set name comprised of constants and [symbolic qualifiers](#) (see page 113).

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

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

Create Only

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

Create or Replace

Use *Create or Replace* to:

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

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

Create a Methodology

You can create a methodology.

Note: The asterisk indicates that the field is mandatory.

Follow these steps:

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

The Create a New Methodology dialog appears.

2. Enter the methodology name.

Limits: Maximum 64 characters.

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

3. Enter the description of this methodology.

Limits: Maximum 255 characters.

4. Enter the data mask name, click the file icon, and select a [symbolic name](#) (see page 113).

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 113). For example, assume you enter, CAPRODS.&SYSID. In this case, the &SYSID. will be replaced by its values. If the SYSID that is being deployed to is X16, the DSN mask will be: CAPRODS.X16

Limits: Maximum 64 characters.

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

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

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

■

5. Select a style of Deployment.

Create only

Creates new data sets.

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

Create or Replace

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

Partitioned data set

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

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

Directory in a UNIX file system

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

Sequential data set or a file in the UNIX file system

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

For a VSAM data set (cluster)

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

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

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

6. Click Save.

The methodology is saved.

Note: Click Cancel to close this dialog without saving.

Symbolic Qualifiers

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

Data Set Name Mask

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

Directory Path

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

Symbolic Substitution

Symbolic substitution, or translation, is a process performed by CA MSM to resolve the mask values specified in the data set name mask and directory path, into real names based upon the contents of the symbolic variables at translation time. A CA MSM symbol is defined in the list of symbols. Each symbol begins with an ampersand (&) and ends with a period (.). For example, the symbol &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 data set name segment.

Example: Assume MSMDID is 255.

SYSWORK.D&MSMDID..DATASET

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

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

Numeric Values

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

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

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

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

An incorrect specification of the mask would be:

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

Directory Paths

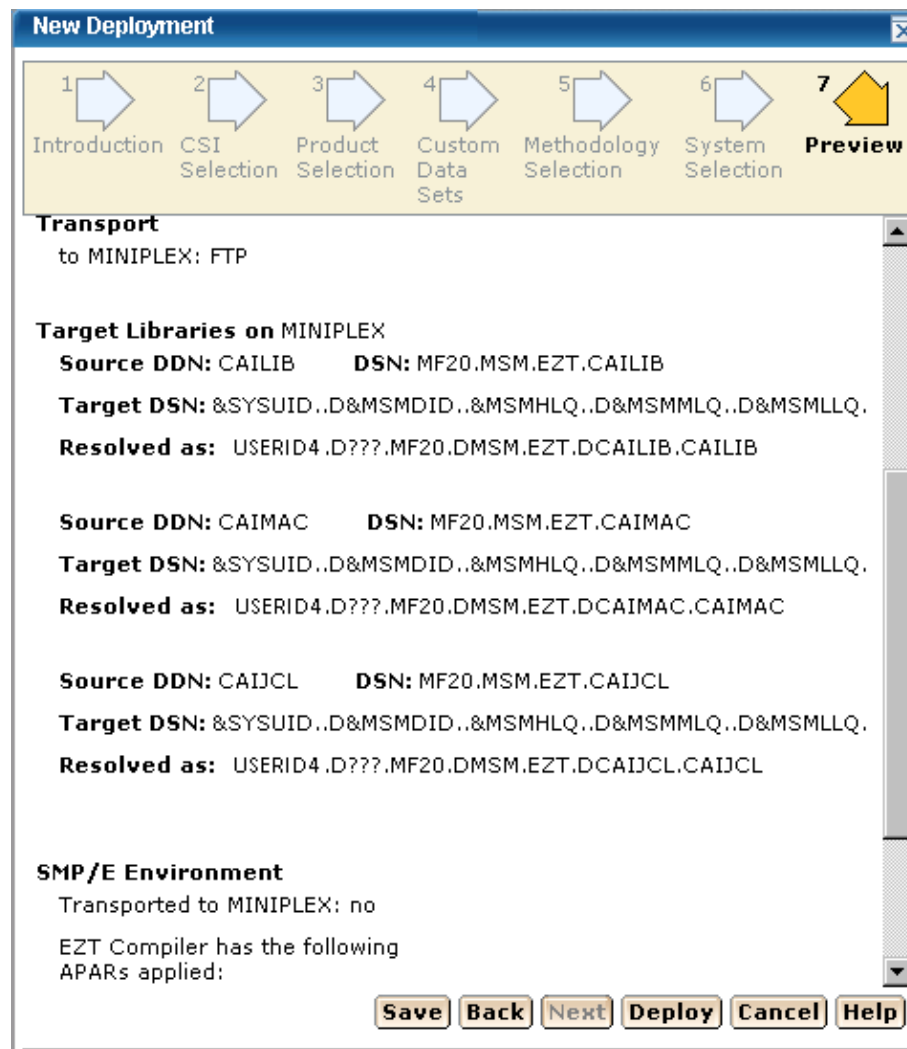
Symbolic substitution works in the same logical way for directory paths. However, directory paths do not typically have periods in them, so you will typically not see the double dots in directory paths.

Example: Assume the target system is SYSZ.

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

Preview Example

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



Symbolic Qualifiers

ID and System Information

MSMDID

This is the CA MSM deployment ID.

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

MSMMPN

This is the CA MSM Mount Point Name. The value is entered into the mount point name field when [adding a custom data set](#) (see page 103) with both the USS radio button and the Container copy radio button set. It is of primary value in remote path.

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

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

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

Remote path: &MSMMPN.

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

MSMSYSNM

This is the CA MSM system object name.

SYSCONE

This is the shorthand name of the system.

Limits: Maximum 2 characters.

SYSNAME

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

SYSPLEX

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

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

SYSUID

The current user ID.

Target Libraries

MSMHLQ

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

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

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

MSMMLQ

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

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

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

MSMLLQ

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

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

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

MSMSLQ

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

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

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

MSMPREF

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

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

MSMDLIBN

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

Example: Assume 3 target libraries in a deployment.

DSN = USER456.LIBR473.CAIPROC

DSN = USER456.LIBR473.CAILOAD

DSN = USER456.LIBR473.CAIEEXEC

Assume the methodology specified a mask of:

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

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

Deployed library = USER789.D877.LIB1.CAIPROC

Deployed library = USER789.D877.LIB2.CAILOAD

Deployed library = USER789.D877.LIB3.CAIEEXEC

Local Date and Time

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

LYR2

This is the local two-digit year.

LYR2 two-digit year

Example: 10

LYR4

This is the local four-digit year.

LYR4 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

Maintain Methodologies

You can edit, replace, or [remove](#) (see page 125) methodologies.

Follow these steps:

1. Click the Deployments tab, and in the Actions section click the Maintain Methodologies link. The Maintain Methodologies select window appears.

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

Select	Name	Description	DSN Mask	Actions
<input type="checkbox"/>	DEPL1		DEPL.D&MSMDID.	Actions▼
<input type="checkbox"/>	MSM01		&MSMHLQ.&MSMLLQ..D&SYSUID.	Actions▼
<input type="checkbox"/>	METH1		&MSMHLQ.	Actions▼

2. Select a methodology. Select Edit from Actions list.

[The Methodology window appears for editing](#) (see page 123).

More information:

[Delete Methodologies](#) (see page 125)

[Edit a Methodology](#) (see page 123)

Edit a Methodology

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

Follow these steps:

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

The Edit Methodologies dialog appears.

Note: The asterisk indicates that the field is mandatory.

As with Add a Methodology, all fields are available to be edited and the details for each field are listed.

3. Enter the Methodology Name.

Limits: Maximum 64 characters.

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

4. Enter the Description of this Methodology.

Limits: Maximum 255 characters.

5. Enter the data set name mask, click the file icon, and select a [symbolic name](#) (see page 113).

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 113).

Example: CAPRODS.&SYSID. - in this case the &SYSID. will be replaced by its values. If the SYSID that is being deployed to is XX16 the DSN mask will be: CAPRODS.XX16

Limits: Maximum 64 characters.

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

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

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

■

6. Select a Style of Deployment.

Create only

Creates new data sets.

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

Create or Replace

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

Partitioned data set

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

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

Directory in a UNIX file system

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

Sequential data set or a file in the UNIX file system

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

For a VSAM data set (cluster)

Create or Replace indicates that an existing VSAM cluster should be populated with the data from the source file.

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

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

7. Click Save.

Your changes are saved.

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

More information:

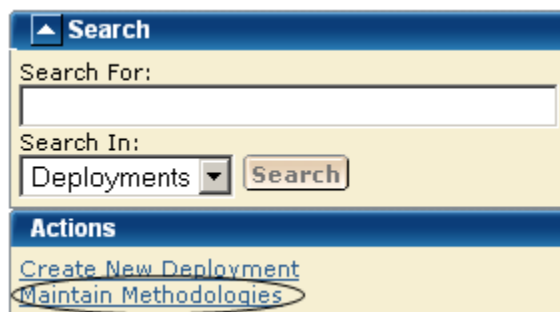
[Symbolic Qualifiers](#) (see page 113)

Delete Methodologies

Follow these steps:

1. Click the Deployments tab, and in the Actions section click the Maintain Methodologies link.

The Maintain Methodologies select window appears.



2. Select the methodology that you want to delete.

Note: A grayed select box indicates that the methodology is assigned and cannot be deleted. It can be edited.

3. Click Delete and then OK to the Delete Methodologies confirmation window.
The methodology is deleted.

Systems

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

Target System Types

There are two types of *target systems*.

Test Environment

Test Environment target systems isolate untested deployment changes and outright experimentation from the production environment or repository. This environment is used a temporary work area where deployments can be tested, modified, overwritten, or deleted.

Production

Production target systems contain current working product deployments. When activating products in a production target system care must be taken, CA MSM recommends using the following procedure.

1. Copy the product to that target system with the data set names set to private. This allows only those assigned to this area to test these deployed products. The purpose of this first stage is to test or verify that the product is working.
2. Use intermediate test phases for products as they move through various levels of testing. For example you may want to let the application development group as a whole use the product in its test mode prior to moving to production.
3. Move the deployed products to production.

View a System List

You can view a system list.

Follow these steps:

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

The detailed deployment information appears on the right side.

System Name Sort Arrows

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

Type Sort Arrows

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

Description Sort Arrows

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

Add a System

You can add a system to a deployment.

Follow these steps:

1. Click the Deployments tab.
The Deployment page appears.
2. On the right, in the Deployments panel click the Current Deployment link.
A list of current deployments appears.
3. Click the deployment name link.
4. In the System List panel, click Add Systems.
The Add Systems window appears.
5. Select a system to add and click OK.

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

The Preview window appears, and the system is added.

Note: Sysplex systems are denoted by Sysplex System:System Name. For example, PLEX1:CO11, where PLEX1 is Sysplex name and CO11 is the system name.

Remove a System

You can remove a system from a deployment.

Follow these steps:

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

System Name Sort Arrows

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

Type Sort Arrows

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

Description Sort Arrows

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

4. In the System List panel, select a system you want to remove.
5. Click Remove and then OK to the Remove Products confirmation window.
The system is removed.

Deployment Summary

The Action button is available after a successful deployment.

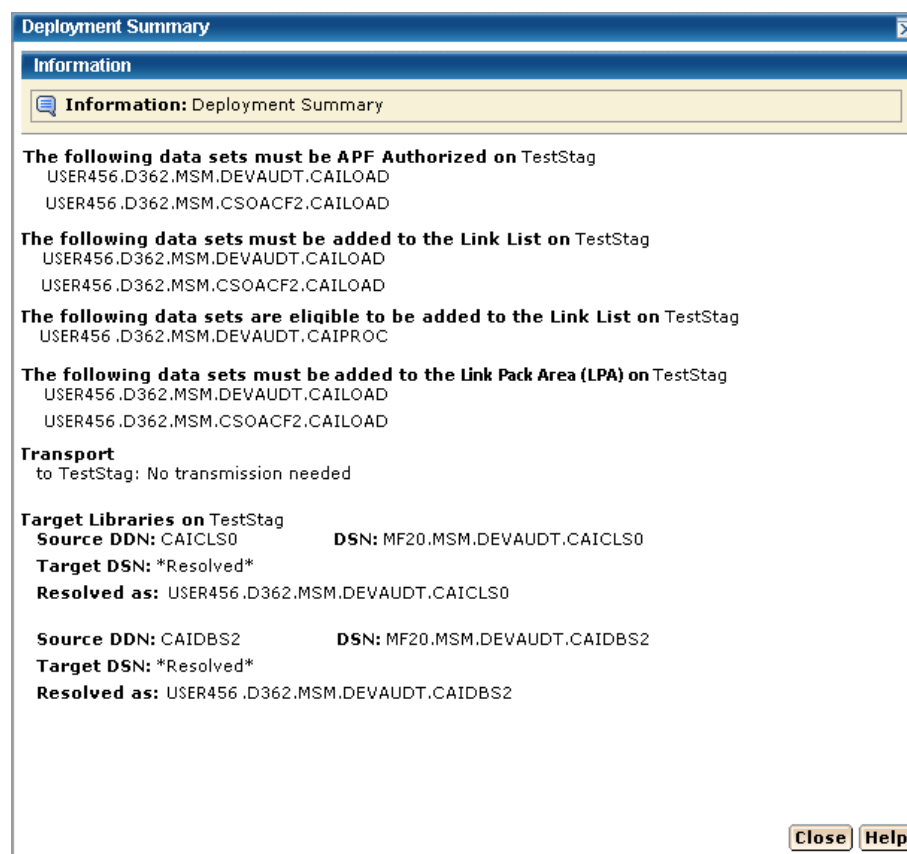
Important! Data sets may need to be APF-authorized and added to the Link List and Link Pack Area. These data sets are identified in this dialog.

The Deployment Summary window may contain the following:

- Deployment ID
- Name
- Products
- Systems
- Data Sets actions
- Transport information

- Target libraries including: source, target, and resolved data set names.
- SMP/E environment
- Snapshot path and container

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



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

Chapter 4: Installing Your Product from Pax-Enhanced ESD

This section contains the following topics:

[How to Install a Product Using Pax-Enhanced ESD](#) (see page 131)

[Allocate and Mount a File System](#) (see page 137)

[Copy the Product Pax Files into Your USS Directory](#) (see page 140)

[Create a Product Directory from the Pax File](#) (see page 145)

[Copy Installation Files to z/OS Data Sets](#) (see page 146)

[Receiving the SMP/E Package](#) (see page 147)

[Clean Up the USS Directory](#) (see page 150)

[Apply Maintenance](#) (see page 151)

How to Install a Product Using Pax-Enhanced ESD

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

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

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

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

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

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

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

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

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

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

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

More Information:

[USS Environment Setup](#) (see page 136)

[Allocate and Mount a File System](#) (see page 137)

[Copy the Product Pax Files into Your USS Directory](#) (see page 140)

[Create a Product Directory from the Pax File](#) (see page 145)

[Copy Installation Files to z/OS Data Sets](#) (see page 146)

How the Pax-Enhanced ESD Download Works

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

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

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

The CA Support Online web page appears.

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

The CA Product Download window appears.

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

For both options, [The ESD Product Download Window](#) (see page 133) topic explains how the download interface works.

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

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

The product is installed on the mainframe.

ESD Product Download Window

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

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

CA Earl - MVS

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

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

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

[View Download Cart](#)

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

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

Download Method

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


HTTP via Download Manager

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

[Download](#)

HTTP via Internet Browser

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

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

FTP

This method allows you to download your file(s) via FTP from CA's content delivery network or via native FTP servers.

Note: Processing is required and an email notification will be sent when your request is ready for downloading.

[FTP Request](#)

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

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

Download Method

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

HTTP via Download Manager

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

[Download](#)

Create a Zip File

This method allows you to bundle your download files into one or more zip files of up to 3.5 GB each. These zip files can then be downloaded via HTTP or FTP.

Note: Processing is required and an email notification will be sent when your request is ready for downloading.

[Create Zip](#)

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

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

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

Review Download Requests

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

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

Today's Downloads

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

Previous 6 day Download History

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

USS Environment Setup

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

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

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

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

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

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

Allocate and Mount a File System

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

This procedure describes how to perform the following tasks:

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

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

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

Important! USS commands are case-sensitive.

Follow these steps:

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

- On a zFS, use the following sample:

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

- On an HFS, use the following sample:

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

The file system is allocated.

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

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

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

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

The mount point is created.

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

- On a zFS, use the following sample:

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

- On an HFS, use the following sample:

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

The file system is mounted.

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

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

Write access is granted.

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

Copy the Product Pax Files into Your USS Directory

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

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

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

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

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

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

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

More Information:

[How the Pax-Enhanced ESD Download Works](#) (see page 133)
[ESD Product Download Window](#) (see page 133)

Download Using Batch JCL

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

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

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

Follow these steps:

1. Supply a valid JOB statement.
2. Replace *yourTCPIP.PROFILE.dataset* with the name of the TCP/IP profile data set for your system. Consult your local network administrators, if necessary.
The job points to your profile.
3. Replace *YourEmailAddress* with your email address.
The job points to your email address.
4. Replace *yourUSSESDdirectory* with the name of the USS directory that you use for ESD downloads.
The job points to your USS directory.
5. Locate the product component to download on the CA Support Product Download window.
You have identified the product component to download.
6. Click Download for the applicable file.
Note: For multiple downloads, add files to a cart.
The Download Method window opens.
7. Click FTP Request.
The Review Download Requests window displays any files that you have requested to download.

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

8. Select one of the following methods:

Preferred FTP

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

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

Alternate FTP

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

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

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

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

9. Submit the job.

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

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

Example: CAtoMainframe.txt, JCL

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

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

Download Files to Mainframe through a PC

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

Follow these steps:

1. Follow the procedures in [How the Pax-Enhanced ESD Download Works](#) (see page 14) to download the product pax or zip file to your PC. If you download a zip file, first unzip the file to use the product pax files.

The pax or zip file resides on your PC.

2. Open a Windows command prompt.

The command prompt appears.

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

The pax file is transferred to the mainframe.

Example: FTP Commands

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

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


Create a Product Directory from the Pax File

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

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

Follow these steps:

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

The job points to your specific directory.

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

The job points to your specific pax file.

4. Submit the job.

The job runs and creates the product directory.

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

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

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

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

Copy Installation Files to z/OS Data Sets

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

Follow these steps:

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

You have identified the product-specific installation details.

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

The job is edited.

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

Your view is of the product-specific directory.

4. If ICSF is not active, perform the following steps:

- a. Change the SMPJHOME DD PATH to your Java runtime directory. This directory varies from system to system.

Note: The default Java location is the following:

`/usr/lpp/java/Java_version`

- b. Perform one of the following steps:

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

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

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

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

6. Submit the UNZIPJCL job.

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

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

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

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 PanAPT. 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 APTSEDIT 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 APTSEDIT 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 APTSEDIT macro each time you open a new SAMPJCL member. To edit all SAMPJCL members simultaneously, read and follow the instructions in the APTEDALL member.

2. Open the SAMPJCL member APT1ALL in an edit session and execute the APTSEDIT macro from the command line.

APT1ALL is customized.

3. Submit APT1ALL.

This job produces the following results:

- The target and distribution data sets for CA PanAPT are created.
- Unique SMPPTS, SMPMTS, SMPSCDS, and SMPSTS data sets for this target zone are created.

4. Open the SAMPJCL member APT2CSI in an edit session and execute the APTSEDT macro from the command line.

APT2CSI is customized.

5. Submit APT2CSI.

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. Submit the *yourhlq*.SAMPJCL member APT3RECD to receive SMP/E base functions.
CA PanAPT is received and now resides in the global zone.
2. Customize and submit the *yourhlq*.SAMPJCL member APT4APP to APPLY SMP/E base functions.
Your product is applied and now resides in the target libraries.
3. Customize and submit the *yourhlq*.SAMPJCL member APT5ACC to ACCEPT SMP/E base functions.
Your product is accepted and now resides in the distribution libraries.

Clean Up the USS Directory

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

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

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

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

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

Follow these steps:

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

Your view is of the applicable USS directory.

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

```
rm paxfile
```

paxfile

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

The pax file is deleted.

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

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

product-specific_directory

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

The product-specific directory is deleted.

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

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

Apply Maintenance

CA Support Online may have maintenance and hold data that have been published since the installation data was created.

To apply maintenance

1. Check CA Support Online and download any PTFs and hold data published since this release was created.

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

The PTFs and hold data become accessible to the *yourhlq.SAMPJCL* maintenance members.

3. Edit and submit the APTSEEDIT macro.

The *yourhlq.SAMPJCL* members APT6RECP, APT7APYP, and APT8ACCP are customized.

4. Customize the APT6RECP SMPPTFIN and SMPHOLD DD statements to reference the FB 80 data sets for the PTFs and hold data.

5. Submit APT6RECP.

The PTFs and hold data are received.

6. Submit APT7APYP.

The PTFs are applied.

7. (Optional) Customize and submit yourhlq.SAMPJCL member APT8ACCP.

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, you are ready to configure 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 system and external HOLDDATA.

Copy Modules to Authorized Link List Library (Optional)

Member BY32UM01 is an SMP/E USERMOD that moves the modules used by the CA Panvalet REXX Move procedures to an APF-authorized load library. Only users who intend to use this feature need to apply this USERMOD. See the JCL comments for detailed instructions in applying this USERMOD. If the USERMOD APPLY completes with a return code greater than 0, review the output, correct the problem, and resubmit the job.

Also, manually update member IKJTSOxx of SYS1.PARMLIB to include command name APTALLOC by adding or merging this statement:

```
AUTHCMD NAMES(APTALLOC) .
```

Program APTALLOC, which allocates data sets for REXX move procedures, must be run authorized, or must be run under a user ID allowed to mount tapes, if tape data sets are to be used in REXX Move procedures. If you choose to run it authorized, then you must apply the USERMOD that copies load modules APTALLOC, APTALLMS, APAS0095, and APAS0097 to an authorized load library in the link list. If the load library is not in the link list, then you might have problems running authorized if non-authorized libraries are concatenated with it in JOBLIB or STEPLIB specifications.

Update Your Security System

The following steps cover updating your security system to authorize data set access to CA PanAPT users. In addition, if you plan to use an external security system, this step covers updating your security system to allow access for standard CA PanAPT security checks.

Data Set Authorization

All data sets created so far should be regarded as protected production data sets with the exception of the database and history files. Update your security system to the appropriate access for your site.

To update your security system

1. Set your security system to grant update authority to data in the database and the history files for anyone who needs to use CA PanAPT.

CA PanAPT built-in security protects data in the database and the history files. CA PanAPT users must be able to read from and write to these data sets.

2. Give system administrators update authority for the following data sets:

- Data Set Name Description
- prefix.APTDB Database
- prefix.APTHIST History File
- CABYDATA Model Library

The prefix is the prefix specified at your site by the individual who installed CA PanAPT.

External Security Setup

CA PanAPT issues external security calls almost about every function and action related to CA PanAPT functionality. CA PanAPT uses the CA Standard Security Facility (CAISSF), which is a standardized security interface to CA ACF2, CA Top Secret, and RACF. The CA PanAPT User Identification Facility (UIF) also interfaces with external security. All security rules are in DSN format so that the rules built by CA PanAPT are the same regardless of the security package you are running.

To use the external security interface

1. Define PANAPT as a resource class to your security system.
2. Use the high-level ownership for CA Top Secret or the key for CA ACF2 as follows:
 - PANAPTF for CA PanAPT functionality
 - PANAPTU for CA PanAPT/UIF functionality
3. If your security package requires access rules, then you must update your security system to allow access for the following security checks:
 - Require a CA PanAPT/UIF logon system ID to access CA PanAPT. The CAISSF rule is:
`PANAPTU.PANAPT`
 - Authorize the system ID entered or that was selected from an MSL. The CAISSF rule is:
`PANAPTU.PANSYSID.system-id`
 - Authorize CA-PanAPT/UIF usage to create or change logon system IDs. The CAISSF rule is:
`PANAPTU.PANUIF`
 - Allow CA-PanAPT activities for authorized system ID. The CAISSF rule is:
`PANAPTF.system-id.xxxxxxxx.xxxxxxxx.xxxxxxx`

See the CA ACF2 Example that allows access to all users and all activities.

CA ACF2 Example

The following steps are for CA ACF2, which requires rules to exist before access is granted.

1. Create a CLASMAP for CA PanAPT.

For example, you can create the resource type as type(APT).

```
ACF
```

```
T C(GSO)
```

```
INSert CLASMAP.PANAPT resource(PANAPT) rsrcType(APT)
```

```
List LIKE(CLASMAP.-)
```

```
--List clasmap to see if the type you created is defined.
```

2. Add R-RAPT into the GSO INFODIR record by issuing the following command in GSO control mode:

```
CH INFODIR types(R-RAPT)
```

3. Create resource rules for CA PanAPT/UIF to allow users to log on to CA PanAPT and:

- Not require a CA PanAPT logon system ID when entering CA PanAPT.
- Allow any CA PanAPT logon system ID to be used, if using system IDs.
- Use CA-PanAPT/UIF to create and or change CA PanAPT logon system IDs.

```
T R(APT) -- --RSRCTYPE created in step 1
COMP *
$key(PANAPTU) type(APT) --RSRCTYPE created in step 1
PANAPT uid(*) allow- --Not require a system ID
PANSYSID.- uid(*) allow --Allow all system IDs
PANUIF uid(*) allow --Allow CA-PanAPT/UIF
--functionality
STORE
L PANAPTU --List the resource rules
```

4. Create resource rules for CA-PanAPT to allow all users to perform all CA-PanAPT activities.

```
COMP *
$key(PANAPTF) type(APT) --RSRCTYPE created in step 1
- uid(*) allow --Allow CA-PanAPT functionality
STORE
L PANAPTF --List the resource rules
END --Exit CA-ACF2
```

5. Refresh CLASMAP and INFODIR records.

```
F ACF2,REFRESH(CLASMAP,INFODIR),SYSID(yyyy)
```

(where yyyy is your system ID)

6. Rebuild resource directory.

F ACF2,REBUILD(APT),CLASS(R) RSRCTYPE created in step 1

Define or Convert the VSAM CA PanAPT Database

New Users Member BY32VSDB is an IDCAMS job that defines a CA PanAPT VSAM “starter” database file on DASD, with DSN <VPFX>.APTDB. New users should run this job to define the starter data set.

To define or convert the database

1. New users, edit the JCL to specify the DSN and VOLSER of the target data set.
Make the changes indicated and submit the job.
See the instructions in the JCL for further details.
2. Existing users see the Conversion chapter for detailed instructions on how to upgrade your existing database.

Define or Convert the VSAM CA PanAPT History Database

New Users Member BY32VSHS is an IDCAMS job that defines a CA-PanAPT VSAM history file on DASD, with DSN <VPFX>.APTHIST. New users should run this job to define the history file.

To define or convert the history database

New users, edit the JCL to specify the DSN and VOLSER of the target data set.

Make the changes indicated and submit the job.

See the instructions in the JCL for further details.

Existing users, see the Conversion chapter for detailed instructions on how to upgrade your existing history database.

Update the Model Exchange PDS (Optional)

Member BY32EXCH is an IEBCOPY job that unloads the model exchange CAI.MODEL.EXCHANGE PDS to DASD.

To update the model exchange PDS

1. Edit the JCL to specify the DSN and VOLSER of the target data set for the PDS.
Make the changes indicated and submit the job.
2. See the instructions in the JCL for further details.

The exchange file consists of many members containing user-developed CA PanAPT models that are applicable to a variety of OS/390 environments. Examine the table of contents in member \$\$INDEX for items of relevance and interest.

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 160)

[How to Install Products Using Native SMP/E JCL](#) (see page 161)

[Apply Maintenance](#) (see page 163)

Unload the Sample JCL from Tape

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

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

Follow these steps:

1. Run the following sample JCL:

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

unitname

Specifies the tape unit to mount the tape.

nnnnnnnn

Specifies the tape volume serial number.

yourHLQ

Specifies the data set prefix for the installation.

sysda

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

The SAMPJCL data set is created and its contents are downloaded from the tape.

2. Continue with one of the following options:
 - If you already have set up the SMP/E environment, go to Run the Installation Jobs for a Tape Installation.
 - If you have *not* set up the SMP/E environment, go to Prepare the SMP/E Environment for Tape Installation.

How to Install Products Using Native SMP/E JCL

The following steps describe the process to install products using native SMP/E JCL:

1. Allocate product data sets and SMP/E data sets.
2. Create SMP/E CSI.
3. Receive base functions.
4. Apply base functions.
5. Accept base functions.
6. Configure the product according to your site requirements.

Prepare the SMP/E Environment for Tape Installation

The members in this procedure prepare the data sets, initialize the zones, and create the DDDEFs for CA PanAPT. 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 APTSEEDIT 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 APTSEEDIT on the TSO command line, and press Enter to replace the defaults with your specifications.

The macro is ready to customize your hlq.SAMPJCL members.

Note: The following steps include instructions to execute the APTSEEDIT macro each time you open a new SAMPJCL member. To edit all SAMPJCL members simultaneously, read and follow the instructions in the APTEDALL member.

2. Open the SAMPJCL member APT1ALL in an edit session and execute the APTSEEDIT macro from the command line.

APT1ALL is customized.

3. Submit APT1ALL.

This job produces the following results:

- The target and distribution data sets for CA PanAPT are created.
- Unique SMPPTS, SMPMTS, SMPSCDS, and SMPSTS data sets for this target zone are created.

4. Open the SAMPJCL member APT2CSI in an edit session and execute the APTSEEDIT macro from the command line.

APT2CSI is customized.

5. Submit APT2CSI.

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. Submit the *yourhlq*.SAMPJCL member APT3RECT to receive SMP/E base functions.

CA PanAPT is received and now resides in the global zone.

2. Customize and submit the *yourhlq*.SAMPJCL member APT4APP to APPLY SMP/E base functions.

Your product is applied and now resides in the target libraries.

3. Customize and submit the *yourhlq*.SAMPJCL member APT5ACC to ACCEPT SMP/E base functions.

Your product is accepted and now resides in the distribution libraries.

Note: We recommend that you check for available maintenance; however, you may find that none is available.

Apply Maintenance

CA Support Online may have maintenance and hold data that have been published since the installation data was created.

To apply maintenance

1. Check CA Support Online and download any PTFs and hold data published since this release was created.
2. Transfer the downloaded files to two separate FB 80 sequential data sets. Use one data set to contain the PTFs and the other to contain the hold data.

The PTFs and hold data become accessible to the *yourhlq.SAMPJCL* maintenance members.

3. Edit and submit the APTSEEDIT macro.

The *yourhlq.SAMPJCL* members APT6RECP, APT7APYP, and APT8ACCP are customized.

4. Customize the APT6RECP SMPPTFIN and SMPHOLD DD statements to reference the FB 80 data sets for the PTFs and hold data.

5. Submit APT6RECP.

The PTFs and hold data are received.

6. Submit APT7APYP.

The PTFs are applied.

7. (Optional) Customize and submit *yourhlq.SAMPJCL* member APT8ACCP.

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, you are ready to configure your product.

Hold Data

When you apply maintenance, you typically encounter SMP/E hold data. We use hold data to notify your SMP/E system of SYSMODs that have errors or special conditions. We support two types of hold data:

System hold data

Indicates data that is an in-stream part of the SYSMOD instructing you of special conditions. Examples of system hold data 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 hold data

External hold data 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 hold data from CA Support Online to a DASD file, and allocate the file to the SMPHOLD DD statement. To take advantage of the external hold data, receive it into your SMP/E environment. If you use the jobs supplied by CA, SMP/E receives the hold data.

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 hold data 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 hold data, 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.

Copy Modules to Authorized Link List Library (Optional)

Member BY32UM01 is an SMP/E USERMOD that moves the modules used by the CA Panvalet REXX Move procedures to an APF-authorized load library. Only users who intend to use this feature need to apply this USERMOD. See the JCL comments for detailed instructions in applying this USERMOD. If the USERMOD APPLY completes with a return code greater than 0, review the output, correct the problem, and resubmit the job.

Also, manually update member IKJTSOxx of SYS1.PARMLIB to include command name APTALLOC by adding or merging this statement:

```
AUTHCMD NAMES(APTALLOC) .
```

Program APTALLOC, which allocates data sets for REXX move procedures, must be run authorized, or must be run under a user ID allowed to mount tapes, if tape data sets are to be used in REXX Move procedures. If you choose to run it authorized, then you must apply the USERMOD that copies load modules APTALLOC, APTALLMS, APAS0095, and APAS0097 to an authorized load library in the link list. If the load library is not in the link list, then you might have problems running authorized if non-authorized libraries are concatenated with it in JOBLIB or STEPLIB specifications.

Update Your Security System

The following steps cover updating your security system to authorize data set access to CA PanAPT users. In addition, if you plan to use an external security system, this step covers updating your security system to allow access for standard CA PanAPT security checks.

Data Set Authorization

All data sets created so far should be regarded as protected production data sets with the exception of the database and history files. Update your security system to the appropriate access for your site.

To update your security system

1. Set your security system to grant update authority to data in the database and the history files for anyone who needs to use CA PanAPT.

CA PanAPT built-in security protects data in the database and the history files. CA PanAPT users must be able to read from and write to these data sets.

2. Give system administrators update authority for the following data sets:
 - Data Set Name Description
 - prefix.APTDB Database
 - prefix.APTHIST History File
 - CABYDATA Model Library

The prefix is the prefix specified at your site by the individual who installed CA PanAPT.

External Security Setup

CA PanAPT issues external security calls almost about every function and action related to CA PanAPT functionality. CA PanAPT uses the CA Standard Security Facility (CAISSF), which is a standardized security interface to CA ACF2, CA Top Secret, and RACF. The CA PanAPT User Identification Facility (UIF) also interfaces with external security. All security rules are in DSN format so that the rules built by CA PanAPT are the same regardless of the security package you are running.

To use the external security interface

1. Define PANAPT as a resource class to your security system.
2. Use the high-level ownership for CA Top Secret or the key for CA ACF2 as follows:
 - PANAPTF for CA PanAPT functionality
 - PANAPTU for CA PanAPT/UIF functionality
3. If your security package requires access rules, then you must update your security system to allow access for the following security checks:
 - Require a CA PanAPT/UIF logon system ID to access CA PanAPT. The CAISSF rule is:
`PANAPTU.PANAPT`
 - Authorize the system ID entered or that was selected from an MSL. The CAISSF rule is:
`PANAPTU.PANSYSID.system-id`
 - Authorize CA-PanAPT/UIF usage to create or change logon system IDs. The CAISSF rule is:
`PANAPTU.PANUIF`
 - Allow CA-PanAPT activities for authorized system ID. The CAISSF rule is:
`PANAPTF.system-id.xxxxxxxx.xxxxxxxx.xxxxxxx`

See the CA ACF2 Example that allows access to all users and all activities.

CA ACF2 Example

The following steps are for CA ACF2, which requires rules to exist before access is granted.

1. Create a CLASMAP for CA PanAPT.

For example, you can create the resource type as type(APT).

```
ACF
```

```
T C(GSO)
```

```
INSert CLASMAP.PANAPT resource(PANAPT) rsrcrctype(APT)
```

```
List LIKE(CLASMAP.-)
```

--List clasmap to see if the type you created is defined.

2. Add R-RAPT into the GSO INFODIR record by issuing the following command in GSO control mode:

```
CH INFODIR types(R-RAPT)
```

3. Create resource rules for CA PanAPT/UIF to allow users to log on to CA PanAPT and:

- Not require a CA PanAPT logon system ID when entering CA PanAPT.
- Allow any CA PanAPT logon system ID to be used, if using system IDs.
- Use CA-PanAPT/UIF to create and or change CA PanAPT logon system IDs.

```
T R(APT) -- --RSRCTYPE created in step 1
COMP *
$key(PANAPTU) type(APT) --RSRCTYPE created in step 1
PANAPT uid(*) allow- --Not require a system ID
PANSYSID.- uid(*) allow --Allow all system IDs
PANUIF uid(*) allow --Allow CA-PanAPT/UIF
--functionality
STORE
L PANAPTU --List the resource rules
```

4. Create resource rules for CA-PanAPT to allow all users to perform all CA-PanAPT activities.

```
COMP *
$key(PANAPTF) type(APT) --RSRCTYPE created in step 1
- uid(*) allow --Allow CA-PanAPT functionality
STORE
L PANAPTF --List the resource rules
END --Exit CA-ACF2
```

5. Refresh CLASMAP and INFODIR records.

```
F ACF2,REFRESH(CLASMAP,INFODIR),SYSID(yyyy)
```

(where yyyy is your system ID)

6. Rebuild resource directory.

F ACF2,REBUILD(APT),CLASS(R) RSRCTYPE created in step 1

Define or Convert the VSAM CA PanAPT Database

New Users Member BY32VSDB is an IDCAMS job that defines a CA PanAPT VSAM “starter” database file on DASD, with DSN <VPFX>.APTDB. New users should run this job to define the starter data set.

To define or convert the database

1. New users, edit the JCL to specify the DSN and VOLSER of the target data set.
Make the changes indicated and submit the job.
See the instructions in the JCL for further details.
2. Existing users see the Conversion chapter for detailed instructions on how to upgrade your existing database.

Define or Convert the VSAM CA PanAPT History Database

New Users Member BY32VSHS is an IDCAMS job that defines a CA-PanAPT VSAM history file on DASD, with DSN <VPFX>.APTHIST. New users should run this job to define the history file.

To define or convert the history database

New users, edit the JCL to specify the DSN and VOLSER of the target data set.

Make the changes indicated and submit the job.

See the instructions in the JCL for further details.

Existing users, see the Conversion chapter for detailed instructions on how to upgrade your existing history database.

Update the Model Exchange PDS (Optional)

Member BY32EXCH is an IEBCOPY job that unloads the model exchange CAI.MODEL.EXCHANGE PDS to DASD.

To update the model exchange PDS

1. Edit the JCL to specify the DSN and VOLSER of the target data set for the PDS.
Make the changes indicated and submit the job.
2. See the instructions in the JCL for further details.

The exchange file consists of many members containing user-developed CA PanAPT models that are applicable to a variety of OS/390 environments. Examine the table of contents in member \$\$INDEX for items of relevance and interest.

Note: When you have completed the procedures in this section, go to Configuring Your Product.

Chapter 6: Preparing to Start Your Product

This chapter describes the tasks needed before CA PanAPT can be started and used.

This section contains the following topics:

[Verify Installation Checklist](#) (see page 171)

[Complete Installation Checklist](#) (see page 181)

Verify Installation Checklist

Use the following steps as a checklist for verifying the installation:

1. Create TSO logon procedure.
2. Modify the ISPF Primary Option Menu.
3. Create test PDS libraries.
4. Set up PF keys.
5. Edit members in CABYCLS0.
6. Verify online system.
7. Edit members in CAI.CABYDATA
8. Edit members in CAI.CABYJCL.
9. Verify batch system.

Create TSO Logon Procedure

Create a TSO logon procedure to allocate the necessary CA PanAPT software libraries. Concatenate these data sets with the corresponding IBM ISPF/PDF data sets.

To create a TSO logon procedure

1. Concatenate the corresponding CA PanAPT software library as the first data set for each applicable ddname.
2. Specify the CA PanAPT load library and the LE/390 COBOL Compiler runtime library in the allocation for the ddname STEPLIB or ISPLLIB.

As an alternative, place these libraries in the link list.

Ensure that the CA PanAPT PDS libraries have a block size that is equal to or larger than all of the other data sets in each concatenation, or unpredictable results occur.

The SYSOUT DD is required by some sort programs. Without it, the sort might pass back a non-zero return code, causing online reports to fail.

The following is a sample TSO logon procedure:

Authorize several TSO user IDs to use this logon procedure so you can see the effects of CA PanAPT security authorization.

```
//STEPNAME      EXEC  PGM=IKJEFT01,PARM='PROFILE',DYNAMNBR=25
//*
//* Note: This example LOGON procedure assumes that a CLIST
//*       named PROFILE exists in the SYSPROC concatenation,
//*       and that it will allocate the user's ISPPROF data set.
//*       This is done via the PARM='PROFILE' on the EXEC
//*       statement. If you do not want to follow this
//*       procedure, remove the PARM='PROFILE' from the EXEC.
//*
//STEPLIB      DD  DISP=SHR,DSN=CAI.CABYLOAD
//              DD  DISP=SHR,DSN=SYS1.COB2LIB
//              DD  DISP=SHR,DSN=ISR.V2R3M0.ISRLOAD
//              DD  DISP=SHR,DSN=ISP.V2R3M0.ISPLOAD
//ISPLLIB      DD  DISP=SHR,DSN=CAI.CABYLOAD
//              DD  DISP=SHR,DSN=SYS1.COB2LIB
//              DD  DISP=SHR,DSN=ISR.V2R3M0.ISRLOAD
//              DD  DISP=SHR,DSN=ISP.V2R3M0.ISPLOAD
//ISPPLIB      DD  DISP=SHR,DSN=CAI.CABYPENU
//              DD  DISP=SHR,DSN=ISR.V2R3M0.ISPPLIB
//              DD  DISP=SHR,DSN=ISP.V2R3M0.ISPPLIB
//ISPMLIB      DD  DISP=SHR,DSN=CAI.CABYMSG0
//              DD  DISP=SHR,DSN=ISR.V2R3M0.ISRMLIB
//              DD  DISP=SHR,DSN=ISP.V2R3M0.ISPMLIB
```

```

//ISPSLIB DD DISP=SHR,DSN=CAI.CABYSKL0
// DD DISP=SHR,DSN=ISR.V2R3M0.ISRSLIB
// DD DISP=SHR,DSN=ISP.V2R3M0.ISPSLIB
//ISPTLIB DD DISP=SHR,DSN=CAI.CABYTL0
// DD DISP=SHR,DSN=ISR.V2R3M0.ISRTLIB
// DD DISP=SHR,DSN=ISR.V2R3M0.ISPTLIB
//SYSPROC DD DISP=SHR,DSN=CAI.CABYCLS0
// DD DISP=SHR,DSN=ISR.V2R3M0.ISRCLIB
//APTSIDTB DD DISP=SHR,DSN=CAI.APTSIDTB
//SYSPRINT DD TERM=TS
//SYSOUT DD TERM=TS
//SYSIN DD TERM=TS
//*
/* If you are not using the UIF function and you are invoking
/* CA PanAPT without invoking the APT CLIST, you must allocate
/* the APTDB and CABYDATA data sets prior to executing
/* PGM(APCS1000) from the primary option menu.
/*
/* APTDB DD DISP=SHR,DSN=CAI.APTDB
/* APTMODEL DD DISP=SHR,DSN=CAI.CABYDATA

```

How the Modifying the ISPF Primary Option Menu Works

A modified copy of the IBM sample ISPF/PDF Primary Option Menu panel is distributed with CA PanAPT on the CAI.CABYPENU data set as member APIPPRIM. It has been modified to place the CA PanAPT option on the display definition and on the corresponding SELECT statement in the PROC section. The modifications have been changed with this release to activate the new User Identification Facility (UIF). A sample SELECT statement for CA PanAPT without UIF has been provided as a comment line. APIPPRIM has been provided with the assumption that you will want to use the UIF feature.

Examine these modifications and make the same modifications to your Primary Option Menu panel (ISR@PRIM). Or, use APIPPRIM as distributed after renaming it ISR@PRIM and after reviewing it for compatibility with your system.

You can make three modifications to your Primary Option Menu panel:

- CA PanAPT using the new User Identification Facility (UIF). Call CA PanAPT for development under a specific pre-defined UIF development environment.
- CA PanAPT UIF setup and administration. Call UIF to define or administer a development environment.
- CA PanAPT without UIF activated.

A sample ISPF/PDF Primary Option Menu panel for CA PanAPT with both the UIF (Option A) and the UIF administrator's function (Option U) visible is shown next. Notice the line below Option A. An input field is associated with the selection of this option. Be sure to include this line if you want to use CA PanAPT with the UIF feature.

```

----- ISPF/PDF PRIMARY OPTION MENU -----
OPTION ==>
0 ISPF PARMs - Specify terminal and user parameters
1 BROWSE - Display source data or output listings
2 EDIT - Create or change source data
3 UTILITIES - Perform utility functions
4 FOREGROUND - Invoke language processors in foreground
5 BATCH - Submit job for language processing
6 COMMAND - Enter TSO command or CLIST
7 DIALOG TEST - Perform dialog testing
8 LM UTILITIES - Perform library management utility functions
A CA PanAPT - Development and Production Turnover System:
  For UIF, Enter CA PanAPT Logon System-ID or * for MSL => _____
U CA PanAPT/UIF - APT User Identification Facility, System-ID setup
C CHANGES - Display summary of changes for this release
T TUTORIAL - Display information about ISPF/PDF
X EXIT - Terminate ISPF using log and list defaults

Enter END command to terminate ISPF.

```

You can invoke CA PanAPT with and without the UIF

Invoke CA PanAPT With the UIF

You can modify your ISPF/PDF Primary Option Menu panel to invoke CA PanAPT and have the UIF establish a development environment at the same time.

To invoke CA PanAPT from your ISPF/PDF Primary Option Menu

Add the following statements to ISR@PRIM:

```

)BODY section:
"% A +CA PanAPT - Development and Production Turnover System:      "
"  For UIF, Enter CA PanAPT Logon System-ID or * for MSL =>_APTSYSID+ "
)INIT section:
".CURSOR = ZCMD "
)PROC section:
"A, 'PGM(APCS1000) NEWAPPL(APT) PARM(&ZTRAIL;&APTSYSID) NOCHECK' "

```

Invoke the UIF Administration Function

You can modify your ISPF/PDF Primary Option Menu panel to invoke the CA PanAPT UIF administration function

To invoke the CA PanAPT UIF administration function

1. Add the following statements to ISR@PRIM:

)BODY section:

```
"% U +CA PanAPT/UIF - APT User Identification Facility, System-ID setup "
```

)PROC section:

```
" U, 'PGM(APAS4UIF) NOCHECK' "
```

The UIF feature requires the presence of an ISPF table data set allocated to ddname APTSIDTB.

2. Create a new ISPF table data set or use an existing one, as appropriate for your environment.

Suggested DCB attributes: (RECFM FB LRECL 80 BLKSIZE 3120).

Invoke CA PanAPT Without the UIF

You can modify your ISPF/PDF Primary Option Menu panel to invoke CA PanAPT without the UIF feature.

Add the following statements to ISR@PRIM:

)BODY section:

```
"% A +CA PanAPT - Development and Production Turnover System "
```

)PROC section:

```
"A, 'CMD(%APT) NOCHECK' "
```

Alternatively, if you have previously allocated the APTDB and APTMODEL data sets, use the following statement:

```
"A, 'PGM(APCS1000) NEWAPPL(APT) PARM(&ZTRAIL) NOCHECK' "
```

The following is a sample panel invoking CA PanAPT without the UIF feature.

```
----- ISPF/PDF PRIMARY OPTION MENU -----  
  
OPTION ==>  
  
0 ISPF PARMs - Specify terminal and user parameters      USERID - BUTR002  
1 BROWSE     - Display source data or output listings    TIME    - 17:29  
2 EDIT       - Create or change source data              TERMINAL - 3278  
3 UTILITIES  - Perform utility functions                 PF KEYS - 24  
4 FOREGROUND - Invoke language processors in foreground  
5 BATCH      - Submit job for language processing  
6 COMMAND    - Enter TSO command or CLIST  
7 DIALOG TEST - Perform dialog testing  
8 LM UTILITIES - Perform library management utility functions  
A CA PanAPT   - Development and Production Turnover System  
C CHANGES   - Display summary of changes for this release  
T TUTORIAL    - Display information about ISPF/PDF  
X EXIT       - Terminate ISPF using log and list defaults  
  
Enter END command to terminate ISPF.
```

Create Test PDS Libraries

Member BY31PDST allocates five test PDSs to test the batch portion of CA PanAPT.

To create test PDS libraries

1. Edit the JCL to conform to your installation standards and the installation worksheet before submitting this job.

The data sets allocated are as follows:

```
user-id.TEST.PDS  
user-id.QUAL.PDS  
user-id.PROD.PDS  
user-id.BKUP.PDS  
user-id.BKOT.PDS
```

2. Substitute your TSO user ID for the characters user-id.
3. Substitute a valid VOLSER to receive the test PDSs.

After these PDSs are allocated, the PROD library and the TEST library have five members each for testing purposes. The programs in the TEST library simulate new versions of programs to be placed into the PROD library by CA PanAPT.

Set Up PF Keys

Many of the modifications you perform during installation and implementation involve changing all occurrences of certain character strings. We recommend that you set up PF keys to perform CHANGE commands using < and > signs.

To change the following strings

- Add <SPFX> to the prefix used for the CAI software libraries (1-30 characters)
- Add <VPFX> to the prefix used for your CAI VSAM files (1-30 characters)
- Add <OPFX> to the prefix used for all other non-VSAM files (1-21 characters)
Note: The previous three prefixes can be the same. There is no requirement that they be different.
- Add <MDSCB> to the name of your Model DSCB used for creating new generations of a Generation Data Group (GDG).

Edit Members in the CABYCLS0

Member APT in the CABYCLS0 allocates CA PanAPT files before entry into the product.

Use the PF keys you set up to change the character string <VPFX> to the VSAM prefix, and to change <SPFX> to the "CAI" software prefix you indicated during the Set Up PF Keys step.

Verify Online System

To access the online portion of the system

1. Log on to TSO using your newly created logon procedure and select ISPF.
The ISPF/PDF Primary Option Menu panel should now show the CA PanAPT option.
2. Select the CA PanAPT option and press Enter.
The CA PanAPT Main Menu panel displays. CA PanAPT has now been activated.
3. Press PF3 to exit CA PanAPT.
4. From the ISPF/PDF Primary Option Menu, type TSO APT on the command line and press Enter.

This is an alternate method of entering CA PanAPT and can be performed from any ISPF/PDF command line.

See the *Reference Guide* for further information.

Process Test Control Files

If you are familiar with processing test control files, perform the following steps. If not, for more information see the *Reference Guide*.

To process test control files

1. Update the system information record in the control file with the system ID, company name, date format, date separator, and time separator of your choice.

You can revise CA PanAPT system information at any time to add other system information such as Approval Category Descriptions and Retrieve Options.

2. Add a user to CA PanAPT.

You can have several user IDs available to test authorization requirements.

Process Test Library Code

If you are familiar with processing test Library Codes, perform the following steps. If you are not familiar with processing test Library Codes, for more information see the *Reference Guide*.

To process test library codes

1. Add a Library Code using the test PDS libraries created.

Use the PDS member existence exit (APAS0200) and a model specification of INCLUDE APJMPDS.

2. Require approvals and enable inventory assignment and Retrieve when you set up the Library Code.

Use a Retrieve model specification of INCLUDE APJCPDS; INCLUDE APJCMSGs.

Note: Add a STEPLIB statement to model APJCMSGs to point to the CA PanAPT loadlib, CAI.CABYLOAD.

Process Test Inventory Records

If you are familiar with processing test Inventory Records, perform the following steps. If you are not familiar with processing test Inventory Records, for more information, see the *Reference Guide*.

To process test inventory records

1. Add an Inventory Record for one of the members of the Library Code you created in when processing test library code.
2. Assign the Inventory Record to yourself.
3. Retrieve the member and make sure it is copied to your test library.

Create a Move Request

If you are familiar with test Move Requests, perform the following steps. If you are not familiar with test Move Requests, for more information see the *Reference Guide*.

To create a move request

1. Add a Move Request using the Library Code and the members you placed in the test PDSs.
2. Schedule the move for today's date.
3. Close the Move Request.
4. Approve the Move Request.
5. Browse the Move Request (perform an inquiry on it).

This completes the basic online verification.

Edit Members in CAI.CABYDATA

You can modify a member in CAI.CABYDATA:

To modify member APJMJBST

1. Change all <SPFX> to the value specified for CAI.
2. Add any accounting information to the job statement that is necessary at your site.

Edit Members in CAI.CABYJCL

You can modify the JCL required to run the CA PanAPT move cycle, members APJJ5310 and APJJ5320. Use the following guidelines when modifying any member in CAI.CABYJCL to conform to your site's standards and file names. These members contain the jobs that perform the moves, create CA PanAPT reports, and support the CA PanAPT system. You modify the balance of the members later on in Phase Three.

To modify the JCL

1. Perform the following global change commands:
 - Change all <SPFX> to the value specified for CAI.
 - Change all <VPFX> to the value specified for CAI.
 - Change all <OPFX> to the value specified for CAI.

2. Change the JOB statement to conform to your site's standards.

- All jobs have null accounting parameters. Your standards might require valid values.
- All production jobs use MSGCLASS=J, TYPRUN=HOLD, and CLASS=P in the job statement. Change these to your site's standards.
- All jobs use default time and line limits. A larger value might be required if your defaults are small.
- Most jobs use the default region size. A larger value might be required if your default region size is small. The maximum region size required by CA PanAPT steps is 2048K.

Note: It might be convenient for you to create a member called JOBCARD in the CABYJCL that contains valid job statement parameters. You can insert this job statement at the beginning of any JCL member and delete the job statements supplied with CA PanAPT.

3. Override SYSOUT classes in the JCL, if necessary. By default, all jobs:

- Send their production reports to class P by the REPORT symbolic procedure parameter.
- Send any dumps to the class specified on the job PARM MSGCLASS by the DUMPS symbolic procedure parameter (DUMPS=*).
- Send all other SYSOUT data (such as sort messages and record counts) to the class specified on the job PARM MSGCLASS by the JCLLIST symbolic procedure parameter (JCLLIST=*).

If these classes are not satisfactory, override them in the JCL rather than change the cataloged procedures. The installation of later releases of CA PanAPT is easier if PROCs remain unchanged since they can then be replaced as a unit in later releases.

4. Add the LE/390 COBOL compiler runtime library to the link list, if necessary. If it is not in the link list and you cannot add it to the link list, add it to the JOBLIB DD for each job.

5. Complete the following modifications in CAI.CABYJCL. Follow general CAI.CABYJCL editing guidelines.

- Modify member APJJ5310. Include the character corresponding to your Move Request cycle in the selection criteria for program APCSS310. You must specify this same character as the Move Type on each Move Request. The default Move Type is M.

Remember that you can have two Move Requests ready for selection, but if they have different Move Types, APJJ5310 might select one without selecting the other.

- Modify member APJJ5320.

Verify Batch System

To verify batch system portion of CA PanAPT

1. Run job APJJ5310 from CABYJCL to select the Move Request you created.
If the Move Request is not selected, make sure its status is Approved for QA. Only approved Move Requests can be selected. Also make sure the next move date is the current date or earlier, or blank. Make any necessary corrections to the Move Request and rerun APJJ5310.
2. Run job APJJ5320 from CABYJCL to move the members in the selected Move Request.
3. Approve the Move Request for production and rerun the above two steps if your Move Request now needs to be moved to production (that is, you are using QA libraries).
4. If you specified to delete members from old libraries following a move, verify that the members have been moved to the production libraries and deleted from the old libraries by reviewing the job output and directory listings of the libraries.

When you complete this step, the installation process is complete.

Complete Installation Checklist

Use the following steps as a checklist to complete CA PanAPT installation:

1. Complete Editing Members in CABYJCL.
2. Edit Members in CABYPENU (Optional).
3. Edit Members in CABYSKL0.
4. Edit Members in CABYPARM.
5. Back Up CA PanAPT Files.
6. Test Complete CA PanAPT System.
7. Improve Initial Entry Performance.
8. Implement Move Cycles.
9. Implement Purge Move Request Processing.
10. Implement Security Event Exit.
11. Implement MSL Exits.
12. Implement External Security Rules.

Complete Editing Members in CABYJCL

Modify all of the remaining members in CAI.CABYJCL whose names begin with APJJ.

To modify all the remaining members in CAI.CABYJCL

Using the general editing guidelines for CAI.CABYJCL members as outlined in the Edit Members in CAI.CABYJCL section.

Take caution not to reduce the REGION parameter on any of the JOB statements.

Edit Members in CABYJCL (Optional)

To modify members in CABYJCL:

1. Modify member APIP200.

This panel is used to print a hard copy of a Move Request.

2. Change it to support all SYSOUT classes and destinations used when printing Move Request forms.

These SYSOUT classes and destinations are the defaults used when the user first sees the panel.

You can then modify those fields as desired. Follow the instructions contained in APIP200.

Edit Members in CABYSKLO

Complete the following modifications in CABYSKLO. Follow general CABYJCL editing guidelines.

To modify member APIK200:

1. Change this skeleton to conform to your JCL standards and file names.

Fields that might need to be changed are marked with <VPFX> and <SPFX>; these should match the value selected for CAI.

2. Add it to the JOBLIB DD, if your LE/390 COBOL compiler runtime library is not in the link list.

Edit Members in CABYPARM (CA Panvalet Users Only)

To edit members in CABYPARM

1. Modify member APJRRDSN.
 - Change <PVLOAD> to the data set name of your CA Panvalet load library.
 - Change <APTLOAD> to the data set name of your CA PanAPT load library.
2. Modify member APJR5423.
 - Change <PVVERSION> to the version of CA Panvalet you have installed. This should be in the format VV.R where VV is the version and R is the release, for example 14.2.
 - Change <MDSCB> to the name of your model DSCB used to create new generations of a GDG (as described in Step 4 of Phase One of the installation).
3. Review the REXX variables and change them if necessary.
 - PfUnit
 - PfDcb
 - TMSParm

Back Up CA PanAPT Files

To backup your CA PanAPT files

Run the APJJBKUP job every night.

Running the APJJBKUP job guards your CA PanAPT files from any type of hardware or software failure.

To recover from a hardware or software failure

Use CABYJCL member APJJREST to restore your CA PanAPT files to their status at the time of the prior backup.

See instructions in APJJREST for additional information.

Test Complete CA PanAPT System

Now that you have completed all of the required installation modifications, test all of the capabilities of the CA PanAPT system. Use the test plan outline below to ensure that you have correctly loaded all the components from the installation tape, and that you have made all necessary installation modifications. This testing also allows you to become more familiar with the functions of CA PanAPT.

Note: You have modified your system to handle only PDS moves. See the *CA PanAPT Reference Guide* for more information about how to handle other types of moves.

Test Plan

Because each site has its own testing procedures and standards, you must decide what to test and how to test. The following is a list of general guidelines for developing a test plan:

1. Define Move Requests with many different members and Library Codes. Include various combinations of members and Library Codes.
2. Define a large group of Move Requests, all to be moved at the same time.
3. Perform the batch jobs that physically move the members. Study all reports and verify that all CA PanAPT status updates are correct.
4. Use the Modeling Facility. Modify copies of the supplied models and write your own to perform some of your site's unique processing requirements for member movement into production libraries.
5. Use the Retrieve Facility. Modify copies of the supplied Retrieve models. Write models of your own to meet your site's unique requirements.
6. Run all of the reports. Specify all parameters for each report.

When you complete your testing and are satisfied that CA PanAPT is working as documented, you have completed the installation.

You are now ready to begin using CA PanAPT to move members into your production libraries.

Implement Move Cycles

CA PanAPT lets you process multiple move processing cycles concurrently. With the Move Type field, you control the processing cycle of a Move Request.

To create a move cycle, perform the following procedure:

1. Determine which Move Type values are to be part of a cycle.
2. Assign an ID for this cycle. The ID can be from one to eight characters long and can be as simple as the single-character Move Type. The ID must conform to OS/390 JCL naming conventions for a node name that is part of a data set name.
3. Create a copy of each of the move processing batch jobs (APJJ5310, APJJ5311, and APJJ5320).
4. In jobs APJJ5310 and APJJ5311, change the parameter MPC in procedure APJP5310 to include only the Move Types that define this cycle (for example, MPC='MBX').
5. In all jobs, change the parameter MMPCPFX for each of the procedures used in the job to specify the ID that was assigned to this move cycle in Step 2. For example, job APJJ5310 uses procedures APJP5310 and APJP5391. Specify MMPCPFX='ID' in each procedure.

For information on parameters MPC and MMPCPFX, see the *Reference Guide*.

Chapter 7: Deploying Your Product

We recommend that you deploy your product according to your site-specific requirements. If you have questions, contact us at <http://ca.com/support>.

This section contains the following topics:

[Improve Initial Entry Performance](#) (see page 187)

Improve Initial Entry Performance

Enter CA PanAPT by executing the APT CLIST that is delivered with the CA PanAPT system. This CLIST allocates the CA PanAPT system libraries (with the installation defaults specified in the CLIST) and passes control to APCS1000, the main online CA PanAPT module. When you exit CA PanAPT, the CLIST will deallocate the system libraries. Using this APT CLIST lets you switch to an alternate CA PanAPT system (if you are using more than one) when you enter CA PanAPT.

You can speed up the performance of entering CA PanAPT (but also limit your flexibility of being able to switch CA PanAPT systems on demand) by making the following changes:

1. Change the TSO logon PROC or TSO CLIST you use to allocate the ISPF and CA PanAPT software libraries to also allocate the CA PanAPT VSAM system libraries. The files you must allocate are:

```
//APTDDB      DD DISP=SHR,DSN=<VPFX>.APTDDB  
//APTMODEL    DD DISP=SHR,DSN=<SPFX>.CABYDATA
```
2. Change the ISPF panel you use to select the CLIST APT to select the program APCS1000 as follows:
 - In the)PROC section, ensure that variable &ZTRAIL is set to .TRAIL before variable &ZSEL is set. In many cases, it is set after variable &ZSEL is set. If this is the case, move the assignment statement. Panel APIPPRIM shows the proper way if you are in doubt.
 - Change the entry for option A in the &ZSEL assignment to:

```
A, 'PGM(APCS1000) NEWAPPL(APT) PARM(&ZTRAIL) NOCHECK'
```


Chapter 8: Configuring Your Product

This chapter describes the minimum configuration tasks needed before CA PanAPT can be started, customized, and used in your environment.

This section contains the following topics:

[Implement Purge Move Request](#) (see page 189)

[Implement Security Event Exit](#) (see page 189)

[Implement MSL Exits](#) (see page 190)

[Implement External Security Rules](#) (see page 190)

Implement Purge Move Request

The Move Request purge programs (APCS5950 and APCS5955) can be used together with a CA PanAPT history file to migrate old Move Requests from the pending file. However, use of these programs and the creation of the history VSAM file are optional.

In Phase One, you modified the installation JCL and chose whether to create the APTHIST file. You must have a created history file to implement the Purge Move Requests feature.

Make sure that CABYPROC member APJPBKUP agrees with your decision about the history file. In Phase Two, Step 8, you edited CABYPROC members. Therefore, you should have set the HISTFL= parm in APJPBKUP to zero if you are implementing the Purge Move Request feature or to one if you are not.

Implement Security Event Exit

External security can be implemented in several ways. You may want to use CA PanAPT/UIF's logon system IDs to allow access to CA PanAPT and CA PanAPT activities. Or you may just implement the CA PanAPT activity access rules, defaulting the system ID in the rules. You can also mix and use a combination of both logon system IDs with the CA PanAPT activity access rules.

In Phase One you updated your security system to allow access for standard security checks. Following are the SSF rules to further restrict or allow access to CA PanAPT and CA PanAPT/UIF activities.

Implement MSL Exits

Implement the supplied sample CA Librarian, CA Panvalet or PDS Member Selection List (MSL) exit programs. These exits provide support for building MSLs based on the contents of the libraries defined to your Library Codes. You can also create your own exits to support other types of libraries. (See Appendix B, "User Exits," in the *CA PanAPT Administrator Guide* for complete documentation.)

Implement External Security Rules

External security can be implemented in several ways. You may want to use CA PanAPT/UIF's logon system IDs to allow access to CA PanAPT and CA PanAPT activities. Or you may just implement the CA PanAPT activity access rules, defaulting the system ID in the rules. You can also mix and use a combination of both logon system IDs with the CA PanAPT activity access rules.

CA PanAPT Activity Access

When users attempt functions in CA PanAPT, CA PanAPT validates external security first (and if authorization is granted) then validates the internal security system (set up through Control File Maintenance). If authorization is not granted during external security validation, a security error appears and the function is not allowed.

Set up security rules as defined in the following table and set up permits (as applicable) according to your site standards.

An example of a Standard Security Facility (SSF) rule follows:

```
PANAPTF.system-id.CTLSYS.SYSINFO.CHG
```

where:

- PANAPTF is your high-level ownership in CA Top Secret or your key in CA-ACF2.
- *system-id* is the logon system ID when using the User Identification Facility (UIF). If the UIF is not being used, CA PanAPT puts in a dollar sign (\$) as the default.
- CTLSYS is the activity name.

- SYSINFO is the record type.
- CHG is the action.

Activity Name	Description and SSF Rule
CTL/ENTRY	Control file maintenance entry: PANAPTF. <i>system-id</i> .CTL
CTLACT/CHG	Control file activity change: PANAPTF. <i>system-id</i> .CTLACT. <i>activity-name</i> .CHG
CTLACT/INQ	Control file activity inquire: PANAPTF. <i>system-id</i> .CTLACT. <i>activity-name</i> .INQ
CTLSYS/ADD	Control file system information add (for adding CA Pan/LCM Configuration Manager Option information): PANAPTF. <i>system-id</i> .CTLSYS.ACCSMTHD.ADD PANAPTF. <i>system-id</i> .CTLSYS.CONFIG.ADD
CTLSYS/CHG	Control file system information change: PANAPTF. <i>system-id</i> .CTLSYS.SYSINFO.CHG PANAPTF. <i>system-id</i> .CTLSYS.SECURITY.CHG PANAPTF. <i>system-id</i> .CTLSYS.VERPROCS.CHG PANAPTF. <i>system-id</i> .CTLSYS.LIBLEVEL.CHG PANAPTF. <i>system-id</i> .CTLSYS.ACCSMTHD.CHG PANAPTF. <i>system-id</i> .CTLSYS.CONFIG.CHG
CTLSYS/DEL	Control file system information delete (for deleting CA Pan/LCM Configuration Manager Option information): PANAPTF. <i>system-id</i> .CTLSYS.ACCSMTHD.DEL PANAPTF. <i>system-id</i> .CTLSYS.CONFIG.DEL
CTLSYS/INQ	Control file system information inquire: PANAPTF. <i>system-id</i> .CTLSYS.SYSINFO.INQ PANAPTF. <i>system-id</i> .CTLSYS.SECURITY.INQ PANAPTF. <i>system-id</i> .CTLSYS.VERPROCS.INQ PANAPTF. <i>system-id</i> .CTLSYS.LIBLEVEL.INQ PANAPTF. <i>system-id</i> .CTLSYS.ACCSMTHD.INQ PANAPTF. <i>system-id</i> .CTLSYS.CONFIG.INQ
CTLUSER/ADD	Control file user ID add: PANAPTF. <i>system-id</i> .CTLUSER. <i>user-id</i> .ADD
CTLUSER/CHG	Control file user ID change: PANAPTF. <i>system-id</i> .CTLUSER. <i>user-id</i> .CHG
CTLUSER/DEL	Control file user ID delete: PANAPTF. <i>system-id</i> .CTLUSER. <i>user-id</i> .DEL

Activity Name	Description and SSF Rule
CTLUSER/INQ	Control file user ID inquire: PANAPTF.system-id.CTLUSER.user-id.INQ
DEV/ENTRY	Development facility entry: PANAPTF.system-id.DEV
DEV/MM	Development modify members command: PANAPTF.system-id.DEV.MM
DEV/PRINTTBL	Development print move request member table: PANAPTF.system-id.DEV.PRINTTBL
DEVADMIN/ENTRY	Project administration entry: PANAPTF.system-id.DEVADMIN
INVENTORY/ADD	Inventory add: PANAPTF.system-id.INVENTORY.name.ADD
INVENTORY/APP	Inventory approve: PANAPTF.system-id.INVENTORY.name.APP
INVENTORY/ASN	Inventory assign: PANAPTF.system-id.INVENTORY.name.ASN
INVENTORY/CHG	Inventory change: PANAPTF.system-id.INVENTORY.name.CHG
INVENTORY/DEL	Inventory delete: PANAPTF.system-id.INVENTORY.name.DEL
INVENTORY/ENTRY	Inventory maintenance entry: PANAPTF.system-id.INVENTORY
INVENTORY/INQ	Inventory inquire: PANAPTF.system-id.INVENTORY.name.INQ
INVENTORY/REL	Inventory release: PANAPTF.system-id.INVENTORY.name.REL
INVENTORY/RET	Inventory assign and retrieve: PANAPTF.system-id.INVENTORY.name.RET
INVENTORY/TRN	Inventory transfer: PANAPTF.system-id.INVENTORY.name.TRN
LIBCODE/ADD	Library code add: PANAPTF.system-id.LIBCODE.libcode/subcode.ADD

Activity Name	Description and SSF Rule
LIBCODE/CHG	Library code change: PANAPTF. <i>system-id</i> .LIBCODE. <i>libcode/subcode</i> .CHG
LIBCODE/COP	Library code copy: PANAPTF. <i>system-id</i> .LIBCODE. <i>libcode/subcode</i> .COP
LIBCODE/DEL	Library code delete: PANAPTF. <i>system-id</i> .LIBCODE. <i>libcode/subcode</i> .DEL
LIBCODE/ENTRY	Library code maintenance entry: PANAPTF. <i>system-id</i> .LIBCODE
LIBCODE/INQ	Library code inquire: PANAPTF. <i>system-id</i> .LIBCODE. <i>libcode/subcode</i> .INQ
LIBCODE/SECURITY	Library code view security codes: PANAPTF. <i>system-id</i> .LIBCODE. <i>libcode/subcode</i> .SECURITY
MEMBER/BROWSE	Browse a member: PANAPTF. <i>system-id</i> .MEMBER. <i>member-name</i> .BROWSE
MEMBER/CHECKIN	Checkin a member: PANAPTF. <i>system-id</i> .MEMBER. <i>member-name</i> .CHECKIN
MEMBER/CHECKOUT	Checkout a member: PANAPTF. <i>system-id</i> .MEMBER. <i>member-name</i> .CHECKOUT
MEMBER/COMPARE	Compare members: PANAPTF. <i>system-id</i> .MEMBER. <i>member-name</i> .COMPARE
MEMBER/COMPILE	Compile a member: PANAPTF. <i>system-id</i> .MEMBER. <i>member-name</i> .COMPILE
MEMBER/COMPLINK	Compile and link a member: PANAPTF. <i>system-id</i> .MEMBER. <i>member-name</i> .COMPLINK
MEMBER/EDIT	Edit a member: PANAPTF. <i>system-id</i> .MEMBER. <i>member-name</i> .EDIT
MEMBER/HISTORY	View member history: PANAPTF. <i>system-id</i> .MEMBER. <i>member-name</i> .HISTORY
MEMBER/LINK	Link edit a member: PANAPTF. <i>system-id</i> .MEMBER. <i>member-name</i> .LINK
MEMBER/LISTING	View a member's output listing: PANAPTF. <i>system-id</i> .MEMBER. <i>member-name</i> .LISTING

Activity Name	Description and SSF Rule
MEMBER/MERGE	Merge members: PANAPTF. <i>system-id</i> .MEMBER. <i>member-name</i> .MERGE
MEMBER/OUTPUTCP	View member compare output: PANAPTF. <i>system-id</i> .MEMBER. <i>member-name</i> .OUTOUTCP
MEMBER/OUTPUTMG	View member merge output: PANAPTF. <i>system-id</i> .MEMBER. <i>member-name</i> .OUTOUTMG
MEMBER/UTILITY	Member utilities: PANAPTF. <i>system-id</i> .MEMBER. <i>member-name</i> .UTILITY
MEMBER/XIR	View member cross reference: PANAPTF. <i>system-id</i> .MEMBER. <i>member-name</i> .XIR
MOVEREQ/ADD	Move request add: PANAPTF. <i>system-id</i> .MOVEREQ. <i>number</i> .ADD
MOVEREQ/APB- <i>short-name</i>	Move request approve for back out at level short-name: PANAPTF. <i>system-id</i> .MOVEREQ. <i>number</i> .APB- <i>short-name</i>
MOVEREQ/APM- <i>short-name</i>	Move request approve for move at level short-name: PANAPTF. <i>system-id</i> .MOVEREQ. <i>number</i> .APM- <i>short-name</i>
MOVEREQ/BAK	Move request back out: PANAPTF. <i>system-id</i> .MOVEREQ. <i>number</i> .BAK
MOVEREQ/BRO	Move request browse: PANAPTF. <i>system-id</i> .MOVEREQ. <i>number</i> .BRO
MOVEREQ/CHG	Move request change (for move requests being created): PANAPTF. <i>system-id</i> .MOVEREQ. <i>number</i> .CHG
MOVEREQ/CHGAWAPP	Move request change (for move requests awaiting approvals): PANAPTF. <i>system-id</i> .MOVEREQ. <i>number</i> .CHGAWAPP
MOVEREQ/CLO	Move request close: PANAPTF. <i>system-id</i> .MOVEREQ. <i>number</i> .CLO
MOVEREQ/CLOASSGN	Move request assignment test at close: PANAPTF. <i>system-id</i> .MOVEREQ. <i>number</i> .CLOASSGN
MOVEREQ/COP	Copy move request: PANAPTF. <i>system-id</i> .MOVEREQ. <i>number</i> .COP
MOVEREQ/CR	Copy a move request for rework: PANAPTF. <i>system-id</i> .MOVEREQ. <i>number</i> .CR

Activity Name	Description and SSF Rule
MOVEREQ/DAT	Move request change date: PANAPTF. <i>system-id</i> .MOVEREQ. <i>number</i> .DAT
MOVEREQ/DEL	Move request change date: PANAPTF. <i>system-id</i> .MOVEREQ. <i>number</i> .DEL
MOVEREQ/DELCLOSD	Move request delete (for closed move requests): PANAPTF. <i>system-id</i> .MOVEREQ. <i>number</i> .DELCLOSD
MOVEREQ/ENTRY	Move request maintenance entry: PANAPTF. <i>system-id</i> .MOVEREQ
MOVEREQ/INQ	Move request inquire: PANAPTF. <i>system-id</i> .MOVEREQ. <i>number</i> .INQ
MOVEREQ/MEMBER	Move request member add: PANAPTF. <i>system-id</i> .MOVEREQ. <i>number</i> .MEMBER. <i>member-name</i>
MOVEREQ/MEMCHG	Move request member change: PANAPTF. <i>system-id</i> .MOVEREQ. <i>number</i> .MEMCHG. <i>member-name</i>
MOVEREQ/MEMDEL	Move request member delete: PANAPTF. <i>system-id</i> .MOVEREQ. <i>number</i> .MEMDEL. <i>member-name</i>
MOVEREQ/MEMPURGE	Move request member purge: PANAPTF. <i>system-id</i> .MOVEREQ. <i>number</i> .MEMPURGE. <i>member-name</i>
MOVEREQ/PRT	Move request print: PANAPTF. <i>system-id</i> .MOVEREQ. <i>number</i> .PRT
MOVEREQ/RVP	Move request run verification: PANAPTF. <i>system-id</i> .MOVEREQ. <i>number</i> .RVP
MOVEREQ/STA	Move request status: PANAPTF. <i>system-id</i> .MOVEREQ. <i>number</i> .STA
PROJECT/ADD	Add a project: PANAPTF. <i>system-id</i> .PROJECT. <i>project</i> .ADD
PROJECT/CHG	Change a project: PANAPTF. <i>system-id</i> .PROJECT. <i>project</i> .CHG
PROJECT/DEL	Delete a project: PANAPTF. <i>system-id</i> .PROJECT. <i>project</i> .DEL
PROJECT/INQ	Project inquiry: PANAPTF. <i>system-id</i> .PROJECT. <i>project</i> .INQ

Activity Name	Description and SSF Rule
REPORT/APCS5105	Online approval group cross reference report: PANAPTF. <i>system-id</i> .REPORT.APCS5105
REPORT/APCS5104	Online approval category cross reference report: PANAPTF. <i>system-id</i> .REPORT.APCS5104
REPORT/APCS6111	Online assignment report: PANAPTF. <i>system-id</i> .REPORT.APCS6111
REPORT/ENTRY	Online report entry: PANAPTF. <i>system-id</i> .REPORT
USERLIB/CHG	Change user work libraries: PANAPTF. <i>system-id</i> .USERLIB. <i>user-id</i> .CHG
USERLIB/INQ	User work library inquiry: PANAPTF. <i>system-id</i> .USERLIB. <i>user-id</i> .INQ

CA PanAPT/UIF Security

If you want to use external security with CA PanAPT/UIF, the following table shows how to build the security rules for the type of security you want to activate.

In this table, PANAPTU is your high-level ownership in CA Top Secret or your key in CA ACF2.

Activity Name	Description/SSF Rule
Force UIF usage	CA PanAPT logon system ID required: PANAPTU.PANAPT
Authorize system ID	Authorize logon system ID entered: PANAPTU.PANSYSID. <i>system-id</i>
Authorize UIF usage	Authorize usage of UIF (creating or changing): PANAPTU.PANUIF

Chapter 9: Conversion

This chapter describes the steps necessary to convert your CA PanAPT system to the current release. If you are installing CA PanAPT for the first time or are already using Release 3.0, no conversion to Release 3.1 is necessary. Therefore, you can skip this chapter entirely.

WARNING! The conversion process supports converting only from CA PanAPT Releases 1.3 and 2.0.

This chapter refers to the following terms:

Site-specific Modifications/Customizations:

Changes you make that alter the manner in which CA PanAPT was designed to work. These modifications are usually made to accommodate unique processing requirements that CA PanAPT does not handle. An example of a site-specific modification is changing one of the cataloged procedures to perform an additional step (or perhaps to skip a step).

Back Out:

To begin using your current CA PanAPT system again as your production turnover system.

Dual Maintenance:

While converting non-critical parts of CA PanAPT, you can continue to use the old CA PanAPT version. However, the data that is updated on your old system must also be updated on the new CA PanAPT system to ensure that the new system is consistent with the old system.

This section contains the following topics:

[Conversion Procedures](#) (see page 198)

[Conversion Checklist](#) (see page 198)

[Determine CA PanAPT Customizations](#) (see page 200)

[Install CA PanAPT](#) (see page 200)

[Reimplement Customization Into CA PanAPT](#) (see page 201)

[Convert Database](#) (see page 203)

[Complete Conversion](#) (see page 205)

[Convert History](#) (see page 206)

[Complete Testing with Test Move Requests](#) (see page 207)

[Conversion Cleanup](#) (see page 207)

Conversion Procedures

The conversion of your CA PanAPT system to Release 3.2 consists of several steps as outlined in this chapter. By following these steps, you can convert to this new release of CA PanAPT.

While you are setting up for the conversion and during most of the conversion process, you can continue to run your production CA PanAPT system. You must follow certain steps if you want to run your old CA PanAPT system while going through the conversion process. These steps are outlined later in this chapter.

Important! You must read this entire chapter before attempting to convert your CA PanAPT system.

This is a guide only. It highlights the changes that you must consider. Some steps that your installation must take due to site-specific requirements might not be covered in this chapter.

In general, complete the tasks in the order listed.

Conversion Checklist

This is a checklist of the steps to follow in the CA PanAPT Release 3.2 conversion. To ensure a successful conversion, you must follow the steps in sequence as they appear in the checklist. Check off each step upon completion.

When this process is completed, you will have a working CA PanAPT 3.2 system.

Important! Read this entire "Conversion" chapter before beginning the conversion process.

1. Determine all customizations of CA PanAPT distributed source made at your site:
 - CABYJCL
 - CABYPROC
 - CABYPARM
 - CABYDATA
 - CABYPENU
 - CABYSKLO
 - CABYCLSO
2. Complete the CA PanAPT installation for the new release including system verification steps (see next step also).

3. Reimplement any desired customizations in the new CA PanAPT distributed source.
 - a. Make source module changes:
 - CABYJCL
 - CABYPROC
 - CABYPARM
 - CABYDATA
 - CABYPENU
 - CABYSKLO
 - CABYCLSO
 - b. Update user exit, if used.
 - c. Update your security package (CA Top Secret, CA ACF2, RACF, and so forth).
 - d. Update any scheduling package (CA 7 Workload Automation, and so forth).
 - e. Complete system modifications.
 - f. Set symbolic parameters.
4. Convert database.
 - a. Tailor CABYJCL member #PJJCNDB.
 - b. Tailor CABYJCL member #PJJBLDB.
 - c. Verify conversion.
 - d. Complete testing.
5. Complete conversion.
 - a. Shut down the current CA PanAPT system.
 - b. Disallow online functions.
 - c. Complete batch functions.
6. Convert history.
 - a. Tailor CABYJCL member #PJJCHS1.
 - b. Tailor CABYJCL member #PJJCHS2.
7. Complete testing with test move requests.
8. Conversion cleanup.
 - a. Clean up test data.
 - b. Back up new CA PanAPT VSAM file to GSGs.
 - c. Clean up scheduling and security packages.
 - d. Clean up old system.

Determine CA PanAPT Customizations

Your current CA PanAPT system might be heavily tailored to your environment.

You must identify the changes you have made to each CA PanAPT product component to change the new CA PanAPT version of that product component accurately. You might not require all your old modifications.

A comparator utility is the most accurate method to determine the changes to each modified distributed CA PanAPT component.

If your site has CA Panvalet installed, you can use CA Panvalet PCOMPARE to compare your Production components with the original CA PanAPT components. See the *CA Panvalet Compare Reference Guide* for details.

These are some of the libraries that you might have customized. To ensure that you find all customizations, be sure to check all libraries.

- CABYJCL
- CABYPROC
- CABYPARM
- CABYDATA
- CABYPENU
- CABYSKLO
- CABYCLSO

Install CA PanAPT

Install CA PanAPT using the appropriate instructions. Create all new data sets for this installation.

Test CA PanAPT for functionality as outlined previously in this guide. This step lets you become familiar with the new version of CA PanAPT and the differences from the previous version.

Do not attempt to convert your VSAM files to test with live data at this time.

Reimplement Customization Into CA PanAPT

Now that you have completed the installation and have tested the new version for functionality, most of your customizations have probably been made. You might want to make additional site-specific changes to make CA PanAPT work the same way as your current CA PanAPT system. Examples of these types of additional modifications are:

- Override data set names when invoking cataloged procedures.
- Determine how many move processing cycles you want to run, create individual move processing jobs for each cycle, and override the MMPCPF parameter appropriately for each job cycle.
- Change the APT CLIST to perform additional preprocessing before entering CA PanAPT
- You can also eliminate the APT CLIST entirely and invoke CA PanAPT directly.
- Change the Retrieve models for the changes made to modeling keywords for consistency between retrieve and normal move processing.

Make Source Changes

Complete any changes to the distributed source modules using the list of changes you have generated to assist in reimplementing these changes.

These are some of the libraries that you might want to re-customize:

- CABYJCL
- CABYPROC
- CABYPARM
- CABYDATA
- CABYPENU
- CABYSKLO
- CABYCLSO

Update User Exits

If your site used the Inventory-Edit or the Member-Existence Exits in a previous release, you must update the exits because the record layouts and record layout field names might have changed.

Source and executable code for the sample exits that are provided on the installation tape are listed in the following table:

Exit Name	Library Type
APAS0200	PDS member existence
APCS0221	CA Librarian member existence
APAS0222	CA Panvalet member existence
APAS0223	CA Panexec member existence
APAS0226	CA Telon TDF member existence
APCS0304	Inventory edit
APCS0401	Security
APAS0600	CA Panvalet MSL
APAS0610	PDS MSL
APAS0620	CA Librarian MSL
APCS1410	PDS browse
APCS1420	PDS edit

Update Security Package

If your installation uses a security package (such as CA ACF2, CA Top Secret, RACF) to control access to your production libraries, CA PanAPT VSAM data sets, and so forth, you must update your security definitions, rules, and so forth to allow the new CA PanAPT system to have the same access as your current system.

You might need to make additional updates to your security package to account for new jobs you want to run and new data sets that are accessed for different move cycles.

Update Scheduling Package

If your installation uses a scheduling package (such as CA 7 Workload Automation) to submit your CA PanAPT batch jobs, you must add scheduling definitions, rules, and so forth to allow the new CA PanAPT system to be controlled in the same way as your current system.

You might need to make additional updates to your scheduling package to account for new jobs you want to run and new data sets that are accessed for different move cycles.

Complete System Modifications

If there are any other changes that we have not provided for in this conversion guide, you can make them at this point. If you do not have any additional changes to make, you have completed the system modifications.

Now, you have installed, customized, and tested CA PanAPT. In addition, you have set up your security and scheduling systems (if any) to allow the new CA PanAPT to work the same as the old release. The next conversion step is to begin converting the CA PanAPT VSAM files.

Symbolic Parameters

There are two symbolic parameters found in the instream procedures of the conversion JCL. These symbolic parameters are set as follows:

Symbolic Parameter	Release Version
CVRT13=1	To convert from Release 1.3.
CVRT20=1	To convert from Release 2.0.

Convert Database

Follow these steps to convert your CA PanAPT VSAM data sets to Version 3.2.

1. Tailor CABYJCL member #PJCNDDB.
2. Tailor CABYJCL member #PJJBLDB.
3. Verify conversion.

Tailor CABYJCL Member #PJCNDB

The first step is to tailor the CABYJCL member #PJCNDB. This job reads the data on your production file. Follow normal CABYJCL tailoring guidelines as described in the installation procedures except for the VSAM prefix, <VPF0>. <VPF0> must be set to the VSAM prefix for your current CA PanAPT production system. After you complete the tailoring, submit the job. This job creates a single flat file in the new format.

Tailor CABYJCL Member #PJBLDB

The second step is to tailor the CABYJCL member #PJBLDB, if you have not tailored it already. This step writes data to your new CA PanAPT 3.2 file. Follow normal CABYJCL tailoring guidelines as described in the installation procedures.

Note: Do not use your current CA PanAPT <VPFX> VSAM prefix. Use of it results in destruction of your current CA PanAPT production file.

The member APJRDB also must be updated with the new VSAM data set name and the volume on which it is located. The APJRDB member is located on the new distributed CABYPARM.

After you complete the tailoring, submit the job. This job takes the flat file in the new format and restores to the new APTDB file, as specified using CA PanAPT Version 3.2 <VPFX>.

Verify Conversion

After the conversion jobs have run, a new VSAM database is available. Submit CABYJCL member APJJ5103 to print the control contents of this file. Review the reports for correctness. If you must make additional modifications, you can use the online CA PanAPT commands to complete them. To check the contents of the inventory portion of the database, submit job APJJ6111 to print the reports on the contents of this file. Review these reports for correctness. To check the Library Code segment of the file, submit job APJJ5102 to print reports on the contents of this file. Review these reports for correctness. Finally, to check the pending portion of this new database, submit jobs APJJ5111 and APJJ5112 to print the reports on the contents of this file. Review these reports for correctness.

Remember, your old system is still your production turnover system. Any changes made to the old file are not reflected in the new APTDB file unless you make the corresponding changes to the new file yourself. This dual maintenance is necessary until you make the new CA PanAPT your production turnover system.

Complete Conversion

Up to this point, you have converted CA PanAPT files and tested the new CA PanAPT system while still running your old version production turnover system. You are performing dual maintenance on the old APTDB file or APTCTL, APTLIBC, APTDIBS, and APTPEND files, and the new APTDB file. To finish the conversion and testing, you must shut down and de-activate the old system. If you decide to put the new CA PanAPT version into production after the final testing, it is ready to use.

If you decide to put the new CA PanAPT into production, you can back out to the old system. However, since the conversion programs convert only from the old version to the new, you cannot transfer any data entered during the final conversion back to the old system. Data entered on CA PanAPT during the conversion should not be production data unless you are willing to risk losing the data if you decide not to put the new CA PanAPT into production. To attempt the conversion and testing again, simply restart at this point.

You might want to do this final part of the conversion when no one is likely to want to use the online portion of the system. This minimizes any impact your conversion and testing have on your users and your production CA PanAPT system. This impact can be in the form of users waiting for you to re-activate the system, or having to re-key in any Move Requests made on the new version if you decide not to put it into production at the completion of your testing.

Shut Down the Current CAPanAPT System

You must shut down the current CA PanAPT system before attempting the final part of the conversion to minimize the chance of losing any CA PanAPT data that could be entered while the conversion and final testing take place. Shutting down is a two-step process, as follows:

1. Disallow online functions.
2. Complete batch functions.

Step 1: Disallow Online Functions

First, disallow the use of the online portion of the old CA PanAPT system. Do this by renaming the load module APCS1000 to XXX1000 in the old version CA PanAPT executable program library. This causes an 806abend error for anyone who tries to use the old CA PanAPT version. A variation of this technique is to rename the old version CA PanAPT CLIST. Alternatively, depending on how your site is configured, you might be able to simply disallow the use of signon authority for *DEFAULT in the old version to keep users from entering data.

Step 2: Complete Batch Functions

Second, successfully complete the batch portion of the new system. This clears any pending Move Requests and keeps them from being moved accidentally during your testing. Before running the batch cycle, run APJJ5111 to make sure that there are no approved Move Requests from the converted pending file that are scheduled to move during your testing period. If there are, use the CA PanAPT Change Date function to push back the move date so they move before this cycle. Or, push the move date forward so they move after the test period. If you do not change the move date, you should schedule a different time to complete the conversion and testing. Your system administrator should determine which action to take if there are moves scheduled during the conversion and testing time frame.

Do not move any real production software with CA PanAPT until you have decided to go into production with the new CA PanAPT system. You can enter test Move Requests on the CA PanAPT VSAM files that move test modules into your installation's production libraries. If you decide to back out, then you lose only test data.

Convert History

Follow these steps to convert the APTHIST file:

1. Tailor CABYJCL member #PJJCHS1.
2. Tailor CABYJCL member #PJJCHS2.
3. Verify conversion.

Note: Convert the control and Library Code files before the history file (APTHIST).

Tailor CABYJCL Member #PJJCHS1

The first step is to tailor the CABYJCL member #PJJCHS1. This step reads the data from your production file. Follow normal CABYJCL tailoring guidelines as described in the installation procedures except for the VSAM prefix, <VPF0>. <VPF0> must be set to the VSAM prefix for your current CA PanAPT production system. After you complete the tailoring, submit the job. This job creates a flat file in the new format.

Tailor CABYJCL Member #PJJCHS2

The second step is to tailor the CABYJCL member #PJJCHS2, if you have not tailored it already. This step writes data to your new CA PanAPT 3.2 file. Follow normal CABYJCL tailoring guidelines as described in the installation procedures.

Note: Do not use your current CA PanAPT <VPFX> VSAM prefix. Use of it results in destruction of your current CA PanAPT production file.

The member APJRHIST also must be updated with the new VSAM data set name and the volume on which it is located. The APJRHIST member is located on the new distributed CABYPARM.

After you complete the tailoring, submit the job. This job takes the flat file in the new format and restores it to the APTHIST file.

Verify Conversion

When the conversion jobs have run, you have a copy of the APTHIST file converted to the new format. Submit job APJJ5112 to print the reports on the contents of this file. (Be sure you have APTHIST specified in the job and not APTDB.) Review these reports for correctness.

Complete Testing with Test Move Requests

Now you have a converted copy of the CA PanAPT VSAM file and are ready to test your tailored CA PanAPT system.

Test the system according to your site's standards. This should include creating test Move Requests that move test modules into your production libraries.

If the new CA PanAPT meets your testing requirements and you decide to go live with CA PanAPT in production, the conversion is complete and only cleanup tasks remain. Ensure that your old system is completely de-activated.

If the new CA PanAPT does not meet your testing requirements or you are unable to complete your testing, simply back out to your old system by reversing whatever method you used to shut it down. When you are ready to test again, simply repeat the final conversion and testing (APTDB and APTHIST) until your testing requirements are satisfied.

Conversion Cleanup

Now that the conversion process is completed, a few things must be cleaned up as follows:

1. Clean up test data.
2. Back up new CA PanAPT VSAM file to GDGs.
3. Clean up scheduling and security packages.
4. Clean up old system.

Clean Up Test Data

If you have test data in your new production CA PanAPT files (from the testing that you performed), you probably want to clean it up. Likely candidates for cleanup might be Inventory Records, Library Codes, user IDs, and Move Requests. Use the CA PanAPT online functions to perform this cleanup.

Back Up New CA PanAPT VSAM File to GDGs

After you have cleaned up your CA PanAPT VSAM files (if necessary), back them up using CABYJCL member APJJBKUP. This member backs up the files to generation data groups (GDGs). The GDG indexes were initialized as part of the installation. If the indexes have not been initialized yet, run CABYJCL member #PJJDGDG to define the GDG indexes.

Run APJJBKUP every night to guard your CA PanAPT files from any type of hardware or software failure.

Back Up New CA PanAPT VSAM File to GDGs

After you have cleaned up your CA PanAPT VSAM files (if necessary), back them up using CABYJCL member APJJBKUP. This member backs up the files to generation data groups (GDGs). The GDG indexes were initialized as part of the installation. If the indexes have not been initialized yet, run CABYJCL member #PJJDGDG to define the GDG indexes.

Run APJJBKUP every night to guard your CA PanAPT files from any type of hardware or software failure.

Clean Up Scheduling and Security Packages

If you use any type of scheduling package or security package to control the processing of your old system, you can now remove and change any rules, definitions, and so on that apply to your old system because they no longer apply to your site. Now, these packages should all see the new CA PanAPT version.

Clean Up Old System

The last task is to clean up your old system. This includes deleting all of the software and control libraries and the VSAM files.

Before you delete any data sets, you might want to copy them to tape first, in case you need to refer to them in the future. There is no anticipated reason you would need to refer to them, as the data is now stored in the CA PanAPT files, but it might be standard practice at your site.

Appendix A: CA PanAPT DB2 Option

This section contains the following topics:

[Receiving the SMP/E Package](#) (see page 211)

[Clean Up the USS Directory](#) (see page 213)

[Apply Maintenance](#) (see page 215)

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 PanAPT. 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 AKASEDIT 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 AKASEDIT 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 AKASEDIT macro each time you open a new SAMPJCL member. To edit all SAMPJCL members simultaneously, read and follow the instructions in the AKAEDALL member.

2. Open the SAMPJCL member AKA1ALL in an edit session and execute the AKASEDIT macro from the command line.

AKA1ALL is customized.

3. Submit AKA1ALL.

This job produces the following results:

- The target and distribution data sets for CA PanAPT are created.
- Unique SMPLTS, SMPMTS, SMPSCDS, and SMPSTS data sets for this target zone are created.

4. Open the SAMPJCL member AKA2CSI in an edit session and execute the AKASEDIT macro from the command line.

AKA2CSI is customized.

5. Submit AKA2CSI.

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. Submit the *yourhlq*.SAMPJCL member AKA3RECD to receive SMP/E base functions.
CA PanAPT is received and now resides in the global zone.
2. Customize and submit the *yourhlq*.SAMPJCL member AKA4APP to APPLY SMP/E base functions.
Your product is applied and now resides in the target libraries.
3. Customize and submit the *yourhlq*.SAMPJCL member AKA5ACC to ACCEPT SMP/E base functions.
Your product is accepted and now resides in the distribution libraries.

Clean Up the USS Directory

Important! This procedure is optional. Do not use this procedure until you complete the entire installation process.

To free file system disk space for subsequent downloads after downloading and processing the pax files for your CA Technologies product, we recommend removing the files from your USS directory and deleting unnecessary MVS data sets. You can delete the following items:

- Pax file
- Product-specific directory that the pax command created and all of the files in it
- SMP/E RELFILES, SMPMCS, and HOLDDATA MVS data sets

These data sets have the HLQ that you assigned in the UNZIPJCL job.

Note: Retain non-SMP/E installation data sets such as *yourHLQ.INSTALL.NOTES* for future reference.

Follow these steps:

1. Navigate to your Pax-Enhanced ESD USS directory.

Your view is of the applicable USS directory.

2. Delete the pax file by entering the following command:

```
rm paxfile
```

paxfile

Specifies the name of the CA Technologies pax file that you downloaded.

The pax file is deleted.

3. Delete the product-specific directory by entering the following command:

```
rm -r product-specific_directory
```

product-specific_directory

Specifies the product-specific directory that the pax command created.

The product-specific directory is deleted.

Note: You can also use TSO ISHELL to navigate to the pax file and product-specific directory, and delete them using the D line command.

Apply Maintenance

CA Support Online may have maintenance and hold data that have been published since the installation data was created.

To apply maintenance

1. Check CA Support Online and download any PTFs and hold data published since this release was created.

2. Transfer the downloaded files to two separate FB 80 sequential data sets. Use one data set to contain the PTFs and the other to contain the hold data.

The PTFs and hold data become accessible to the *yourhlq.SAMPJCL* maintenance members.

3. Edit and submit the AKASEDIT macro.

The *yourhlq.SAMPJCL* members AKA6RECP, AKA7APYP, and AKA8ACCP are customized.

4. Customize the AKA6RECP SMPPTFIN and SMPHOLD DD statements to reference the FB 80 data sets for the PTFs and hold data.

5. Submit AKA6RECP.

The PTFs and hold data are received.

6. Submit AKA7APYP.

The PTFs are applied.

7. (Optional) Customize and submit *yourhlq.SAMPJCL* member AKA8ACCP.

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, you are ready to configure your product.

Note: We recommend that you check for available maintenance; however, you may find that none is available.

Hold Data

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.

Review DB2 Setup JCL

For this step, review member KA32DB2 of CABYJCL, and become familiar with the job steps and their instructions. The comments contained in the JCL describe in detail the processing to be done and your required actions.

Important! Do not attempt to modify the JCL at this point; do that in a later step.

This JCL invokes the IBM DB2 program DSNTIAD to create the views for the catalog tables and, if specified, the PANAPT_PRODPLAN table. DSNTIAD is a sample program provided with DB2.

If this program is not available for any reason, you can use SPUFI to create the table and view before running the installation job; the input which you create in VIEWLIB (VIEWS) is in a compatible format and can be used as input to SPUFI.

Note: If you use SPUFI, you must log on to TSO with the same user ID as in the USER parameter of the JOB statement in the installation JCL. Otherwise, the CA PanAPT utility programs are bound to a different OWNER than that of the views, causing the BIND to fail.

If this is not possible, then while you are in SPUFI, qualify the views with the owner of the installation job or create a synonym for the views to the owner of the installation job.

An alternative for DB2 version 2.1 or above is to change the bind commands in the installation job to provide an owner corresponding to your TSO user ID.

After reviewing all the steps of the installation JCL and their instructions, proceed to the next step.

Grant Authority

Whether you use the default ownerid and user ID of CA PanAPT or select another ownerid for the views, the following conditions must be met:

_ A DB2 System Administrator (SYSADM authority) must grant the ownerid the select privilege on the DB2 system catalog tables by executing the following GRANT commands:

```
GRANT SELECT on SYSIBM.SYSDBRM to ownerid with GRANT OPTION
GRANT SELECT on SYSIBM.SYSPACKAGE to ownerid with GRANT OPTION
GRANT SELECT on SYSIBM.SYSPACKLIST to ownerid with GRANT OPTION
GRANT SELECT on SYSIBM.SYSPKSYSTEM to ownerid with GRANT OPTION
GRANT SELECT on SYSIBM.SYSPLSYSTEM to ownerid with GRANT OPTION
GRANT SELECT on SYSIBM.SYSPLAN to ownerid with GRANT OPTION
```

where ownerid is the ownerid chosen for the CA PanAPT views (if you select an ownerid other than PANAPT you must modify JCL member KA32DB2 to reflect the ownerid chosen).

You must either provide a user ID with SYSADM authority on the JOB card, or use the ownerid of the catalog views. The user ID provided on the JOB card becomes the ownerid of the CA PanAPT plans.

Create VIEWLIB(VIEWS)

In this step, you create the member VIEWLIB(VIEWS) from one of the sample members provided in VIEWLIB. The member is used to create the views used by these utilities. You must select one of our sample members and modify it to create VIEWLIB(VIEWS).

The DB2 Validation Utility and the three stand-alone utilities (APCS5520, APCS5521, and APCS5522) use views to access the DB2 catalog tables. These views perform the following two major functions:

- They ensure that the programs are compatible with different versions of DB2.
- They filter out rows in the SYSPLAN and SYSDBRM tables that do not pertain to Production.

There are three types of sample view members in VIEWLIB:

- The member named ALL describes an environment where all the activity in the DB2 subsystem is considered to be production activity.
- The member named RULE describes an environment where production and non-production plans are mixed in one DB2 subsystem, but naming conventions are implemented that enable you to distinguish between the two. You need to edit the member to provide a rule to be used.
- The member named LIST describes an environment where production and non-production are mixed in one DB2 subsystem, and it is necessary to specifically list the names of the production plans. You need to edit the member statements to provide the plan names.

Browse the members to determine which of the sample views best suits your environment. Later you copy that member to create member VIEWS, then customize VIEWS to suit your specific environment, as described later. VIEWS are used as input to a step in job KA32DB2 that creates the views used by CA PanAPT.

For additional discussion on the methods for handling your product environment with DB2 VIEWS, see *The DB2 Reference Guide*, "Production Plan and Production Package Tables," chapter.

Each view definition member contains several view definitions:

```
PANAPT_SYSPLAN
PANAPT_SYSDBRM
PANAPT_SYSPACKAGE
PANAPT_SYSPACKLIST
PANAPT_SYSPKSYSTEM
PANAPT_SYSPLSYSTEM
PANAPT_SYSPLAN_P
PANAPT_SYSDBRM_P
PANAPT_SYSPACK_P
```

The first six definitions define the views to access all plans, DBRMs, and packages. The last three definitions define the views to access only Production plans and DBRMs.

Create the Member

The VIEWS member should now be created and, in most cases, tailored to restrict the scope of the rows accessed to Production plans and DBRMs. You do not need to restrict these rows if your Production DB2 is maintained exclusively in its own DB2 subsystem, with no Test or QA plans bound in that subsystem.

The following guidelines help you determine which member to select and how to modify its contents.

Dedicated DB2 Subsystems

If you do not need to restrict rows from your views because the DB2 subsystem environment is solely dedicated to production:

- Copy member ALL, creating the member VIEWS
- Verify your version of DB2 (see note below).

Shared DB2 Subsystem

If you must restrict rows from your view because production shares a DB2 subsystem environment, you should copy either RULEn or LISTn to create the member VIEW, then edit VIEWS so it differentiates Production plans from other plans.

If catalog information can be used to identify Production plans and packages:

- Copy sample member RULE, creating the member VIEWS
- Verify your version of DB2 (see note)
- Edit VIEWS to recognize production. For example, if all Production plans start with the letter P or plans and packages created or owned by a particular set or user IDs are production, then a rule can be applied to the view in a WHERE clause.
- If catalog information cannot be used in a WHERE clause to isolate

Production plans and packages:

- Copy sample member LIST, creating the member VIEWS
- Verify your version of DB2 (see note)
- Edit VIEWS to recognize production
- Create tables that list each Production plan and package by name
- Use table name PANAPT_PRODPLAN for the list of Production plans
- Use table name PANAPT_PRODPACK for the list of Production Packages
- Join these tables to the catalog tables
- Use a WHERE clause to restrict the scope of the rows

Note: Verify your version of DB2. Whichever member you select to create member VIEWS, the contents must reflect the version of DB2 on which it is to be used. In the source, there are multiple occurrences of the line:

```
AS SELECT SUBSTR('x.y',1,3),
```

Replace x.y with one of the following to indicate your version of DB2:

```
4.1 - DB2 version 4.1
5.1 - DB2 version 5.1
6.1 - DB2 version 6.1 or above
```

When editing VIEWS, remember that, of its contents, only the three view names describe Production views:

1. PANAPT_SYSPLAN_P
2. PANAPT_SYSDBRM_P
3. PANAPT_SYSPACK_P

The other view names are general views and should not be altered.

Modify DB2 Setup JCL

For this step, modify the CABYJCL (KA32DB2) according to your site's unique requirements and standards. Follow the detailed modification instructions contained in the beginning documentation box in the JCL itself. These instructions appear under the USAGE heading.

Parts of the instructions direct you to make a copy of the DB2 Setup JCL. This is an important step because it provides an online, unmodified copy of the JCL in case you have problems with the JCL modification or need to submit additional jobs for each DB2 subsystem.

If you run the CA PanAPT DB2 Option on more than one host system or on more than one DB2 subsystem, you must install the CA PanAPT DB2 Option on each host system, and you must do the bind installation step on each DB2 subsystem.

Review Setup Job Results

Review the job output for completeness and correctness. All job steps should complete with a condition code of zero. If any step does not, correct the error and restart the job from the beginning.

Also, review the DSNTIAD output for completeness and correctness. DSNTIAD ends with a condition code of zero even if it fails. The only SQL statements that should fail are the DROP statements, which are provided to assist with the reinstall of CA PanAPT DB2. If any step does not complete as expected, correct the error and restart the job.

Keep a printed copy of all installation output. The output provides technical documentation for resolving problems in the future and might be requested by CA Technical Support at <http://support.ca.com/>.

Update Your Security System

All data sets created so far should be protected Production data sets. Update your security system to provide access appropriate to your site.

Run the CA PanAPT DB2 Option Enable Program

Run APJJ0590 to enable the DB2 Option in CA-PanAPT. The JCL to run this is provided with the base CA PanAPT product. Edit the JCL to conform to your installation standards.

Index

A

- acquiring the product • 14, 32
- acquisition
 - download • 22, 33
- adding
 - custom data set • 103
 - data destination • 77
 - FTP locations • 72
 - product • 101
 - system • 127
- aggregated package, viewing • 48
- allocate and mount • 137
- authorization
 - modes • 63

C

- CA MSM access
 - login • 31
- CA MSM usage scenarios • 22
- CAI.SAMPJCL
 - library • 160
 - sample jobs • 160
- catalog, update • 32
- confirming deployment • 98
- contact system • 69
- contacting technical support • 3
- copy files to USS directory • 140, 141, 144
- creating
 - data destination • 76
 - deployment • 86
 - methodology • 110
 - monoplex • 60
 - shared DASD cluster • 61
 - staging • 62
 - sysplex • 60
- custom data sets
 - add • 103
 - edit • 106
 - remove • 109
 - view • 102
- customer support, contacting • 3

D

- data class • 126

- data set name mask • 113
- data sets, file systems
 - data destinations
 - add • 77
 - create • 76
 - delete • 80
 - edit • 78
 - maintain • 78
 - set default • 80
- default
 - data destination • 80
 - FTP location • 74
- deleting
 - data destination • 80
 - development • 97
 - system registry • 71
- delivery, product acquisition • 14
- deployments
 - confirm • 98
 - create • 86
 - current state • 84
 - delete • 97
 - maintain • 93
 - preview • 90
 - reset status • 96
 - select a product • 100
 - select a system • 127
 - summary • 128
 - validation, failed • 67
 - view • 90
- distribution
 - tape • 14
- distribution tape • 14
- download • 22, 33
 - files using ESD • 133
 - installation packages • 22, 33
 - LMP keys • 43
 - maintenance packages • 22, 45, 46
 - options • 140
 - overview • 131
 - to mainframe through a PC • 144
 - using batch JCL • 141

E

- edit

- custom data set • 106
- edit, data destination • 78
- methodology • 123
- ESD (Electronic Software Delivery) • 14
- external HOLDDATA • 151
- external packages
 - installation • 35, 37
 - migration • 34, 47

F

- failed validation • 67
- free space • 136
- FTP locations
 - add • 72
 - edit • 73
 - remove • 74
 - set default • 74

G

- GIMUNZIP utility • 146
- GROUPEXTEND mode • 53

H

- hash setting • 146
- high-level qualifier • 146
- HOLDDATA • 151
 - external • 151
 - internal • 151

I

- IEBCOPY • 160
- installation • 22, 37
- installation packages
 - download • 33
 - migration • 34
- installing
 - from Pax-Enhanced ESD • 131
 - from tape • 159
- Integrated Cryptographic Services Facility (ICSF) • 146
- internal HOLDDATA • 151
- investigating failed validation • 67

J

- Java version support • 146

L

- libraries
 - acquiring the product • 14, 32
 - acquisition
 - download • 22, 33
 - adding
 - custom data set • 103
 - data destination • 77
 - FTP locations • 72
 - product • 101
 - system • 127
 - aggregated package, viewing • 48
 - allocate and mount • 137
 - authorization
 - modes • 63
 - CA MSM access
 - login • 31
 - CA MSM usage scenarios • 22
 - CAI.SAMPJCL
 - library • 160
 - sample jobs • 160
 - catalog, update • 32
 - confirming deployment • 98
 - contact system • 69
 - contacting technical support • 3
 - copy files to USS directory • 140, 141, 144
 - creating
 - data destination • 76
 - deployment • 86
 - methodology • 110
 - monoplex • 60
 - shared DASD cluster • 61
 - staging • 62
 - sysplex • 60
 - custom data sets
 - add • 103
 - edit • 106
 - remove • 109
 - view • 102
 - customer support, contacting • 3
 - data class • 126
 - data set name mask • 113
 - data sets, file systems
 - data destinations
 - add • 77
 - create • 76
 - delete • 80
 - edit • 78

- maintain • 78
 - set default • 80
- default
 - data destination • 80
 - FTP location • 74
- deleting
 - data destination • 80
 - development • 97
 - system registry • 71
- delivery, product acquisition • 14
- deployments
 - confirm • 98
 - create • 86
 - current state • 84
 - delete • 97
 - maintain • 93
 - preview • 90
 - reset status • 96
 - select a product • 100
 - select a system • 127
 - summary • 128
 - validation, failed • 67
 - view • 90
- distribution
 - tape • 14
- download • 22, 33
 - files using ESD • 133
 - installation packages • 22, 33
 - LMP keys • 43
 - maintenance packages • 22, 45, 46
 - options • 140
 - overview • 131
 - to mainframe through a PC • 144
 - using batch JCL • 141
- edit
 - custom data set • 106
 - edit, data destination • 78
 - methodology • 123
- ESD (Electronic Software Delivery) • 14
- external HOLDDATA • 151
- external packages
 - installation • 35, 37
 - migration • 34, 47
- failed validation • 67
- free space • 136
- FTP locations
 - add • 72
 - edit • 73
 - remove • 74
 - set default • 74
- GIMUNZIP utility • 146
- GROUPEXTEND mode • 53
- hash setting • 146
- high-level qualifier • 146
- HOLDDATA • 151
- IEBCOPY • 160
- installation • 22, 37
- installation packages
 - download • 33
 - migration • 34
- installing
 - from Pax-Enhanced ESD • 131
 - from tape • 159
- Integrated Cryptographic Services Facility (ICSF) • 146
- internal HOLDDATA • 151
- investigating failed validation • 67
- Java version support • 146
- LMP keys • 43
- maintain
 - data destinations • 78
 - deployment • 93
 - maintain by list, system register • 70
 - system registry • 64
- maintenance
 - application • 22, 49
 - backout • 57
 - GROUPEXTEND mode • 53
 - USERMODs • 53
- maintenance packages
 - backout • 57
 - download • 22, 45, 46
 - installation • 22, 49, 52
 - migration • 47
 - USERMODs • 53
 - viewing status • 52
- methodology
 - create • 110
 - remove • 125
 - symbolics qualifiers • 113
- migrations
 - installation packages • 34
 - maintenance packages • 47
- monoplex
 - create • 60
- nested packages • 48
- pax ESD procedure
 - copy product files • 140

- create product directory • 145
- download files • 133
- set up USS directory • 136
- pax file
 - copy files to USS directory • 140, 141, 144
- process overview • 131
- product
 - acquisition • 14
- product download window • 133
- product-level directory • 145
- products
 - acquired externally • 35, 47
 - add • 101
 - download • 22, 33
 - installation • 22, 37
 - maintenance • 22, 49, 57
 - remove from deployment • 101
- read me • 131, 146
- remote credentials
 - add • 81
 - delete • 83
 - edit • 82
- remove
 - custom data sets • 109
 - FTP locations • 74
 - methodologies • 125
 - product • 101
 - system • 128
- reset status • 96
- sample JCL • 160
- sample jobs • 141, 145
 - CAtoMainframe.txt • 141
 - Unpackage.txt • 145
- scenarios, usage • 22
- SMP/E
 - GIMUNZIP utility • 146
- SMP/E environments
 - creation • 40
 - migration • 22
- software
 - delivery • 14
 - inventory • 32
- support, contacting • 3
- symbolic qualifiers • 113
- system
 - add • 127
 - remove • 128
- system registry
 - authorization • 63

- create non-sysplex • 59
- create, data destination • 76
- create, shared DASD cluster • 61
- create, staging • 62
- create, sysplex • 60
- delete • 71
- maintain • 58
- maintain using list • 70
- view • 58
- tape, installing from • 159
- technical support, contacting • 3
- UNIX System Services (USS)
 - access requirements • 131, 136
 - directory cleanup • 150
 - directory structure • 136
- UNZIPJCL • 146
- USERMODs • 53
- viewing
 - aggregated package • 48
 - custom data sets • 102
 - deployment • 90
 - maintenance package status • 52
 - product list • 100
 - system list • 127
 - system registry • 58
- zFS candidate volumes • 70
- LMP keys • 43

M

- maintain
 - data destinations • 78
 - deployment • 93
 - maintain by list, system register • 70
 - system registry • 64
- maintenance
 - application • 22, 49
 - backout • 57
 - GROUPEXTEND mode • 53
 - USERMODs • 53
- maintenance packages
 - backout • 57
 - download • 22, 45, 46
 - installation • 22, 49, 52
 - migration • 47
 - USERMODs • 53
 - viewing status • 52
- methodology
 - create • 110

- remove • 125
- symbolics qualifiers • 113
- migrations
 - installation packages • 34
 - maintenance packages • 47
- monoplex
 - create • 60

N

- nested packages • 48

P

- pax ESD procedure
 - copy product files • 140
 - create product directory • 145
 - create product-specific directory • 146
 - download files • 133
 - set up USS directory • 136
- pax file
 - copy files to USS directory • 140, 141, 144
- process overview • 131
- product
 - acquisition • 14
- product download window • 133
- product-level directory • 145
- products
 - acquired externally • 35, 47
 - add • 101
 - download • 22, 33
 - installation • 22, 37
 - maintenance • 22, 49, 57
 - remove from deployment • 101

R

- read me • 131, 146
- remote credentials
 - add • 81
 - delete • 83
 - edit • 82
- remove
 - custom data sets • 109
 - FTP locations • 74
 - methodologies • 125
 - product • 101
 - system • 128
- reset status • 96

S

- sample JCL • 160
- sample jobs • 141, 145
 - CAt>Mainframe.txt • 141
 - Unpackage.txt • 145
- scenarios, usage • 22
- SMP/E
 - GIMUNZIP utility • 146
- SMP/E environments
 - creation • 40
 - migration • 22
- software
 - delivery • 14
 - inventory • 32
- software delivery • 14
- support, contacting • 3
- symbolic qualifiers • 113
- system
 - add • 127
 - remove • 128
- system registry
 - authorization • 63
 - create non-sysplex • 59
 - create, data destination • 76
 - create, shared DASD cluster • 61
 - create, staging • 62
 - create, sysplex • 60
 - delete • 71
 - maintain • 58
 - maintain using list • 70
 - view • 58

T

- tape, installing from • 159
- technical support, contacting • 3

U

- UNIX System Services (USS)
 - access requirements • 131, 136
 - directory cleanup • 150
 - directory structure • 136
 - product directory cleanup • 150
- UNZIPJCL • 146
- USERMODs • 53

V

- viewing

aggregated package • 48
custom data sets • 102
deployment • 90
maintenance package status • 52
product list • 100
system list • 127
system registry • 58

Z

zFS candidate volumes • 70