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 © 2011 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.
CA Technologies Product References

This document references the following CA products:

- CA ACF2™ for z/OS
- CA Auditor for z/OS
- CA Common Services for z/OS
- CA Service Desk
- CA SMF Director®
- CA Top Secret® for z/OS

Contact CA Technologies

Contact CA Support

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

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

Provide Feedback

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

If you would like 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.
## Contents

### Chapter 1: Overview
- Audience .................................................................................................................... 9
- How the Installation Process Works ........................................................................... 9

### Chapter 2: Preparing for Installation
- Software Requirements .................................................................................................. 11
  - SMF Records Processed ............................................................................................... 12
  - RMF Records Processed ............................................................................................. 13
  - SMF Extensions .......................................................................................................... 14
  - XML Requirements ..................................................................................................... 14
  - Library Authorization ................................................................................................. 14
- CA Common Services Requirements ........................................................................... 15
- Storage Requirements .................................................................................................... 16
  - TSO Requirements ...................................................................................................... 16
  - DASD Requirements .................................................................................................... 16
- Other Requirements ....................................................................................................... 20
  - JARS/OLF Requirements ............................................................................................ 20
- Concurrent Releases ...................................................................................................... 21

### Chapter 3: Installing Your Product Using CA MSM
- CA MSM Documentation .............................................................................................. 23
- Getting Started Using CA MSM .................................................................................... 24
  - How to Use CA MSM: Scenarios ................................................................................. 24
  - Access CA MSM Using the Web-Based Interface ....................................................... 33
- Acquiring Products ........................................................................................................ 34
  - Update Software Catalog ........................................................................................... 34
  - Download Product Installation Package ..................................................................... 35
  - Migrate Installation Packages Downloaded External to CA MSM ......................... 37
  - Add a Product .............................................................................................................. 37
- Installing Products ......................................................................................................... 40
  - Install a Product .......................................................................................................... 40
  - Create a CSI .................................................................................................................. 43
  - Download LMP Keys ................................................................................................... 46
- Maintaining Products ..................................................................................................... 47
  - How to Apply Maintenance Packages ....................................................................... 47
  - Download Product Maintenance Packages ............................................................... 48
Download Maintenance Packages for Old Product Releases and Service Packs ........................................ 49
Manage Maintenance Downloaded External to CA MSM ........................................................................... 50
Manage Maintenance ............................................................................................................................... 52
GROUPEXTEND Mode .............................................................................................................................. 56
Back Out Maintenance .............................................................................................................................. 60
Setting System Registry .......................................................................................................................... 61
View a System Registry ............................................................................................................................ 61
Create a Non-Sysplex System .................................................................................................................. 62
Create a Sysplex or Monoplex .................................................................................................................. 63
Create a Shared DASD Cluster .................................................................................................................. 64
Create a Staging System ........................................................................................................................... 65
Authorization ........................................................................................................................................... 65
Change a System Registry ....................................................................................................................... 66
Maintain a System Registry using the List Option .................................................................................. 72
Delete a System Registry ........................................................................................................................ 73
FTP Locations .......................................................................................................................................... 73
Data Destinations ..................................................................................................................................... 77
Remote Credentials ............................................................................................................................... 83
Deploying Products .................................................................................................................................. 86
Deployment Status ................................................................................................................................. 86
Creating Deployments ............................................................................................................................. 87
View a Deployment ................................................................................................................................. 92
Change Deployments ............................................................................................................................... 93
Delete a Deployment ............................................................................................................................... 99
Confirm a Deployment ............................................................................................................................ 101
Products ................................................................................................................................................... 103
Custom Data Sets ..................................................................................................................................... 104
Methodologies .......................................................................................................................................... 112
Systems .................................................................................................................................................... 129
Deployment Summary ............................................................................................................................. 132

Chapter 4: Installing Your Product from Pax-Enhanced ESD ...................................................................... 135
How to Install a Product Using Pax-Enhanced ESD ................................................................................ 135
How the Pax-Enhanced ESD Download Works ....................................................................................... 136
ESD Product Download Window ............................................................................................................. 137
USS Environment Setup .......................................................................................................................... 140
Allocate and Mount a File System ........................................................................................................... 141
Copy the Product Pax Files into Your USS Directory ............................................................................... 143
Download Using Batch JCL ..................................................................................................................... 144
Download Files to Mainframe through a PC ......................................................................................... 147
Create a Product Directory from the Pax File ......................................................................................... 148
Example Job to Execute the Pax Command (Unpackage.txt) ........................................... 149
Copy Installation Files to z/OS Data Sets ........................................................................ 149
Receiving the SMP/E Package ....................................................................................... 150
How to Install Products Using Native SMP/E JCL ....................................................... 151
Prepare the SMP/E Environment for PAX Installation .................................................. 152
Run the Installation Jobs for a Pax Installation ............................................................... 153
Clean Up the USS Directory ............................................................................................. 154
Apply Maintenance ......................................................................................................... 155
HOLDDATA ................................................................................................................... 156

Chapter 5: Installing Your Product from Tape ................................................................. 157
Unload the Sample JCL from Tape ................................................................................ 157
How to Install Products Using Native SMP/E JCL ....................................................... 158
  Prepare the SMP/E Environment for Tape Installation .............................................. 159
  Run the Installation Jobs for a Tape Installation ......................................................... 160
Apply Maintenance ......................................................................................................... 161
HOLDDATA ................................................................................................................... 162

Chapter 6: Configuring Your Product .............................................................................. 163
Step 1. Tailor LMP Keys ................................................................................................. 163
Step 2. Run CAIRIM for CA JARS SMP/E .................................................................... 164
Step 3. Define Wizard Company Name .......................................................................... 164
Step 4. Run CA JARS Installation Verification Tests ....................................................... 165
Step 5. Invoke the ISPF Interface .................................................................................. 166
Step 6. Install XML Support ........................................................................................... 166
Step 7. Integrate with CA SMF Director ......................................................................... 166
  Why Use CA SMF Director .......................................................................................... 167
  SPLIT Processing ......................................................................................................... 167
Step 8. Integrate with CA Auditor for z/OS .................................................................. 168
Step 9. Complete the Configuration Worksheet ............................................................ 168
Step 10. Run cBASE Link-Edit ....................................................................................... 170
Step 11. Run cBASE Data Dictionary Link-Edit for CA Datacom .................................. 170
Step 12. Run DB2 BIND Procedure .............................................................................. 170
Step 13. Allocate CAIKSPAR ....................................................................................... 171
Step 14. Customize CAIKSPAR .................................................................................... 171
Step 15. Prepare the Database ....................................................................................... 171
  Step 15a. Prepare CA Datacom/DB Database ............................................................... 171
  Step 15b. Prepare CA Datacom/AD Database ............................................................... 172
  Step 15c. Prepare DB2 Database .................................................................................. 172
Step 16. Create Schema for CA Datacom Users ............................................................. 173
Step 17. Create and Load Tables .................................................................................... 173
Chapter 1: Overview

This guide describes how to install and implement CA JARS RA.

This section contains the following topics:

Audience (see page 9)
How the Installation Process Works (see page 9)

Audience

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

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

You may need to work with the following personnel:

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

How the Installation Process Works

The following steps describe the installation process:

1. Prepare for the installation by confirming that your site meets all installation requirements.

2. Acquire the product using one of the following methods:

   - CA MSM
     
     Note: If you do not have CA MSM, you can download it from the Download Center at 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.

   - Pax-Enhanced Electronic Software Delivery (ESD)

   - Tape
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. Configure each component that has configuration parameters.
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:

Software Requirements (see page 11)
CA Common Services Requirements (see page 15)
Storage Requirements (see page 16)
Other Requirements (see page 20)
Concurrent Releases (see page 21)

Software Requirements

CA JARS provides a single, integrated report writer that accepts data from the following multiple input sources:

<table>
<thead>
<tr>
<th>Data Source</th>
<th>System Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMF</td>
<td>z/OS</td>
</tr>
<tr>
<td>DOS/VSE VM</td>
<td>CA-$JOBACCT VM/SP</td>
</tr>
<tr>
<td>ROSCOE</td>
<td>Release 5.2 or above</td>
</tr>
<tr>
<td>ADABAS</td>
<td>Release 4.1 or above</td>
</tr>
<tr>
<td>IMS</td>
<td>Release 1.3 or above</td>
</tr>
<tr>
<td>CA Datacom</td>
<td>All supported CA Datacom releases</td>
</tr>
<tr>
<td>DB2</td>
<td>Release 2 or above</td>
</tr>
<tr>
<td>Disk Space Accounting</td>
<td>z/OS</td>
</tr>
<tr>
<td>CICS</td>
<td>Release 6.2 or above (CA JARS Resource Management for CICS is a chargeable option)</td>
</tr>
<tr>
<td>IDMS</td>
<td>Release 12.0 or above (CA JARS Resource Management IDMS Option is a chargeable option)</td>
</tr>
<tr>
<td>TVA</td>
<td>CA 1 Release 4.1 or above TLMS Release 5.3 or above</td>
</tr>
<tr>
<td>Network</td>
<td>IBM NetView product</td>
</tr>
</tbody>
</table>
## SMF Records Processed

Full use of this product requires that SMF statistics for the following record types be collected. SMF collection specifications are defined in the SYS1.PARMLIB member SMFPRMxx.

<table>
<thead>
<tr>
<th>SMF Record Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>IPL</td>
</tr>
<tr>
<td>4</td>
<td>Step/Session Totals</td>
</tr>
<tr>
<td>5</td>
<td>Job/Session END</td>
</tr>
<tr>
<td>6</td>
<td>Output Writer (JES2/JES3)</td>
</tr>
<tr>
<td>7</td>
<td>Data Lost</td>
</tr>
<tr>
<td>8</td>
<td>I/O Configuration</td>
</tr>
<tr>
<td>9</td>
<td>Vary Device ONLINE</td>
</tr>
<tr>
<td>10</td>
<td>Allocation Recovery</td>
</tr>
<tr>
<td>11</td>
<td>Vary Device OFFLINE</td>
</tr>
<tr>
<td>19</td>
<td>DASD Volumes at IPL</td>
</tr>
<tr>
<td>25</td>
<td>JES3 Device Allocation</td>
</tr>
<tr>
<td>26</td>
<td>Job Purge (JES2/JES3)</td>
</tr>
<tr>
<td>30</td>
<td>Task Measured Usage</td>
</tr>
<tr>
<td></td>
<td>Task OpenEdition Usage</td>
</tr>
<tr>
<td>30-1</td>
<td>Job Initiation</td>
</tr>
<tr>
<td>30-2</td>
<td>Interval End</td>
</tr>
<tr>
<td>30-3</td>
<td>Step/Session Termination</td>
</tr>
<tr>
<td>30-4</td>
<td>Step/Session Total</td>
</tr>
<tr>
<td>30-5</td>
<td>Job/Session END</td>
</tr>
<tr>
<td>32</td>
<td>TSO/E User Work Accounting</td>
</tr>
<tr>
<td>33</td>
<td>APPC TP Accounting</td>
</tr>
<tr>
<td>39</td>
<td>NLDM Response Time (NETVIEW Interface Only)</td>
</tr>
<tr>
<td>41</td>
<td>DIV Access/Unaccess VLF Statistics</td>
</tr>
<tr>
<td>42</td>
<td>DFSMS and DFP Statistics</td>
</tr>
<tr>
<td>42-5</td>
<td>Storage Class Response</td>
</tr>
</tbody>
</table>
### SMF Record Type

<table>
<thead>
<tr>
<th>SMF Record Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>42-6</td>
<td>Data Set Statistics</td>
</tr>
<tr>
<td>47</td>
<td>RJE Signon (JES2/JES3)</td>
</tr>
<tr>
<td>48</td>
<td>RJE Signoff (JES2/JES3)</td>
</tr>
<tr>
<td>49</td>
<td>RJE Integrity (JES2/JES3)</td>
</tr>
<tr>
<td>50</td>
<td>VTAM Statistics</td>
</tr>
<tr>
<td>52</td>
<td>Supported - EXT + JARS</td>
</tr>
<tr>
<td>53</td>
<td>Supported - EXT + JARS</td>
</tr>
<tr>
<td>54</td>
<td>Supported - EXT + JARS</td>
</tr>
<tr>
<td>57</td>
<td>Network Transmission</td>
</tr>
<tr>
<td>88</td>
<td>System Logger</td>
</tr>
<tr>
<td>89</td>
<td>System Measured Usage</td>
</tr>
<tr>
<td>92</td>
<td>Hierarchical File System Usage</td>
</tr>
<tr>
<td>94</td>
<td>VTS (Virtual Tape Subsystem)</td>
</tr>
<tr>
<td>101</td>
<td>DB2 User Accounting (DB2 Interface Only)</td>
</tr>
<tr>
<td>103</td>
<td>Websphere</td>
</tr>
<tr>
<td>110</td>
<td>CICS Monitoring Facility</td>
</tr>
<tr>
<td>115/116</td>
<td>MQSeries</td>
</tr>
<tr>
<td>118</td>
<td>TCP/IP Statistics</td>
</tr>
<tr>
<td>119</td>
<td>TCP/IP</td>
</tr>
<tr>
<td>120</td>
<td>WebSphere</td>
</tr>
<tr>
<td>nnn (default 240)</td>
<td>User Record number (CA JARS DSA Resource Management Option Only)</td>
</tr>
<tr>
<td>nnn (default 237)</td>
<td>User Record number (CA JARS Resource Management for CICS)</td>
</tr>
</tbody>
</table>

### RMF Records Processed

The following RMF records are supported:

<table>
<thead>
<tr>
<th>RMF Record Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>70</td>
<td>CPU Activity</td>
</tr>
<tr>
<td>71</td>
<td>Paging Activity</td>
</tr>
<tr>
<td>RMF Record Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>72</td>
<td>Workload Activity</td>
</tr>
<tr>
<td>73</td>
<td>Channel Path Activity</td>
</tr>
<tr>
<td>74</td>
<td>Device Activity</td>
</tr>
<tr>
<td>75</td>
<td>Page/Swap Data Set Activity</td>
</tr>
<tr>
<td>77</td>
<td>ENQ/Reserve Contention</td>
</tr>
<tr>
<td>78</td>
<td>I/O Queuing Activity</td>
</tr>
</tbody>
</table>

**SMF Extensions**

In addition to these data sources, an optional component called SMF Extensions (SMF/E) is provided that enhances z/OS system capabilities. This exit provides a banner box in all output SYSPRINT and an end of session TSO report that computes an estimated charge for the job, job step, or TSO session. The JARSTATS exit uses a subset of the chargeback capabilities employed in this product. It can serve as an effective tool for improving user awareness of the costs associated with their individual job executions.

There is no SMF exit requirement to support the SMF/E option of this product. The CA Common Services for z/OS Resource Initialization Manager (CAIRIM), supplies a comprehensive step-termination statistic routine without any disturbance or integration with existing IEFACTRT exits.

**XML Requirements**

If CA JARS RA is going to be used to produce XML report documents and schema, the IBM XML Toolkit for z/OS must be installed. You can use either the SMP/E method or the non-SMP/E method to install Version 1.6 or higher of the Toolkit on the system where CA JARS RA will be run.

The IBM XML Toolkit for z/OS can be downloaded from IBM’s website, [http://www.ibm.com](http://www.ibm.com). Installation instructions and documentation are included with the downloads.

**Library Authorization**

CA JARS RA contains authorized programs. To run successfully, they must be executed from an authorized linklist library.
Before installing CA JARS, the following CA Common Services for z/OS must be installed:

- CAIRIM (S910 or higher)

Before installing CA JARS with JARS/OLF, the following CA Common Services for z/OS must also be installed:

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

If Earl and JARS/OLF are being used at your site, the following CA Common Services for z/OS must also be installed:

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

**CAIRIM**

Prepares your operating system environment for all CA applications and starts them. The common driver for a collection of dynamic initialization routines eliminates the need for user SVCs, SMF exits, subsystems, and other installation requirements commonly encountered when installing systems applications.

Integral parts of CAIRIM are CAISSF, CA LMP, and CA zIIP Enablement Services.

**CAISSF**

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

**CA LMP**

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

**CA zIIP Enablement Services**

Provides a common service for CA products to allow their code to run on zIIP processors, if available.

**ViewPoint**

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

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

SRAM Service

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

Earl Service

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

Storage Requirements

TSO Requirements

We recommend that TSO users run the JARS/OLF online facility using 4 MB. However, online processing can function using 2 MB.

DASD Requirements

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

CA JARS Family Permanent (Target) Libraries

<table>
<thead>
<tr>
<th>Library Name</th>
<th>Blksize</th>
<th>Tracks</th>
<th>Dir Blocks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAJRCLS0</td>
<td>32720</td>
<td>8,2</td>
<td>6</td>
<td>JARS Family CLIST Library</td>
</tr>
<tr>
<td>CAJLOAD</td>
<td>6144</td>
<td>105,21</td>
<td>33</td>
<td>JARS Family Load Library</td>
</tr>
<tr>
<td>CAJRMAC</td>
<td>32720</td>
<td>9,2</td>
<td>9</td>
<td>JARS Family Macro Library</td>
</tr>
<tr>
<td>CAJRPROC</td>
<td>32720</td>
<td>4,1</td>
<td>3</td>
<td>JARS Family Procedure Library</td>
</tr>
<tr>
<td>CAJRPNL0</td>
<td>32720</td>
<td>10,2</td>
<td>36</td>
<td>JARS Family ISPF Panel Library</td>
</tr>
<tr>
<td>CAJRTBL0</td>
<td>32720</td>
<td>3,1</td>
<td>5</td>
<td>JARS Family ISPF Table Library</td>
</tr>
<tr>
<td>Library Name</td>
<td>Blksize</td>
<td>Tracks</td>
<td>Dir Blocks</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>---------</td>
<td>--------</td>
<td>------------</td>
<td>-----------------------------------------------------------</td>
</tr>
<tr>
<td>CAJRSKL0</td>
<td>32720</td>
<td>2,1</td>
<td>2</td>
<td>JARS Family ISPF Skeleton Library</td>
</tr>
<tr>
<td>CAJRMNG0</td>
<td>32720</td>
<td>2,1</td>
<td>3</td>
<td>JARS Family ISPF Message Library</td>
</tr>
<tr>
<td>CAJRLMD0</td>
<td>27998</td>
<td>3,1</td>
<td>2</td>
<td>JARS Family ISPF Load Library</td>
</tr>
<tr>
<td>CAJRJCL</td>
<td>32720</td>
<td>15,3</td>
<td>30</td>
<td>JARS Family Sample JCL Library</td>
</tr>
<tr>
<td>CAJRSAMP</td>
<td>32720</td>
<td>16,4</td>
<td>12</td>
<td>JARS Family Sample Source Library</td>
</tr>
<tr>
<td>CAJOPTN</td>
<td>32720</td>
<td>160,32</td>
<td>21</td>
<td>JARS Family Sample Option Library</td>
</tr>
<tr>
<td>CAJRDATA</td>
<td>32720</td>
<td>4,1</td>
<td>2</td>
<td>JARS Family FB80 Data Library</td>
</tr>
<tr>
<td>CAJRDAT1</td>
<td>32600</td>
<td>7,2</td>
<td>2</td>
<td>JARS Family FB200 Data Library</td>
</tr>
<tr>
<td>CAJRDATV</td>
<td>32760</td>
<td>167,34</td>
<td>3</td>
<td>JARS Family Variable Data Library</td>
</tr>
<tr>
<td>CAJREARL</td>
<td>32720</td>
<td>102,21</td>
<td>188</td>
<td>JARS Family EARL Library</td>
</tr>
<tr>
<td>CAJREZTR</td>
<td>32720</td>
<td>70,14</td>
<td>129</td>
<td>JARS Family Easytrieve Library</td>
</tr>
<tr>
<td>CAJRXML</td>
<td>32760</td>
<td>4,1</td>
<td>2</td>
<td>JARS Family XML Library</td>
</tr>
<tr>
<td>CAJRSQL</td>
<td>32720</td>
<td>156,32</td>
<td>42</td>
<td>JARS Family SQL Library - OLF</td>
</tr>
<tr>
<td>CAJCPNO</td>
<td>32760</td>
<td>6,2</td>
<td>23</td>
<td>JARS Family cBASE OLF Panel Library - OLF</td>
</tr>
<tr>
<td>CAJCPNS</td>
<td>32760</td>
<td>30,6</td>
<td>137</td>
<td>JARS Family cBASE Shared Panel Library - OLF</td>
</tr>
<tr>
<td>CAJCLST</td>
<td>32760</td>
<td>5,1</td>
<td>33</td>
<td>JARS Family cBASE List Library - OLF</td>
</tr>
<tr>
<td>CAJCMMSG</td>
<td>32760</td>
<td>16,4</td>
<td>161</td>
<td>JARS Family cBASE Message Library - OLF</td>
</tr>
<tr>
<td>CAJCDLG</td>
<td>32760</td>
<td>208,42</td>
<td>50</td>
<td>JARS Family cBASE Dialog Library - OLF</td>
</tr>
<tr>
<td>CAJCSQL</td>
<td>32720</td>
<td>19,4</td>
<td>168</td>
<td>JARS Family cBASE SQL Library - OLF</td>
</tr>
<tr>
<td>CAJCTMP</td>
<td>32720</td>
<td>2,1</td>
<td>2</td>
<td>JARS Family cBASE Template Library - OLF</td>
</tr>
</tbody>
</table>
## CA JARS Distribution Libraries

<table>
<thead>
<tr>
<th>Library Name</th>
<th>Blksize</th>
<th>Tracks</th>
<th>Dir Blocks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AJRCLS0</td>
<td>32720</td>
<td>8,2</td>
<td>6</td>
<td>AJR CLIST Library</td>
</tr>
<tr>
<td>AAJRMOD0</td>
<td>6144</td>
<td>13,3</td>
<td>12</td>
<td>AJR Object Module Library</td>
</tr>
<tr>
<td>AAJRMAC</td>
<td>32720</td>
<td>7,2</td>
<td>8</td>
<td>AJR Macro Library</td>
</tr>
<tr>
<td>AAJRPROC</td>
<td>32720</td>
<td>3,1</td>
<td>2</td>
<td>AJR Procedure Library</td>
</tr>
<tr>
<td>AAJRPNL0</td>
<td>32720</td>
<td>10,2</td>
<td>36</td>
<td>AJR ISPF Panel Library</td>
</tr>
<tr>
<td>AAJRTBL0</td>
<td>32720</td>
<td>3,1</td>
<td>5</td>
<td>JARS Family ISPF Table Library</td>
</tr>
<tr>
<td>AAJRSKL0</td>
<td>32720</td>
<td>2,1</td>
<td>2</td>
<td>AJR ISPF Skeleton Library</td>
</tr>
<tr>
<td>AAJRMNG0</td>
<td>32720</td>
<td>2,1</td>
<td>3</td>
<td>AJR ISPF Message Library</td>
</tr>
<tr>
<td>AAJRJCL</td>
<td>32720</td>
<td>8,2</td>
<td>1</td>
<td>AJR Sample JCL Library</td>
</tr>
<tr>
<td>AAJRSMAC0</td>
<td>32720</td>
<td>9,2</td>
<td>8</td>
<td>AJR Sample Source Library</td>
</tr>
<tr>
<td>AAJROPTN</td>
<td>32720</td>
<td>6,2</td>
<td>3</td>
<td>AJR Sample Option Library</td>
</tr>
<tr>
<td>AAJRDATA0</td>
<td>32720</td>
<td>4,1</td>
<td>2</td>
<td>AJR FB80 Data Library</td>
</tr>
<tr>
<td>AAJRDA10</td>
<td>32600</td>
<td>7,2</td>
<td>2</td>
<td>AJR FB200 Data Library</td>
</tr>
<tr>
<td>AAJRDATAV</td>
<td>32760</td>
<td>156,32</td>
<td>3</td>
<td>AJR Variable Data Library</td>
</tr>
<tr>
<td>AAJRXNL</td>
<td>32720</td>
<td>4,1</td>
<td>2</td>
<td>JARS Family XML Library</td>
</tr>
<tr>
<td>AAJ1MAC0</td>
<td>32720</td>
<td>4,1</td>
<td>2</td>
<td>AJ1 Macro Library</td>
</tr>
<tr>
<td>AAJ1PROC0</td>
<td>32720</td>
<td>3,1</td>
<td>2</td>
<td>AJ1 Procedure Library</td>
</tr>
<tr>
<td>AAJ1JCL0</td>
<td>32720</td>
<td>6,2</td>
<td>6</td>
<td>AJ1 Sample JCL Library</td>
</tr>
<tr>
<td>AAJ1SAMP0</td>
<td>32720</td>
<td>9,2</td>
<td>5</td>
<td>AJ1 Sample Source Library</td>
</tr>
<tr>
<td>AAJ1OPTN0</td>
<td>32720</td>
<td>158,32</td>
<td>17</td>
<td>AJ1 Sample Option Library</td>
</tr>
<tr>
<td>AAJ1EARL0</td>
<td>32720</td>
<td>83,17</td>
<td>143</td>
<td>AJ1 EARL Library</td>
</tr>
<tr>
<td>AAJ1EURTR0</td>
<td>32720</td>
<td>70,14</td>
<td>129</td>
<td>AJ1 Easytrieve Library</td>
</tr>
<tr>
<td>AAJ1MOD0</td>
<td>27998</td>
<td>59,12</td>
<td>41</td>
<td>AJ1 Object Module Library</td>
</tr>
<tr>
<td>AAJ2MOD0</td>
<td>6144</td>
<td>2,1</td>
<td>2</td>
<td>AJ2 Object Module Library</td>
</tr>
</tbody>
</table>
## CA JARS Wizard Distribution Libraries

<table>
<thead>
<tr>
<th>Library Name</th>
<th>Blksize</th>
<th>Tracks</th>
<th>Dir Blocks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAJWMAC</td>
<td>32720</td>
<td>3,1</td>
<td>2</td>
<td>AJW Macro Library</td>
</tr>
<tr>
<td>AAJWMOD0</td>
<td>6144</td>
<td>9,2</td>
<td>5</td>
<td>AJW Object Module Library</td>
</tr>
<tr>
<td>AAJWJCL</td>
<td>32720</td>
<td>4,1</td>
<td>2</td>
<td>AJW Sample JCL Library</td>
</tr>
<tr>
<td>AAJWSAMP</td>
<td>32720</td>
<td>3,1</td>
<td>2</td>
<td>AJW Sample Source Library</td>
</tr>
</tbody>
</table>

## JARS/OLF Distribution Libraries

<table>
<thead>
<tr>
<th>Library Name</th>
<th>Blksize</th>
<th>Tracks</th>
<th>Dir Blocks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAWFEARL</td>
<td>32720</td>
<td>22,5</td>
<td>36</td>
<td>AWF Earl Library</td>
</tr>
<tr>
<td>AAWFSQL</td>
<td>32720</td>
<td>46,10</td>
<td>18</td>
<td>AWF SQL Library</td>
</tr>
<tr>
<td>AAWFJCL</td>
<td>32720</td>
<td>5,1</td>
<td>2</td>
<td>AWF JCL Library</td>
</tr>
<tr>
<td>AAWFCPNO</td>
<td>32760</td>
<td>6,2</td>
<td>23</td>
<td>AWF cBASE Panel Library</td>
</tr>
<tr>
<td>AAWFMOD0</td>
<td>6144</td>
<td>2,1</td>
<td>2</td>
<td>AWF Object Module Library</td>
</tr>
<tr>
<td>AAKRSAMP</td>
<td>32720</td>
<td>4,1</td>
<td>2</td>
<td>AKR Sample Library</td>
</tr>
<tr>
<td>AAKRSQL</td>
<td>32720</td>
<td>16,4</td>
<td>8</td>
<td>AKR SQL Library</td>
</tr>
<tr>
<td>AAKREARL</td>
<td>32720</td>
<td>8,2</td>
<td>9</td>
<td>AKR Earl Library</td>
</tr>
<tr>
<td>AAKRJCL</td>
<td>32720</td>
<td>7,2</td>
<td>11</td>
<td>AKR JCL Library</td>
</tr>
<tr>
<td>AAKRCLSL</td>
<td>32720</td>
<td>2,1</td>
<td>2</td>
<td>AKR CLIST Library</td>
</tr>
<tr>
<td>AAKRPROC</td>
<td>32720</td>
<td>3,1</td>
<td>2</td>
<td>AKR Procedure Library</td>
</tr>
<tr>
<td>AAKROPTN</td>
<td>32720</td>
<td>5,1</td>
<td>2</td>
<td>AKR Sample Option Library</td>
</tr>
<tr>
<td>AAKRMOD0</td>
<td>27998</td>
<td>24,5</td>
<td>5</td>
<td>AKR Object Module Library</td>
</tr>
<tr>
<td>AAKRCLST</td>
<td>32760</td>
<td>5,1</td>
<td>33</td>
<td>AKR cBASE List Library</td>
</tr>
<tr>
<td>AAKRCMSG</td>
<td>32760</td>
<td>16,4</td>
<td>161</td>
<td>AKR cBASE Message Library</td>
</tr>
<tr>
<td>AAKRCPNS</td>
<td>32760</td>
<td>30,6</td>
<td>137</td>
<td>AKR cBASE Shared Panel Library</td>
</tr>
<tr>
<td>AAKRCDLG</td>
<td>32760</td>
<td>208,42</td>
<td>50</td>
<td>AKR cBASE Dialog Library</td>
</tr>
<tr>
<td>AAKRCSQL</td>
<td>32760</td>
<td>19,4</td>
<td>168</td>
<td>AKR cBASE SQL Library</td>
</tr>
<tr>
<td>AAKRCTMP</td>
<td>32720</td>
<td>2,1</td>
<td>2</td>
<td>AKR cBASE Template Library</td>
</tr>
<tr>
<td>AAKRDATV</td>
<td>32760</td>
<td>13,3</td>
<td>2</td>
<td>AKJ Variable Data Library</td>
</tr>
</tbody>
</table>
### Other Requirements

<table>
<thead>
<tr>
<th>Library Name</th>
<th>Blks</th>
<th>Blks</th>
<th>Dir</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAKSSQL</td>
<td>32720</td>
<td>99,20</td>
<td>18</td>
<td>AKS SQL Library</td>
</tr>
<tr>
<td>AAKSEARL</td>
<td>32720</td>
<td>6,2</td>
<td>2</td>
<td>AKS Earl Library</td>
</tr>
<tr>
<td>AAKSJCL</td>
<td>32720</td>
<td>5,1</td>
<td>3</td>
<td>AKS JCL Library</td>
</tr>
<tr>
<td>AAKSPROC</td>
<td>32720</td>
<td>3,1</td>
<td>2</td>
<td>AKS Procedure Library</td>
</tr>
<tr>
<td>AAKSOPTN</td>
<td>32720</td>
<td>5,1</td>
<td>2</td>
<td>AKS Sample Option Library</td>
</tr>
<tr>
<td>AAKSMODO</td>
<td>27998</td>
<td>19,4</td>
<td>6</td>
<td>AKS Object Module Library</td>
</tr>
</tbody>
</table>

### JARS/OLF Parameter File

<table>
<thead>
<tr>
<th>Library Name</th>
<th>Blks</th>
<th>Blks</th>
<th>Dir</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAI.CAISKPAR</td>
<td>80</td>
<td>85</td>
<td>N/A</td>
<td>JARS/OLF runtime parameters</td>
</tr>
<tr>
<td>CAI.CAISKPAR</td>
<td>80</td>
<td>85</td>
<td>N/A</td>
<td>JARS/OLF runtime parameters</td>
</tr>
</tbody>
</table>

### Other Requirements

**JARS/OLF Requirements**

**Note:** The CA JARS product can be installed in either of two ways: you can install the full product including JARS/OLF, or you can install CA JARS base only without JARS/OLF. To install the full product including JARS/OLF, use the AWF-prefixed SAMPJCL members in the installation steps. To install CA JARS base only without JARS/OLF, use the AJR-prefixed SAMPJCL members.

JARS/OLF can be run on both nonprogrammable color and monochrome terminals. We require that either DB2 release 2 or above, CA Datacom with SQL, or CA Datacom/AD be installed. If your site does not have one of these databases, CA provides CA Datacom/AD as a separate installation.

Also required for database access is either one of the CA security solutions or compatible non-CA security products. JARS/OLF uses the cBase component of ViewPoint to provide online facilities.
Reporting and sorting are accomplished with two CA Common Services for z/OS components: Earl Service XE61 and CA SRAM SR66 or higher.

**Concurrent Releases**

You can install this release of CA JARS RA and continue to use an older release for your production environment. However, due to substantial changes in target and distribution libraries, you must install into a new SMP/E environment.
Chapter 3: Installing Your Product Using CA MSM

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

Note: If you do not have CA MSM, you can download it from the Download Center at 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 (see page 163).

This section contains the following topics:

- CA MSM Documentation (see page 23)
- Getting Started Using CA MSM (see page 24)
- Acquiring Products (see page 34)
- Installing Products (see page 40)
- Maintaining Products (see page 47)
- Setting System Registry (see page 61)
- Deploying Products (see page 86)

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). The PAS retrieves information about the products to which your site is entitled and records these entitlements in a software inventory maintained on your driving system.

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

To do this, complete the following tasks:

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 33), 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 34). 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 35).

After you find your product in the catalog, you can download the product installation packages (see page 35).

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

The product is now ready for you to install or maintain.

**How to Deploy a Product**

The *Software Deployment Service (SDS)* facilitates the deployment of mainframe products from the software inventory of the driving system to the target system, including 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.

1. You first need to set up the system registry:
   a. Determine the systems you have at your enterprise.
   b. Set up remote credentials (see page 83) for those systems.
   c. Set up the target systems (Non-Sysplex (see page 62), Sysplex or Monoplex (see page 63), Shared DASD Cluster (see page 64), and Staging (see page 65)), and validate them.
   d. Add FTP (see page 73) information, including data destination information, to each system registry entry.

2. You then need to set up methodologies (see page 112).

3. Next you need to 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 129), products (see page 103), custom data sets (see page 104), and methodologies (see page 112), 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. Finally, you are ready to deploy the product, which includes taking a snapshot, transmitting to target, and deploying (unpacking) to your mainframe environment.

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 116) 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 116) 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 105).

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 113), 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.

To do this, complete the following tasks:

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 48) 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 49).

3. **Apply the maintenance** (see page 52).

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

The product is now ready for you to deploy.

Access CA MSM Using the Web-Based Interface

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

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

To access CA MSM using the web-based interface

1. Start your web browser, and enter the access URL.
   The login page appears.
   **Note:** If the Notice and Consent Banner appears, read the information provided, and click the link to confirm it.

2. Enter your z/OS login user name and password, and click the Log In button.
   The initial page appears. If you log in for the first time, you are prompted to define your account on the CA Support Online website.
   **Note:** For more information about the interface, click the Help link at the top right corner of the page.
3. Click New.

You are prompted for the 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.

**To update your software catalog**

1. Click the Software Catalog tab.

   **Note:** The information on the Software Status tab for HIPERs and new maintenance is based on the current information in your software catalog. We recommend that you update the catalog on a daily or weekly basis to keep it current.
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 opens that shows the progress of the task. When the task completes, you can click Show Results on the Progress tab to close this dialog and open the task output browser to view the details of the actions. 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.

**To download a product installation package**

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

CA MSM uses the credentials to access the [CA Support Online website](http://www.ca.com).
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 opens that shows the progress of the task. When the task completes, you can click Show Results on the Progress tab to close this dialog and open the task output browser to view the details of the actions. 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 a product and clicking the vendor link in the right panel, but if you use this method and select multiple products, be aware that if one of the selected products cannot be downloaded, the remaining products will not be processed. If this happens, remove the checks from the ones that were processed and repeat the update catalog request.
Migrate Installation Packages Downloaded External to CA MSM

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

Migrating these packages to CA MSM 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 40).

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

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.
To add a product package to CA MSM

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

You are prompted to supply information about the product.

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

The product is added to the software catalog.

3. Click the gen level of the product you want to install on the product tree at the left.

The Base Install Packages section appears at the right.

4. Click the Add External Package button.

You are prompted to identify the package.

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

   Note: If you need to add several packages from the same location, you can use masking (see page 39).

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 37) (or set of maintenance files (see page 50)) from the same location based on a pattern (mask). You can use masking for components, maintenance in USS, and maintenance in data sets. You can use masking for files only, not for directories.

**Masking:** Use the asterisk symbol (*).

- For PDS and PDSE, you can mask members using asterisks.
- For sequential data sets, use the following characters:
  - `?`
    Match on a single character.
  - `*`
    Match on any number of characters within a qualifier of a data set name or any number of characters within a member name or file system name.
  - `**`
    Match on any number of characters including any number of .qualifier within a data set name.

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

**Note:** By default, all files in the list are selected. Make sure you review the list and check what files need to be added.

**Example 1**

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

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

**Example 2**

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

`/a/update/packages/*p0*`
Example 3

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

PUBLIC.DATA.PTFS.**

Example 4

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

PUBLIC.DATA.PTFLIB(RO*)

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

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

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

   ![](Image)

   **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 43).

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

   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 opens that shows the progress of the task. When the task completes, you can click Show Results on the Progress tab to close this dialog and open the task output browser to view the details of the actions. 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 40). 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.

To create a CSI

1. Click Create a New SMP/E CSI from the product installation wizard.
   You are prompted to define a CSI.
2. Specify 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.

To retrieve and list the LMP keys for your products

1. Click the Software Catalog tab, and click the Show LMP Keys link in the Actions section at the left.
   
   ![Software Catalog tab](image)

   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 48)
   - Download Product Maintenance Packages for Old Product Releases and Service Packs (see page 49)
   - Manage Maintenance Downloaded External to CA MSM (see page 50)

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.

To download product maintenance packages

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 opens that shows the progress of the task. When the task completes, you can click Show Results on the Progress tab to close this dialog and open the task output browser to view the details of the actions. 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 49)
Download Maintenance Packages for Old Product Releases and Service Packs

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

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

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

You are prompted to supply information about the product release.

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

   Note: Use the same product name that appears on the product tree, and use the release and gen level values as they appear for Published Solutions 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 opens that shows the progress of the task. When the task completes, you can click Show Results on the Progress tab to close this dialog and open the task output browser to view the details of the actions. 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 52).

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

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

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

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

1. Click the Software Catalog tab, and select the product release for which the maintenance applies.
   The maintenance packages for the release are listed.
2. Click the Add External Maintenance button.
   You are prompted to specify the package type and location.
3. Specify the package type and either the data set name or the USS path.
   **Note**: If you need to add several packages from the same location, you can use masking (see page 39).
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 52)

View Aggregated Package Details

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

To view aggregated package details

1. Click the Software Catalog tab, and select the product release that has the aggregated package whose details you want to view.
   The maintenance packages for the release are listed.
2. Click the Fix # link for the aggregated package.
   The Maintenance Package Details dialog opens.
3. Click the Nested Packages tab.
   A list of nested packages contained in the aggregated package appears.
Manage Maintenance

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

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

The following installation modes are available:

**Receive and Apply**

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.

**To manage maintenance for a product**

1. Click the Software Catalog tab, and select the product from the tree at the left. Maintenance information appears at the right for the releases you have.
2. Click Update Catalog Release for the release on which you want to apply maintenance. The maintenance information is updated.
3. If the information indicates that maintenance is available, click the Release Name link.

   The maintenance packages are listed, for example:

<table>
<thead>
<tr>
<th>Select</th>
<th>Fix #</th>
<th>Description</th>
<th>Confirmed Date</th>
<th>Type</th>
<th>Installed</th>
</tr>
</thead>
<tbody>
<tr>
<td>☑️</td>
<td>005566</td>
<td>&quot;PRODUCT DOCUMENTATION CHANGE&quot;</td>
<td>Jun 27, 2007</td>
<td>PWKPC</td>
<td>Not installable</td>
</tr>
<tr>
<td>☑️</td>
<td>005565</td>
<td>&quot;PRODUCT BRKUP ALERT&quot;</td>
<td>Jun 20, 2007</td>
<td>PWKPC</td>
<td>Not installable</td>
</tr>
<tr>
<td>☑️</td>
<td>005564</td>
<td>&quot;005565&quot;</td>
<td>Jun 17, 2007</td>
<td>PWKPC</td>
<td>Not installable</td>
</tr>
<tr>
<td>☑️</td>
<td>005563</td>
<td>&quot;005564&quot;</td>
<td>Jun 14, 2007</td>
<td>PWKPC</td>
<td>Not installable</td>
</tr>
<tr>
<td>☑️</td>
<td>005562</td>
<td>&quot;005563&quot;</td>
<td>Jun 11, 2007</td>
<td>PWKPC</td>
<td>Not installable</td>
</tr>
<tr>
<td>☑️</td>
<td>005561</td>
<td>&quot;005562&quot;</td>
<td>Jun 08, 2007</td>
<td>PWKPC</td>
<td>Not installable</td>
</tr>
<tr>
<td>☑️</td>
<td>005560</td>
<td>&quot;005561&quot;</td>
<td>Jun 05, 2007</td>
<td>PWKPC</td>
<td>Not installable</td>
</tr>
<tr>
<td>☑️</td>
<td>005559</td>
<td>&quot;005560&quot;</td>
<td>Jun 02, 2007</td>
<td>PWKPC</td>
<td>Not installable</td>
</tr>
<tr>
<td>☑️</td>
<td>005558</td>
<td>&quot;005559&quot;</td>
<td>Jun 29, 2007</td>
<td>PWKPC</td>
<td>Not installable</td>
</tr>
<tr>
<td>☑️</td>
<td>005557</td>
<td>&quot;005558&quot;</td>
<td>Jun 26, 2007</td>
<td>PWKPC</td>
<td>Not installable</td>
</tr>
<tr>
<td>☑️</td>
<td>005556</td>
<td>&quot;005557&quot;</td>
<td>Jun 23, 2007</td>
<td>PWKPC</td>
<td>Not installable</td>
</tr>
</tbody>
</table>

   Red asterisks identify HIPER maintenance packages.

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

   The Maintenance Package Details dialog appears, identifying any prerequisites.

5. Review the information on this dialog, and click Close to return to the Maintenance Packages section.

6. 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.

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

   The packages to install are listed.

8. 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.

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

10. Click Select Zones to review and adjust the zones where the maintenance will be installed, click OK to confirm the selection and return to the wizard, and click Next.

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

SMP/E work DDDEFs of SMPWRKx and SYSUTx, along 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 there is sufficient space 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 automatically update allocation parameters for all DDDEFs, click Retrieve DDDEF. CA MSM provides values for all DDDEFs based on the total size of the selected maintenance packages to be installed. 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 may 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 opens that shows the progress of the task. When the task completes, you can click Show Results on the Progress tab to close this dialog and open the task output browser to view the details of the actions. 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 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 48)
   Download Main
tenance Packages for Old Product Releases and Service Packs (see page 49)

   **View Installation Status of Maintenance Package**

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

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

   Depending on the package status for each zone, you can see available actions for the package. For example, if the package is not received in a CSI zone, the Install action is available.

   **To view installation status of a maintenance package**

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

      The maintenance packages for the release are listed.

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

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

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

A product USERMOD can be provided as a published maintenance package downloaded by CA MSM during the Update Catalog process. When CA MSM downloads a package that includes a ++USERMOD statement, it is loaded under the 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 50).

GROUPEXTEND Mode

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

For some maintenance packages, before you install them, you must first install other maintenance packages (SYSMODs).

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

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

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

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

**How Maintenance in GROUPEXTEND Mode Works**

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

1. Receive all SYSMODs that you want to include by the GROUPEXTEND option.
2. Run the maintenance in Apply check mode.
   - If the task fails, review SMPOUT in the task output to check if there are missing (not received) SYSMODs or HOLDDATA that need to be resolved or bypassed.
   - If the task succeeds, review SMPRPT in the task output to check what SYSMODs were found and applied.
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 needs to correspond to the version of SMP/E that you use.

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

**Manage Maintenance in GROUPEXTEND Mode**

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

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

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 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 to be applied are listed.

Note: If a link in the Status column for a maintenance package is available, you can click it to review a list of zones where the maintenance package is already received, applied, or accepted. Click Close to return to the wizard.

5. Review the packages, and click Next.

The Prerequisites tab of the wizard appears.

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

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

Installation options appear.
7. Specify installation options as follows, and click Next:
   a. Select the installation mode for the selected maintenance.
   b. Review the GROUPEXTEND options and select those you want to apply to the maintenance:
      
      **NOAPARS**
      
      Excludes APARs that resolve error reason ID.
      
      **NOUSERMODS**
      
      Exclude USERMODs that resolve error user ID.
      
   c. (Optional) Enter SYSMODs that should be excluded in the Excluded SYSMODs field. You can enter several SYSMODs separated by a comma.

The Bypass HOLDDATA tab of the wizard appears.

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

9. Click Next.

A summary of the task appears.

10. Review the summary, and click Apply GROUPEXTEND.

A dialog opens that shows the progress of the task. When the task completes, you can click Show Results on the Progress tab to close this dialog and open the task output browser to view the details of the actions. 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 to check what SYSMODs were found and applied.

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

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

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

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

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

To back out a maintenance package from a product release

1. Click the SMP/E Environments tab, and select the SMP/E environment from which you want to back out maintenance on the tree 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: If you want to back out maintenance from all the products in the environment, you can click the Maintenance tab to list all the maintenance packages for the environment.

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

   The maintenance packages for the feature are listed.

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

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

   The Introduction tab of the wizard appears.

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

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

   The packages to back out are listed.

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

   Note: Click Select Zones to review and adjust a list of zones from where the maintenance will be restored, and click OK to confirm the selection and return to the wizard.

   The Prerequisite tab of the wizard appears.

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

   A summary of the task appears.
8. Review the summary, and click Restore.

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

**To view a System Registry**

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 related to the type you selected appears on the right side.
Create a Non-Sysplex System

You can create a Non-Sysplex System Registry.

To create a Non-Sysplex system registry

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

   The New Non-Sysplex System dialog appears.

   Note: The asterisk indicates that the field is mandatory.

2. Enter the following and click Save:

   Non-Sysplex System Name
   Enter the Non-Sysplex system name.
   Limits: Maximum 8 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: Maximum 255 characters.

   CCI System ID
   Enter the CCI system ID.
   Limits: Maximum 8 characters.

   The Non-Sysplex System is saved, and its name appears in the Non-Sysplex System Registry List on the left.

   Note: To withdraw this create request, click Cancel

   Note: 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:

   Property Name: z/OS LPAR Name, Value: ** Not Applicable **.
Create a Sysplex or Monoplex

You can create a Sysplex or Monoplex 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.

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.

To create a Sysplex or Monoplex system registry

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

<table>
<thead>
<tr>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Non-Sysplex System</td>
</tr>
<tr>
<td>Create Sysplex</td>
</tr>
<tr>
<td>Create Shared DASD Cluster</td>
</tr>
<tr>
<td>Create Staging System</td>
</tr>
<tr>
<td>Maintain Data Destinations</td>
</tr>
</tbody>
</table>

   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:** Maximum 8 characters.

   **Description**
   Enter the description.
   **Limits:** Maximum 255 characters.

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

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

The Sysplex System is saved, and its name appears in the Sysplex System Registry List on the right.

**Note:** Click Cancel to withdraw this create request.
Note: z/OS systems running under VM are treated as being in basic mode and not LPAR mode. As result, the LPAR number is null in the z/OS control block. When this is the case, the system validation output will include the following message:

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

Create a Shared DASD Cluster

You can create a Shared DASD Cluster.

To create a Shared DASD Cluster

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

   The New Shared DASD Cluster dialog appears.

   Note: The asterisk indicates that the field is mandatory.

2. Enter the following and click Save:

   ** Name 

   Enter the Shared DASD Cluster name.

   Limits: Maximum 8 characters.

   Note: Each Shared DASD Cluster name must be unique and it is not case-sensitive. For example DASD1 and dasd1 are the same Shared DASD Cluster name. A Staging System may have the same name as a Non-Sysplex, Sysplex, or Shared DASD Cluster.

   ** Description 

   Enter the description.

   Limits: Maximum 255 characters.

The Shared DASD Cluster is saved, and its name appears in the System Registry Cluster List on the right.

Note: Click Cancel to withdraw this create request.
Create a Staging System

You can create a Staging System.

To create a Staging System

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

   The New Staging System dialog appears.

   Note: The asterisk indicates that the field is mandatory.

2. Enter the following and click Save:

   Name
   Enter the Staging System name.
   Limits: Maximum 8 characters.

   Note: Each Staging System name must be unique and is not case-sensitive. For example STAGE1 and stage1 are the same Staging System name. A Staging System may have the same name as a Non-Sysplex, Sysplex, or Shared DASD Cluster.

   Description
   Enter the description.
   Limits: Maximum 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, but not make any changes.

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.

To change a system registry

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 related to the type 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 62), Sysplex (see page 63), Shared DASD Cluster (see page 64), or Staging System (see page 65).
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 71), 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 72).

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 69).

**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 69).

**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 69).

**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 69).

**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

When a validation fails, you can investigate it, make corrections, and validate it again. Use the following procedures in this section:

- **Investigate a Failed Validation using the Tasks Page** (see page 69)
- **Investigate a Failed Validation Immediately After a Validation** (see page 70)
- **Download a Message Log** (see page 70)
- **Save a Message Log as a Data Set** (see page 71)
- **View Complete Message Log** (see page 71)

**Note:** The CA MSM screen samples in these topics use a Non-Sysplex system as an example, but the method also works for a Sysplex or a Shared DASD Cluster.

Investigate a Failed Validation Using Task Output Browser

When a validation fails, you can investigate it, make corrections, and validate it again.

**To investigate a failed validation using the Task Output Browser**

1. On the System Registry Page, in the left hand column 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 Validate System Task Output Browser appears.

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 determine the steps required to troubleshoot them.

7. Correct the issue and validate again.

**Investigate a Failed Validation After Validation**

When a validation fails, you can investigate it, make corrections, and validate it again.

**To investigate a failed validation immediately after validation**

1. On the System Registry Page, in the left hand column, find the system with a validation status error, and make note of it.
2. Click Details to see the error details.
3. If the Message states *Please validate the system again*, click Validate. The system validates again.
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 determine the steps 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 and click Download Zipped Output button on the General menu bar. You will be requested to save this file.
- To download as TXT, click the Deployment Name or the Deployment Results on the left tree, click the Action button on the MessageLog bar and click the Download as TXT. You will be requested to save this file.
- To download as ZIP, click the Deployment Name or the Deployment Results on the left tree, click the Action button on the MessageLog bar and click the Download as ZIP. You will be requested to save this file.
Save a Message Log as a Data Set

You can save a message log as a data set.

To save as a data set

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

   The Save Output as Data Set dialog appears.

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

   **Note:** The asterisk indicates that the field is mandatory.

2. Enter the following 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 that the deployment will be unpackaged on. That is, which system CCI is spawned to run the unpackaging.

When deploying to a Shared DASD Cluster and/or Sysplex, the deployment is sent to only one system in that configuration to be unpackaged. It is expected that all other systems within that configuration will have access to the unpackaged deployment.

For a Shared DASD Cluster or Sysplex, the URI must be the URI of the Contact System. You must also set up Remote Credentials for the contact system, because they will be used to retrieve the deployment results.
zFS Candidate Volumes

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

Use one or more zFS candidate volumes when your environmental setup dictates that zFS container data sets are directed to the specified zFS candidate volumes used by CA MSM in the IDCAMS statement to create the zFS container VSAM data set.

The zFS candidate volumes are only required if the following is 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 hierarchical storage management system.

You can also use the following standard IBM techniques:
- Allocation exits
- ACS routines

If none of these options are implemented by the customer, then a candidate list of volumes is needed to tell z/OS where to place the zFS archive.

Maintain a System Registry using the List Option

You can maintain system registry entries using the List Option.

To maintain a system registry
1. Click the System Registry tab.
   The System Registry window appears.
2. On the right, in the System Registry panel click the System Type link.
   The detailed system entry information appears.
Delete a System Registry

You can delete a system registry.

**To delete a system registry**

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

   The system list appears.

2. Click the Select box for each system registry you want to delete, click Delete, and then click OK to confirm.

   The system is deleted.

FTP Locations

The FTP (see page 73) Locations lists the current FTP locations for this system. You can add (see page 73), edit (see page 75), set default (see page 76), or remove (see page 76) FTP (see page 73) 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.

FTP and Deployments

*File Transfer Protocol (FTP)* is a network protocol responsible for the transfer of information in the form of files from one computer to another over the Internet.

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

You can add FTP (see page 73) locations.

To add FTP locations

1. Click the System Registry tab, and select Non-Sysplex Systems, Sysplexes, or Shared DASD Clusters from the tree on the left side.
   
   *Note:* You cannot set network locations for Staging Systems.
   
   Information about the systems related to the type 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 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 75)
- Set FTP Location Default (see page 76)
- Delete FTP Locations (see page 76)
Edit FTP Locations

You can edit FTP (see page 73) locations.

**Note:** The asterisk indicates that the field is mandatory.

**To edit FTP locations**

1. Click the System Registry tab, and select Non-Sysplex Systems, Sysplexes, or Shared DASD Clusters from the tree on the left side.
   
   **Note:** You cannot set network locations for Staging Systems.
   
   Information about the systems related to the type 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 73) location default.

To set an FTP location default

1. Click the System Registry tab, and select Non-Sysplex Systems, Sysplexes, or Shared DASD Clusters from the tree on the left side.
   
   **Note:** You cannot set network locations for Staging Systems.
   
   Information about the systems related to the type 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 73) locations.

To delete FTP locations

1. Click the System Registry tab, and select Non-Sysplex Systems, Sysplexes, or Shared DASD Clusters from the tree on the left side.
   
   **Note:** You cannot set network locations for Staging Systems.
   
   Information about the systems related to the type 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. 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.
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.

**To create a data destination**

1. Click the System Registry tab, and in the Actions section click the Maintain Data destinations link.
   The Maintains Data Destinations dialog appears.
2. Click Create.
   The New Data Destination dialog appears.
   **Note:** The asterisk indicates that the field is mandatory.
3. Enter 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 72).

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.

To add a current data destination to an existing system
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 82), or create (see page 78) data destinations.

**To maintain existing data destinations**

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 72).

**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.

To set a default for a current data destination
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 link you want to set the data destination default to.
   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 box select Set as Default.
   The word Default appears in the Default column.

Delete Data Destinations

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

Important: A grayed select box indicates that the data destination is assigned and it cannot be deleted. It can be edited.

To delete data destinations
1. Click the System Registry tab, and select Non-Sysplex Systems, Sysplexes, or Shared DASD Clusters from the tree on the left side.
   Note: You cannot set network locations for Staging Systems.
   Information about the systems related to the type 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 box 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. You must use the Apply button to apply and save your changes.

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

You can add (see page 83), edit (see page 84), or delete (see page 85) remote credentials.

Add Remote Credentials

You can add remote credentials.

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

**To add remote credentials**

1. Click the Settings tab, and select Remote Credentials from the tree on the left side. Detailed information appears on the right side.
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:** 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 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. It is the responsibility of the user to have the correct Owner, Remote User ID, Remote System Name, password, and authenticated authorization before creating a new remote credential.

To edit remote credentials

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.

**To delete remote credentials**

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 88).
2. Define a name and description (see page 88).
3. Select a CSI (see page 89).
4. Select a product (see page 89).
5. Select a custom data set (see page 90).
6. Select a methodology (see page 90).
7. Select a system (see page 92).
8. Preview and save (see page 92).
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 93) 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.

**To define the name and description**

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 93) until a successful snapshot has been created.
Select a CSI

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

To select a CSI

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 93) 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.

To select a product

1. On the Product Selection step, select a product from the list.
   - 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.
   - 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 93) 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 parts path.

To select a custom data set

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 105).

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 93) until a successful snapshot has been created.

More information:

Add a Custom Data Set (see page 105)

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.

To select a Methodology

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 113).

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 93) until a successful snapshot has been created.

**More information:**

Create a Methodology (see page 113)
Select a System

After you select a methodology, you select a system.

To select a system

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 93) 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.

To change deployments

1. Click the Deployments tab. The Deployment window appears.
2. On the right, in the Deployments panel click the current deployment link. The detailed deployment information appears.
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 86).

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

The Edit Methodology window (see page 126) appears. The Deployment ID is the value of the MSMID variable.

**Note:** You can perform the following actions:

- You can select (see page 103), add (see page 103), or remove (see page 104) a product, and.
- You can select (see page 130), add (see page 131), or remove (see page 131) a system.
- You can select (see page 105), add (see page 105), or remove (see page 111) 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 101)

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 99)**

You can reset a deployment status when the deployment has a status of *snapshot in progress, transmitting, or deploying.* See reset status (see page 99) for a list of deleted files.

7. Click Save on the Deployment Details window.

You changes are saved.

More information:

- **Edit a Methodology** (see page 126)
- **View the Product List** (see page 103)
- **Add a Product** (see page 103)
- **Remove a Product** (see page 104)
- **View a System List** (see page 130)
- **Add a System** (see page 131)
- **Remove a System** (see page 131)
- **Confirm a Deployment** (see page 101)

Deployment Maintenance

You can maintain a deployment in the following ways:

- Adding
  - **System** (see page 131)
  - **Product** (see page 103)
  - **Custom Data Sets** (see page 105)

- **Delete**

- **Removing**
  - **System** (see page 131)
  - **Product** (see page 104)
  - **Custom Data Sets** (see page 111)

- **Updating/Editing**
  - **Maintain Deployments** (see page 93)
  - **Edit a Custom Data Set** (see page 108)
Failed Deployments

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

- **Investigate a Failed Deployment Using the Tasks Page** (see page 97)
- **Download a Message Log** (see page 70)
- **Save a Message Log as a Data Set** (see page 71)
- **View Complete Message Log** (see page 71)

**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 70)
- **Save a Message Log as a Data Set** (see page 71)
- **View Complete Message Log** (see page 71)
Investigate a Failed Deployment

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

To investigate a failed deployment

1. On the Deployments Page, in the left hand column, find the deployment with an error and note its name.
2. Click the Tasks tab and then click Task History.
   
   **Note:** Click Refresh on the right hand side of the Task History bar to refresh the Task History display.
3. At the Show bar, select All tasks, or select My tasks to only see the tasks assigned to you.
   
   **Note:** You can refine the task list further by selecting task and status types from the drop-down lists, and then sort by Task ID.
4. Find the failed deployment step and click the link in the Name column.
   
   The Task Output Browser appears.

   ![Task Output Browser](image)

5. 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.
6. Correct the issue and deploy again.
More information:

- Download a Message Log (see page 70)
- Save a Message Log as a Data Set (see page 71)
- View Complete Message Log (see page 71)

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 and click Download Zipped Output button on the General menu bar. You will be requested to save this file.

- To download as TXT, click the Deployment Name or the Deployment Results on the left tree, click the Action button on the MessageLog bar and click the Download as TXT. You will be requested to save this file.

- To download as ZIP, click the Deployment Name or the Deployment Results on the left tree, click the Action button on the MessageLog bar and click the Download as ZIP. You will be requested to save this file.

Save a Message Log as a Data Set

You can save a message log as a data set.

To save as a data set

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

   The Save Output as Data Set dialog appears.

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

   **Note:** The asterisk indicates that the field is mandatory.

2. Enter the following 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:**
   
   Volsers: 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 69) 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's 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 69) 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.

To delete a deployment
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.

To confirm a deployment
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.

To view the product list
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.

Add a Product

You can add a product to a deployment.

To add a product to a deployment
1. Click the Deployments tab. The Deployments window appears.
2. On the right, in the Deployments panel click the Current Deployment link.
   A list of current deployments appears.
3. Click the deployment name link.
4. In the Product List panel click Add Products.
   The Add Products wizard appears.
5. Select a CSI and click Next.
   The Product Selection appears.
6. Select a product.
7. If there is a text icon in Text column, click the text icon to read the instructions supplied by CA Support for product, data sets, and other necessary information.
8. Click the "I have read the associated text by selecting the text icon from the list about" box. This box appears only if there is a text icon.
   **Note:** You will not be able to click Next until you click this box.
9. Click Next.
   The Custom Data Set Selection appears
10. If needed, select or add a custom data set (see page 105).
11. Click Add Products.
    The Product is added.
Remove a Product

You can remove a product from a deployment.

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

**To remove a product from a deployment**

1. Click the Deployments tab. The Deployment window appears.
2. On the right, in the Deployments panel click the Current Deployment link.
   
   A list of current deployments appears.
3. Select the deployment that you want to remove the product from.
4. In the Product List panel, select a product to remove.
5. Click the Remove link.
6. Click OK to the Remove Products confirmation window.
   
   The product is removed.

Custom Data Sets

You can view, **add** (see page 105), **edit** (see page 108), and **remove** (see page 111) custom data sets from a deployment.

A custom data set is a data set that contains either a z/OS data set or USS parts 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 116) 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 116)), 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.

To view custom data sets
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.

To add custom data sets to a deployment
1. Click the Deployments tab.
   The Deployments window appears.
2. On the right, in the Deployments panel, click the Current Deployment link.
   A list of current deployments appears.
3. Click the deployment name link.
4. In the 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 116).

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

   **Limits:** Maximum 64 characters.

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

   - When you enter the mask, it consists of one or more qualifiers separated by periods, and has a maximum input length of 64 characters, including the periods.
   - While you are entering the mask, CA MSM validates the mask by replacing symbolics first with the minimum possible values, and then with the maximum possible 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 possible 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 116). 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 116).

   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 116).

   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 containers mount point. Most leaves 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.

**To edit a custom data set**

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 116).

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

**Limits:** Maximum 64 characters.

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

- When you enter the mask, it consists of one or more qualifiers separated by periods, and has a maximum input length of 64 characters, including the periods.
- While you are entering the mask, CA MSM validates the mask by replacing symbolics first with the minimum possible values, and then with the maximum possible 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 possible 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 116). The remote path is the path were 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 116).

   **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 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 116).

   **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 containers mount point. Most leaves 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.

To remove a custom data set

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 113), maintain, edit (see page 126), and delete (see page 129) 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 116).

  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.

**To create a methodology**

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 116).

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

**Limits:** Maximum 64 characters.

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

- When you enter the mask, it consists of one or more qualifiers separated by periods, and has a maximum input length of 64 characters, including the periods.

- While you are entering the mask, CA MSM validates the mask by replacing symbolics first with the minimum possible values, and then with the maximum possible 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 possible 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/&MSMSYNSM./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.

Transport
to MINIPLEX: FTP

Target Libraries on MINIPLEX
Source DSN: CAILIB   DSN: MF20.MSM.EZT.CAILIB
Target DSN: &SYSUID..&MSMDID..&MSMHLQ..&MSMMLQ..&MSNLLQ.
Resolved as: USERID4.D???.MF20.DMSM.EZT.DCAILIB.CAILIB

Source DSN: CAIMAC   DSN: MF20.MSM.EZT.CAIMAC
Target DSN: &SYSUID..&MSMDID..&MSMHLQ..&MSMMLQ..&MSNLLQ.
Resolved as: USERID4.D???.MF20.DMSM.EZT.DCAIMAC.CAIMAC

Source DSN: CAIJCL   DSN: MF20.MSM.EZT.CAIJCL
Target DSN: &SYSUID..&MSMDID..&MSMHLQ..&MSMMLQ..&MSNLLQ.
Resolved as: USERID4.D???.MF20.DMSM.EZT.DCAIJCL.CAIJCL

SNP/E Environment
Transported to MINIPLEX: no
EZT Compiler has the following APARs applied:

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 105) with both the USS radio button and the Container copy radio button set. It is of primary value in remote path.

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

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

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

Remote path: &MSMMPN.

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

**MSMSYSNM**

This is the CA MSM system object name.

**SYSCLONE**

This is the shorthand name of the system.

**Limits:** Maximum 2 characters.

**SYSNAME**

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

**SYSPLEX**

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

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

**SYSUID**

The current user ID.

**Target Libraries**

**MSMHLQ**

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

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

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

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

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

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

MSMLLQ

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

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

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

MSMSLQ

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

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

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

MSMPREF

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

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

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

**Example:** Assume 3 target libraries in a deployment.

DSN = USER456.LIBR473.CAIPROC
DSN = USER456.LIBR473.CAILOAD
DSN = USER456.LIBR473.CAIEXEC

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.CAIEXEC

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 129) methodologies.

To edit or replace a methodology

1. Click the Deployments tab, and in the Actions section click the Maintain Methodologies link. The Maintain Methodologies select window appears.

   ![Maintain Methodologies](image)

   **Note:** A grayed select box indicates that the methodology is assigned and cannot be removed. It can be edited.
Deploying Products

126 Installation Guide

2. Select a methodology. Select Edit from Actions list.

The Methodology window appears for editing (see page 126).

More information:

Delete Methodologies (see page 129)
Edit a Methodology (see page 126)

Edit a Methodology

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

To edit a methodology

1. Click the Deployments tab, and in the Actions section click the Maintain Methodologies link.

2. Select the methodology that you want to edit and click Edit.

The 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 116).

**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 116).

**Example**: CAPRODS.&SYSID. - in this case the &SYSID. will be replaced by its values. If the SYSID that is being deployed to is XX16 the DSN mask will be: CAPRODS.XX16

**Limits**: Maximum 64 characters.

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

- When you enter the mask, it consists of one or more qualifiers separated by periods, and has a maximum input length of 64 characters, including the periods.
- While you are entering the mask, CA MSM validates the mask by replacing symbolics first with the minimum possible values, and then with the maximum possible 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 possible 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 replace 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 116)

**Delete Methodologies**

**To delete methodologies**

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 product as they moves thru 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.

To view a system list

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.

To add a system
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.

To remove a system
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.

**Deployment Summary**

**Information**

**Note:** When you have completed the procedures in this section, go to [Configuring Your Product](see page 163) (see page 163).
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 135)
- Allocate and Mount a File System (see page 141)
- Copy the Product Pax Files into Your USS Directory (see page 143)
- Create a Product Directory from the Pax File (see page 148)
- Copy Installation Files to z/OS Data Sets (see page 149)
- Receiving the SMP/E Package (see page 150)
- Clean Up the USS Directory (see page 154)
- Apply Maintenance (see page 155)

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 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 dedicated to Pax-Enhanced ESD and create the directory in this file system. Ensure that all users who will be working with pax files have write authority to the directory.
2. Copy the product pax files into your USS directory. To download files, choose one of the following options:
   - Download a zip file from CA Support Online to your PC, unzip the file, and then upload the product pax files to your USS file system.
   - FTP the pax files from CA Support Online directly to your USS directory.
   **Note:** Perform Steps 3 through 6 for each pax file that you upload to your USS directory.

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

4. Use the SMP/E GIMUNZIP utility to create z/OS installation data sets. The file UNZIPJCL in the directory created by the pax command in Step 3 contains a sample job to GIMUNZIP the installation package. Edit and submit the UNZIPJCL job.

5. Receive the SMP/E package. For this step, use the data sets created by GIMUNZIP in Step 4. Perform a standard SMP/E RECEIVE using the SMPPTFIN and SMPHOLD (if applicable) DASD data sets. Also, specify the high-level qualifier for the RELFILEs on the RFPREFIX parameter of the RECEIVE command.

6. Proceed with product installation. Consult product-specific documentation, including AREADME files and installation notes to complete the product installation.

7. (Optional) Clean up the USS directory. Delete the pax file, the directory created by the pax command, all of the files in it, and the SMP/E RELFILEs, SMPMCS, and HOLDDATA data sets.

**More Information:**

- [USS Environment Setup](#) (see page 140)
- Allocate and Mount a File System (see page 141)
- Copy the Product Pax Files into Your USS Directory (see page 143)
- Create a Product Directory from the Pax File (see page 148)
- Copy Installation Files to z/OS Data Sets (see page 149)

**How the Pax-Enhanced ESD Download Works**

**Important!** To download pax files for the SMP/E installation as part of the Pax-Enhanced ESD process, you must have write authority to the UNIX System Services (USS) directories used for the ESD process and available USS file space before you start the procedures in this guide. For additional ESD information, go to [ca.com/mainframe](#). Under Events, we offer an ESD webcast to further explain the Pax-Enhanced ESD process.
Use the following process to download files using Pax-Enhanced ESD:

1. Log in to https://support.ca.com/, and click Download Center.
   The CA Support Online web page appears.
2. Under Download Center, select Products from the first drop-down list, and specify the product, release, and genlevel (if applicable), and click Go.
   The CA Product Download window appears.
3. Download an entire CA 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 137) topic explains how the download interface works.
   **Note:** For traditional installation downloads, see the Traditional ESD User Guide. Go to https://support.ca.com/, log in, and click Download Center. A link to the guide appears under the Download Help heading.
4. Perform the steps to install the product based on the product-specific steps.
   The product is installed on the mainframe.

**ESD Product Download Window**

CA Technologies product ESD packages can be downloaded multiple ways. Your choices depend on the size of the individual files and the number of files you want to download. You can download the complete product with all components or you can select individual pax and documentation files for your product or component.
The following illustration shows sample product files. It lists all components of the product. You can use the Download Cart by checking one or more components that you need or check the box for Add All to cart. If you prefer to immediately download a component, click the Download link.

![Product Components Table]

Clicking the link for an individual component takes you to the Download Method page.
Depending on the size and quantity of product files ordered, the Download Method screen could also have these options:

**Note:** For mainframe downloads using this HTTP method, click the Learn More link.
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 shown by the Zip Download Request examples in the next screen.

**USS Environment Setup**

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

- Receive product pax files from CA Support Online.
- Perform utility functions to unpack the pax file into MVS data sets that you can use to complete the product installation.
We recommend that you allocate and mount a file system dedicated to Pax-Enhanced ESD. The amount of space that you need for the file system depends on the following variables:

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

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

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

### Allocate and Mount a File System

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

This procedure details how to perform the following tasks:

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

**Important!** USS commands are case-sensitive.
To allocate and mount the file system

1. Allocate the HFS. For example:
   
   ```
   //ALCHFS  EXEC  PGM=IEFBR14
   //CAESD  DD  DSN=yourHFS dataset name,
   // DISP=(NEW,CATLG,DELETE),UNIT=3390,
   // DSNTYPE=HFS,SPACE=(CYL,(primary,secondary,1))
   ```
   
   The HFS is allocated.

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

2. Create a mount point for the file system. This example shows how to create a /CA/CAESD directory in an existing directory, /u/maint. From the TSO OMVS shell, enter the following commands:
   
   ```
   cd /u/maint/
   mkdir CA
   cd CA
   mkdir CAESD
   ```
   
   **Note:** This document refers to this structure as yourUSSESDdirectory.
   
   The mount point is created.

3. Mount the file system. For example, from TSO, enter the following command:
   
   ```
   MOUNT     FILESYSTEM('yourHFS dataset name')
   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 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's pax file into the USS directory you set up. Use one of the following methods:

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

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

**Important!** 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 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 136)
- ESD Product Download Window (see page 137)
Copy the Product Pax Files into Your USS Directory

Download Using Batch JCL

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

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

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

To download files using batch JCL

1. Supply a valid JOB statement.
2. Replace yourTCPIP.PROFILE.dataset with the name of the TCPIP profile data set for your system. Consult your local network administrators, if necessary.
   The job points to your profile.
3. Replace YourEmailAddress with your email address.
   The job points to your email address.
4. Replace yourUSSESDDirectory with the name of the USS directory that you use for ESD downloads.
   The job points to your USS directory.
5. Locate the product component to download on the CA Support Product Download window.
   You have identified the product component to download.
6. Click Download for the applicable file.
   Note: 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 world-wide content delivery network (CDN). If you are not able to download using the Preferred FTP method, check the security restrictions for all servers that company employees can download from that are outside of your corporate network.

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

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

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

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

   **Note:** For details regarding FTP, see the FTP Help document link in the Review Download Requests window and the Learn More link available in the Download Methods window.

9. Submit the job.

   **Important!** If your FTP commands are incorrect, 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 running the JCL, the pax file resides in the mainframe USS directory that you supplied.
Example: CAtoMainframe.txt, JCL

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

```
//GETPAX   JOB (ACCOUNTNO), 'FTP GET ESD PACKAGE',
// MSGCLASS=X,CLASS=A,NOMFILE=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’s statements in this JCL maybe *
//*   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 "yourUSSESDirectory" 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 *
//*********************************************************************

//GETPAX   EXEC PGM=FTP,REGION=0K
//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 yourUSSESDirectory
binary
get FTP location
quit
```
Download Files to Mainframe through a PC

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

To upload files to the mainframe through a PC

1. Follow the procedures in How the Pax-Enhanced ESD Download Works (see page 9) to download the product pax or zip file to your PC. If you download a zip file, first unzip the file to use the product pax files.

   The pax or zip file resides on your PC.

2. Open a Windows command prompt.

   The command prompt appears.

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

   The pax file is transferred to the mainframe.

Example: FTP Commands

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

```text
ftp mainframe
userid
password
bin
lcd C:\PC\folder\for\thePAXfile
cd /yourUSSESDdirectory/
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 in the lower left corner of the PDF reader. This opens a window displaying attachments. Double-click the file to view the sample JCL.

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

1. Supply a valid JOB statement.
2. Replace `yourUSSESDDirectory` with the name of the USS directory that you use for ESD downloads.
   - The job points to your specific directory.
3. Replace `paxfile.pax.Z` with the name of the pax file.
   - The job points to your specific pax file.
4. Submit the job.
   - The job runs and creates the product directory.

**Note:** After making the changes noted in the job, if the PARM= statement exceeds 71 characters, uncomment and use the second form of UNPAXDIR instead. This sample job uses an X in column 72 to continue the PARM= parameters to a second line.
Example Job to Execute the Pax Command (Unpackage.txt)

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

```
//ESDUNPAX JOB (ACCOUNTNO),’UNPAX ESD PACKAGE ‘,
// MSGCLASS=X,CLASS=A,NOTIFY=&SYSUID

ifndef ESDUNPAX JOB (ACCOUNTNO),’UNPAX ESD PACKAGE ‘,
ifndef 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 "yourUSSESDirectory" 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 /yourUSSESDirectory/; pax -rvf paxfile.pax.Z'  
```
3. Change the SMPDIR DD PATH to the product-specific directory created by the pax command.
Your view is of the product-specific directory.

4. If ICSF is not active, perform the following steps:
   a. Change the SMPJHOME DD PATH to your Java runtime directory. This directory
      varies from system to system.
   b. Perform one of the following steps:
      ■ Change the SMPCPATH DD PATH to your SMP/E Java application classes
         directory, usually /usr/lpp/smp/classes/.
      ■ Change HASH=YES to HASH=NO on the GIMUNZIP parameter.

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

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

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

6. Submit the UNZIPJCL job.

   The UNZIPJCL job 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 you specified in the
   UNZIPJCL job. You use these data sets to perform the product installation. The pax
   file and product-specific directory are no longer needed at this point.

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

---

Receiving the SMP/E Package

If you are installing the package into a new SMP/E environment, use the sample jobs
included with the product to set up an SMP/E environment before proceeding.

At this point, complete the SMP/E RECEIVE using files on DASD that the UNZIPJCL job
created. Consult the product sample JCL library that contains a sample job customized
to receive the product from DASD. Specifically, you must specify the following values:

■ DASD data set names for SMPPTFIN and SMPHOLD (if applicable)
■ The HLQ that you used in the UNZIPJCL job on the RFPREFIX parameter on the
  RECEIVE command
How to Install Products Using Native SMP/E JCL

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

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

**Note:** The CA JARS product can be installed in either of two ways: you can install the full product including JARS/OLF, or you can install CA JARS base only without JARS/OLF. The path you choose determines the value of xxx in the following installation steps:

- Substitute AWF for xxx if you are installing the full product including JARS/OLF (for example, AWFSEDIT).
- Substitute AJR for xxx if you are installing only the base CA JARS without JARS/OLF (for example AJRSEDIT).
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 JARS RA. External DDDEF data sets are required. The default is NULLFILE.

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

Note: We recommend that you make a backup copy of the SAMPJCL members before customizing them.

To prepare the SMP/E environment for your product

1. Customize the macro xxxSEDIT 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 xxxSEDIT on the TSO command line, and press Enter to replace the defaults with your specifications.

   The macro is ready to customize your 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 xxxSEDIT macro each time you open a new SAMPJCL member. To edit all SAMPJCL members simultaneously, read and follow the instructions in the xxxEDALL member.

2. Open the SAMPJCL member xxx1ALL in an edit session and execute the xxxSEDIT macro from the command line.

   xxx1ALL is customized.

3. Submit xxx1ALL.

   This job produces the following results:
   - The target and distribution data sets for CA JARS RA are created.
   - Unique SMPLTS, SMPMTS, SMPSCDS, and SMPSTS data sets for this target zone are created.

   Remove this embedded object if your product does not use USS.

4. Open the SAMPJCL member xxx2CSI in an edit session and execute the xxxSEDIT macro from the command line.

   xxx2CSI is customized.
5. Submit xxx2CSI.
   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.
   Remove this embedded object if your product does not use USS.

**Run the Installation Jobs for a Pax Installation**

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

**To run the installation jobs**

1. Open the SAMPJCL member xxx3RECD in an edit session and execute the xxxSEDIT macro from the command line.
   xxx3RECD is customized.

2. Submit the yourhlq.SAMPJCL member xxx3RECD to receive SMP/E base functions.
   CA JARS RA is received and now resides in the global zone.

3. Open the SAMPJCL member xxx4APP in an edit session and execute the xxxSEDIT macro from the command line.
   xxx4APP is customized.

4. Submit the yourhlq.SAMPJCL member xxx4APP to apply SMP/E base functions.
   Your product is applied and now resides in the target libraries.

5. Open the SAMPJCL member xxx5ACC in an edit session and execute the xxxSEDIT macro from the command line.
   xxx5ACC is customized.

6. Submit the yourhlq.SAMPJCL member xxx5ACC 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 created by the pax command and all of the files in it
- SMP/E RELFILEs, SMPMCS, and HOLDDATA MVS data sets
  These data sets have the HLQ that you assigned in the UNZIPJCL job.

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

To delete the pax files and product-specific directories

1. Navigate to your Pax-Enhanced ESD USS directory.
   Your view is of the applicable USS directory.
2. Delete the pax file by entering the following command:
   ```bash
   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:
   ```bash
   rm -r product-specific-directory
   
   product-specific-directory
   ```
   Specifies the product-specific directory created by the pax command.
   The product-specific directory is deleted.

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

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

To apply maintenance

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

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

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

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

4. Open the SAMPJCL member xxx6RECP in an edit session and execute the xxxSEDIT macro from the command line.

   xxx6RECP is customized with your JOB statement, CSI location, and zone names.

5. Customize the xxx6RECP SMPPTFIN and SMPHOLD DD statements to reference the FB 80 data sets for the PTFs and HOLDDATA.

6. Submit xxx6RECP.

   The PTFs and HOLDDATA are received.

7. Open the SAMPJCL member xxx7APYP in an edit session and execute the xxxSEDIT macro from the command line.

   xxx7APYP is customized.

8. Submit xxx7APYP.

   The PTFs are applied.

9. (Optional) Open the SAMPJCL member xxx8ACCP in an edit session and execute the xxxSEDIT macro from the command line.

   xxx8ACCP is customized.

10. (Optional) Submit yourhlq.SAMPJCL member xxx8ACCP.

    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.
**HOLDDATA**

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

**Note:** When you have completed the procedures in this section, go to [Configuring Your Product](#) (see page 163).
Chapter 5: Installing Your Product from Tape

This section contains the following topics:

Unload the Sample JCL from Tape (see page 157)
How to Install Products Using Native SMP/E JCL (see page 158)
Apply Maintenance (see page 161)

Unload the Sample JCL from Tape

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

To unload the sample JCL from tape

1. Run the following sample JCL:

   //COPY EXEC PGM=IEBCOPY,REGION=4096K
   //SYSPRINT DD SYSOUT=*  
   //SYSUT1 DD DSN=CAI.SAMPJCL,DISP=OLD,UNIT=unitname,VOL=SER=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.

   **nnnnnnn**

   Specifies the tape volume serial number.

   **yourhlq**

   Specifies the data set prefix for the installation.

   **sysda**

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

   The SAMPJCL data set is created and its contents are downloaded from the tape.
2. Continue with one of the following options:
   - If you already have the SMP/E environment set up, go to Run the Installation Jobs for a Tape Installation.
   - If you do not have the SMP/E environment set up, go to Prepare the SMP/E Environment for Tape Installation.

How to Install Products Using Native SMP/E JCL

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

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

Note: The CA JARS product can be installed in either of two ways: you can install the full product including JARS/OLF, or you can install CA JARS base only without JARS/OLF. The path you choose determines the value of xxx in the following installation steps:
   - Substitute AWF for xxx if you are installing the full product including JARS/OLF (for example, AWFSEDIT).
   - Substitute AJR for xxx if you are installing only the base CA JARS without JARS/OLF (for example, AJRSEDIT).
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 JARS RA. External DDDEF data sets are required. The default is NULLFILE.

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

**Note**: We recommend that you make a backup copy of the SAMPJCL members before customizing them.

To prepare the SMP/E environment for your product

1. Customize the macro xxxSEDIT 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 xxxSEDIT on the TSO command line, and press Enter to replace the defaults with your specifications.

   The macro is ready to customize your SAMPJCL members.

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

2. Open the SAMPJCL member xxx1ALL in an edit session and execute the xxxSEDIT macro from the command line.

   xxx1ALL is customized.

3. Submit xxx1ALL.

   This job produces the following results:
   - The target and distribution data sets for CA JARS RA are created.
   - Unique SMPLTS, SMPMTS, SMPSCDS, and SMPSTS data sets for this target zone are created.

   Remove this embedded object if your product does not use USS.

4. Open the SAMPJCL member xxx2CSI in an edit session and execute the xxxSEDIT macro from the command line.

   xxx2CSI is customized.
5. Submit xxx2CSI.
   This job produces the following results:
   - The CSI data set is defined.
   - The SMPPTS and SMPLOG data sets are allocated.
   - The global, target, and distribution zones are initialized.
   - The DDDEF entries for your product are created.
   - The DDDEFs for the required SMP/E data sets are created.

**Run the Installation Jobs for a Tape Installation**

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

**To run the installation jobs**

1. Open the SAMPJCL member xxx3RECT in an edit session and execute the xxxSEDIT macro from the command line.
   
   **Note:** Comment out any unwanted FMIDs.
   
   xxx3RECT is customized.

2. Submit the `yourhlq.SAMPJCL` member xxx3RECT to receive SMP/E base functions.
   
   CA JARS RA is received and now resides in the global zone.

3. Open the SAMPJCL member xxx4APP in an edit session and execute the xxxSEDIT macro from the command line.
   
   **Note:** Comment out any unwanted FMIDs.
   
   xxx4APP is customized.

4. Submit the `yourhlq.SAMPJCL` member xxx4APP to apply SMP/E base functions.
   
   Your product is applied and now resides in the target libraries.

5. Open the SAMPJCL member xxx5ACC in an edit session and execute the xxxSEDIT macro from the command line.
   
   **Note:** Comment out any unwanted FMIDs.
   
   xxx5ACC is customized.

6. Submit the `yourhlq.SAMPJCL` member xxx5ACC to accept SMP/E base functions.
   
   Your product is accepted and now resides in the distribution libraries.
Apply Maintenance

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

To apply maintenance

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

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

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

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

4. Open the SAMPJCL member xxx6RECP in an edit session and execute the xxxSEDIT macro from the command line.

   xxx6RECP is customized with your JOB statement, CSI location, and zone names.

5. Customize the xxx6RECP SMPPTFIN and SMPHOLD DD statements to reference the FB 80 data sets for the PTFs and HOLDDATA.

6. Submit xxx6RECP.

   The PTFs and HOLDDATA are received.

7. Open the SAMPJCL member xxx7APYP in an edit session and execute the xxxSEDIT macro from the command line.

   xxx7APYP is customized.

8. Submit xxx7APYP.

   The PTFs are applied.

9. (Optional) Open the SAMPJCL member xxx8ACCP in an edit session and execute the xxxSEDIT macro from the command line.

   xxx8ACCP is customized.

10. (Optional) Submit yourhlq.SAMPJCL member xxx8ACCP.

    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.
HOLDDATA

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

Note: When you have completed the procedures in this section, go to Configuring Your Product (see page 163).
Chapter 6: Configuring Your Product

This section describes the minimum configuration tasks needed before CA JARS RA can be started, customized, and used in your environment.

This section contains the following topics:

**Step 1. Tailor LMP Keys** (see page 163)
**Step 2. Run CAIRIM for CA JARS SMF/E** (see page 164)
**Step 3. Define Wizard Company Name** (see page 164)
**Step 4. Run CA JARS Installation Verification Tests** (see page 165)
**Step 5. Invoke the ISPF Interface** (see page 166)
**Step 6. Install XML Support** (see page 166)
**Step 7. Integrate with CA SMF Director** (see page 166)
**Step 8. Integrate with CA Auditor for z/OS** (see page 168)
**Step 9. Complete the Configuration Worksheet** (see page 168)
**Step 10. Run cBASE Link-Edit** (see page 170)
**Step 11. Run cBASE Data Dictionary Link-Edit for CA Datacom** (see page 170)
**Step 12. Run DB2 BIND Procedure** (see page 170)
**Step 13. Allocate CAIKSPAR** (see page 171)
**Step 14. Customize CAIKSPAR** (see page 171)
**Step 15. Prepare the Database** (see page 171)
**Step 16. Create Schema for CA Datacom Users** (see page 173)
**Step 17. Create and Load Tables** (see page 173)
**Step 18. Allocate CAIKRPAR** (see page 174)
**Step 19. Customize CAIKRPAR** (see page 174)
**Step 20. Process JARS/OLF IVP** (see page 175)
**Step 21. Print ORD Data File** (see page 175)
**Step 22. Print JARS/OLF Reconciliation File** (see page 176)
**Step 23. Generate JARS/OLF Invoices** (see page 176)
**Step 24. Customize JARS/OLF Online** (see page 176)
**Step 25. Invoke JARS/OLF Online** (see page 177)
**Step 26. Prepare for Live Data** (see page 178)
**Step 27. Grant Access to Additional Users** (see page 178)
**Step 28. Implement Security** (see page 179)
**Step 29. Update Existing IRD/ORD Tables** (see page 180)
**Step 30. Add New IRD/ORD Record Definitions** (see page 180)

**Step 1. Tailor LMP Keys**

The CA License Management Program (LMP) is one of the components of CA TCC (Total Client Care). LMP is comprised of the following three components:

- The CA product
- The LMP Product Key Certificate
Step 2. Run CAIRIM for CA JARS SMF/E

The common LMP Enforcement software

The LMP Product Key Certificate contains an execution key for each CPU licensed at your site.

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

Define the LMP execution key at this time.

Note: For more information, see the CA Common Services for z/OS Getting Started.

Step 2. Run CAIRIM for CA JARS SMF/E

This step is required if you are going to enable the SMF/E option. Even though you may choose to defer actually using the options, the following procedures are recommended.

In order to test SMF/E, you must first install CAIRIM from CA Common Services for z/OS.

Simply submit member JRC6INIT from your CAJRJCL library. If you have other CA products already operational on your system, you will receive informational messages to that effect.

Note: This job will not activate SMF/E. This only prepares the environment for future activation. For more information about implementing the SMF/E option, see the Systems Programmer Guide.

Step 3. Define Wizard Company Name

This step defines the CA JARS RA Wizard default company name. It has the following two parts:

1. Copy member WIZOPT from CAJRSAMP into your own source library and update it to define your company name.

2. Copy, customize, and submit CAJRJCL member WIZCOMP. This JCL is used to assemble and link edit the company name load module, WIZCMPNY, using the WIZOPT member you updated in step 1.

Note: The company name specified may not exceed 40 characters, and can be overridden during reporting using the COMPUTE COMPANY statement. For more information, see the Wizard Reference Guide.
Step 4. Run CA JARS Installation Verification Tests

Successful execution of the Installation Verification Procedure (IVP) is a major goal of the installation process. You should proceed in two steps:

1. activate SMF/E (optionally installed)
2. run the report IVPs

The following supplied job streams will be customized and used to complete this step of the installation process. They are provided in the sample JCL library.

**SMFIVP**
- SMF/E activation (optional)
  
  **Note:** When SMF/E is activated, the subsequent IVP jobs should specify IVP in the appropriate job card accounting field.

**JARIVP**
- Sample CA JARS RA, CA JARS RA Wizard, and Earl Service reports

**VMIIVP**
- Sample translate program and reports for VM

**ADAIVP**
- Sample translate program and reports for ADABAS

**IMSIVP**
- Sample translate program, FFGRAPHS, and reports for IMS

**ROSIVP**
- Sample translate program and reports for Roscoe

**NETIVP**
- Sample translate program and CA JARS RA Wizard report for NETVIEW

**TVAIVP**
- Sample translate program and CA JARS RA Wizard report for TVA

**Note:** Input data for the previous IVPs is supplied with the CA JARS RA system. The supplied IVPs must execute against this data before using data from your own environment. This ensures that the product is successfully installed and assists in problem determination if you experience difficulty during product customization.
**Step 5. Invoke the ISPF Interface**

The following steps are required in order to run the Online System. Steps 1, 2 and 3 are done only once, at installation. Step 4 starts the Online System; it is performed at each execution of the system.

1. The CLISTs in CAI.CAJRCLS0 must be continually available through the TSO SYSPROC DD statement. To achieve this, either copy the entire contents of CAI.CAJRCLS0 into a library that your installation has permanently allocated to SYSPROC, or allocate CAI.CAJRCLS0 to SYSPROC on a permanent basis.

2. Each user of the Online System must have an empty ISPF table library named 'USERID.JOS.V100.ISPTLIB'. This data set will be allocated by the CLIST when it is invoked.

3. Customize the JOS CLIST by changing the value of the JOS ISPF library dsname prefix, set &JOSPREF=.&STR(CAI)., to the high level qualifier of the data set names used during installation.

4. Execute the JOS CLIST to dynamically allocate all other Online System libraries and start the system. To invoke the JOS CLIST, go to the ISPF Primary Option Menu and enter Option 6. From the ISPF Command Shell screen, enter %JOS.

**Step 6. Install XML Support**

If CA JARS RA is going to be used to produce XML report documents, the IBM XML Toolkit for z/OS must be installed.

After the IBM XML Toolkit is installed, it must be made available to CA JARS RA in either of two ways:

- It can be added to the system linklist.
- It can be concatenated to the STEPLIB DD when running CA JARS RA.

**Note:** The XML Toolkit is only needed when generating XML reports from CA JARS RA. For more information about XML reporting with CA JARS RA, see the User Guide.

**More information:**

XML Requirements (see page 14)

**Step 7. Integrate with CA SMF Director**

If you have CA SMF Director installed, you can use a CA SMF Director split file or extract as input to CA JARS RA.
Why Use CA SMF Director

Mainframes produce a large volume of SMF records, many of which are irrelevant to accounting and chargeback. The time spent reading and discarding SMF record types that are not chosen for chargeback can be significant. CA SMF Director split files are created at the time the SMF MANx or SMF logstream files are dumped. The split files are created in a single pass, as SMF data is being dumped. This eliminates redundant EXTRACT processing. If your SMF volume is large and only a small part of that volume is to be processed by CA JARS, integration with CA SMF Director can save processing time and money. A sample SPLIT statement is discussed below.

If policy or procedure at your shop prevents the use of SPLIT files, it is also possible to use the SMF Director EXTRACT function to extract only those SMF records that are processed by CA JARS RA. Although this is not as efficient as using SPLIT, it is still more efficient than passing all SMF data and letting CA JARS RA reject what is not needed.

SPLIT Processing

Typically, CA JARS RA is run once a day after midnight to process the last day’s SMF data. CA SMF Director is run at each SMF dump event. Supplied with a SPLIT statement, as in the example below, CA SMF Director builds a split file that contains only SMF records needed for CA JARS RA.

This sample statement is in CAJOPTN(JARSSPLT):

```plaintext
DUMP.
SPLIT ALL TODD(CAIJSSMF)
SELECT(0,4:11,19,25,26,30,32,33,39,41,42,47:50,
      52:54,57,59,70:79,88,89,92,94,101,103,110,
      115,116,118:120).
```

You can modify the sample SPLIT statement to only select records that are of interest to your CA JARS RA configuration. For more information about the SPLIT statement, see the CA SMF Director User Guide.

The split file is usually configured as a generation data set (GDG) or as a group of GDGs. You must define the //CAIJSSMF DD statement in the CA JARS RA execution JCL to point to the split file. You must also configure CA JARS RA, CA SMF Director, and your own scheduling software to make sure that only the correct split files are input to CA JARS RA.
Step 8. Integrate with CA Auditor for z/OS

Note: If you do not want CA Auditor for z/OS to report on CA JARS RA, skip this section.

Load module CAIXAJ1$ is placed in the target CAJRLOAD during the installation of CA JARS RA. To use the module with CA Auditor for z/OS, either the CA JARS RA CAJRLOAD must be in the system link list, or the module must be moved (via IEBCOPY) to a load library that is in the system link list.

Step 9. Complete the Configuration Worksheet

Follow steps 9 through 23 only if you have installed JARS/OLF. If you have not installed JARS/OLF but have installed CA PMA Chargeback, you can skip to step 24. If you are not planning to use either JARS/OLF or CA PMA Chargeback, you can skip the rest of this chapter.

If you are configuring JARS/OLF, complete the following worksheet. The keywords on the worksheet are the same as the symbolic parameters used in the supplied configuration JCL. If a default has been assigned in the supplied JCL, it is identified below.

<table>
<thead>
<tr>
<th>Description</th>
<th>Keyword</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. What high-level qualifier has been defined for the CA Common Services libraries? Default: CSIND='CAI'</td>
<td>1. CSIND=_________________</td>
</tr>
<tr>
<td>2. If using CA Datacom, what high-level qualifier has been defined for those libraries? Default: DCIND='CAI'</td>
<td>2. DCIND=_________________</td>
</tr>
<tr>
<td>3. If using DB2, what is the name of your DB2 load library? No Default</td>
<td>3. DSNLOAD=_______________</td>
</tr>
<tr>
<td>4. If using DB2, what is the subsystem ID? No default</td>
<td>4. SUBSYSTEM_ID=__________</td>
</tr>
</tbody>
</table>
Step 9. Complete the Configuration Worksheet

5. Which DASD volume do you plan to use for the JARS/OLF parameter files?
   No Default

5. PARMVL=_______________

6. What high-level qualifier do you plan to assign to the parameter files?
   Default: PINDEX='CAI'

6. PINDEX=_______________

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

7. DATABASE_NAME=___________

   DB2 PLAN ID=_____________

   SQL_TYPE=_______________

   SUBSYSTEM_ID=_____________

   CUSTOMER_NAME=___________

   BASE_VERSION=_____________

   CHARGE_PREC=_____________

   RATE_PREC=_______________

   UNIT_PREC=_______________

   EURODB2=_______________

   CBLOAD_VERSION=_________

   RECONCILIATION_FILE=___

Note: For more information about these parameters, see the "Batch Processing & Reporting" chapter in the JARS/OLF User Guide.
Step 10. Run cBASE Link-Edit

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

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

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

Step 11. Run cBASE Data Dictionary Link-Edit for CA Datacom

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

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

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

Step 12. Run DB2 BIND Procedure

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

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

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

Important! The userid (referred to as the owner's ID or ownerid) used in subsequent steps must be authorized for the database by your database administrator. This userid must be used to complete the installation.
Step 13. Allocate CAIKSPAR

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

Step 14. Customize CAIKSPAR

Customize the CAIKSPAR data set to define your database environment.

Note: For more information about customization, see the "Batch Processing and Reporting" chapter in the JARS/OLF User Guide.

Important! All the batch JCL STEPLIB statements need to be reviewed and customized prior to processing. If CA Datacom is being used, make sure that the data set name matches the data set names used during CA Datacom installation. Also delete references to the DB2 library.

If DB2 is being used, make sure that the data set name of the DB2 library is correct. Also delete the references to the CA Datacom libraries and remove the DCIND symbolic from all JCL members and PROCs.

Step 15. Prepare the Database

If the database system used by JARS/OLF is:

- CA Datacom/DB - Then complete step 15a.
- CA Datacom/AD - Then complete step 15b.
- DB2 - Then complete step 15c.

Step 15a. Prepare CA Datacom/DB Database

Before creating the schema (Step 16) for CA Datacom/DB, the PMA490 database must be set up. JCL to set up the database can be found in the CAJRJCL as member name CADBDATA. The JCL contains five steps:

1. DDUPDATE—Adds the PMA490 database definitions to the dictionary
2. COPYPRD—Copies the PMA490 definitions to PROD status
3. CATALOG—Catalogs the PMA490 definitions to the CXX
4. IEFBR14—Allocates the dataspaces for index and data areas
5. INITLD—Initializes and NULL LOADs the PMA490 areas
Step 15. Prepare the Database

After successful completion of the above steps, continue with Step 16.

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

Step 15b. Prepare CA Datacom/AD Database

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

1. CADBDEF—Adds PMA490 database definitions
2. CADDRTV—Verifies, copies to PROD, catalogs, and enables
3. CADBALLC—Allocates dataspace for index and data areas
4. CADBUTIL—INITs and NULL LOADs the database

After successful completion of the above steps, continue with Step 16.

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

Step 15c. Prepare DB2 Database

1. Have the DB2 database administrator authorize the ID being used to install JARS/OLF for DATABASE CREATE, TABLE CREATE, and GRANT authority.
2. Create a database, buffer pool, and storage group to be used by the JARS/OLF product.
3. Grant access to the database and buffer pool to the ID being used to install JARS/OLF.
4. The following SQL commands may be used as a guide for setting up DB2 to prepare for the JARS/OLF product.

```
CREATE DATABASE PMA490
STOGROUP SGMA490
BUFFERPOOL BPO
CREATE STOGROUP SGMA490 VOLUMES ("", ",", ",") VCAT xxxx;
```

The above SQL statement will create and identify the PMA490 database for DB2 using storage group SGMA490 and buffer pool zero. The xxxx represents the four-character database subsystem id.

```
GRANT DBADM ON DATABASE PMA490 TO userid;
GRANT USE OF BUFFERPOOL BPO TO userid;
GRANT USE OF STOGROUP SGMA490 TO userid;
GRANT EXECUTE ON PLAN CAISSQL2,CAISSQL3,CAISSQL9 TO userid;
```
Step 16. Create Schema for CA Datacom Users

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

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

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

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

Step 17. Create and Load Tables

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

1. Member CAKRTBLI in CAJRJCL allocates and loads the required tables for JARS/OLF. This member also creates indexes and synonyms for the owner's ID and loads and commits the startup definitions.

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Input</th>
<th>DB2</th>
<th>Datacom</th>
</tr>
</thead>
<tbody>
<tr>
<td>STEP010</td>
<td>Creates Tables</td>
<td>CAKRDC8</td>
<td>N/A</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CAKRDB8</td>
<td>Y</td>
<td>N/A</td>
</tr>
<tr>
<td>STEP020</td>
<td>Create Synonyms</td>
<td>CAKRCR84</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>
For CA Datacom, input members that need to be customized are CAKRDC8 and CAKRCR84. In member CAKRDC8, change PMA490 to reflect the correct database name. In member CAKRCR84, change ownerid to the DB owner's ID.

For DB2, CAJRSQL library members CAKRDB8 and CAKRCR84 will need to be customized. For member CAKRDB8, change DSNDB04 to reflect the correct database name. For member CAKRCR84, change ownerid to the DB owner ID.

After completing this, customize CAJRJCL library member CAKRTB11. The STEP010 step must be reviewed to make sure that the INPUT symbolic reflects the appropriate input, either CAKRDC8 or CAKRDB8. Submit the job and review the output to verify that processing completed with a return code of 0.

**Note:** Input members are from CAJRSQL.

2. Member CAKRTBLO loads JARS/OLF IRD/ORD tables. Edit this member and select only the tables that you want to load.

**Note:** For more information, see the pre-defined JARS History Records in "Appendix C" of the JARS/OLF User Guide.

CAJRSQL library members distributed with the product that are used as input to program CAKRINST include SQL "COMMIT" statements after every one hundred inserts. The commits will cause all work to that point to be committed to the database and held storage will be freed. It is very important to note that this removes the "ROLLBACK" capability if the job fails for any reason. It will be necessary for users to create BACK-UPS for tables that will be modified after initial installation before using CAKRINST.

### Step 18. Allocate CAIKRPAR

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

### Step 19. Customize CAIKRPAR

Customize the CAIKRPAR data set with the following settings to ensure that the IVPs run successfully:

- **BASE = TEST**
- **CBLOAD = TEST**
Step 20. Process JARS/OLF IVP

This step requires that the record definitions for MBJ exist in your table definitions. This is accomplished by processing the table loaded in Step 17 with CAJRSQ(MVS BAT).

This step uses the committed JARS/OLF startup definitions downloaded during install Step 17, along with the IVP data, to apply charges to the CCCTAB and to generate a detailed reconciliation file.

CAJRJCL library member CAWFIVP processes IVP data using the startup definitions. Edit this JCL to conform to your installation’s standards using the previously completed worksheet. Submit the job and review the output to verify that processing has completed with a return code of 0.

Validate that the IVP processing completed successfully by reviewing the condition codes and the JARS/OLF Summary Control Report. The control report must indicate the following:

<table>
<thead>
<tr>
<th>Input Statistics: JARS Record Read</th>
<th>544</th>
</tr>
</thead>
<tbody>
<tr>
<td>IRDID Records Generated</td>
<td>213</td>
</tr>
<tr>
<td>Output Statistics: CAIKSOP MBJ</td>
<td>213</td>
</tr>
<tr>
<td>Records Read</td>
<td>213</td>
</tr>
<tr>
<td>Original Records Created</td>
<td>419</td>
</tr>
<tr>
<td>Records inserted into CCCTAB</td>
<td>61</td>
</tr>
</tbody>
</table>

Step 21. Print ORD Data File

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

Edit member CASKORSDS to conform to your installation’s standards using the previously completed worksheet. Submit the job and review the output to verify processing completed with a return code of 0.
Step 22. Print JARS/OLF Reconciliation File

The JARS/OLF IVP process included generation of the reconciliation file. CAJRJCL member CAKRECON uses the Earl Service to print the reconciliation file.

Edit this member according to your installation’s standards and the previously completed worksheet. Submit the job and review the output to verify that processing completed successfully. The record count of the SYSEARL should reflect:

<table>
<thead>
<tr>
<th>Hitfile Records Written</th>
<th>419</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grand Total</td>
<td>2931.6712</td>
</tr>
</tbody>
</table>

Step 23. Generate JARS/OLF Invoices

This step generates an invoice from the IVP data processed in Step 20. CAJRJCL member CAKRINVC uses the Earl Service to generate an invoice.

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

Step 24. Customize JARS/OLF Online

A. Customize Template:

Customize member NEWCB in CAI.CAJRCTMP. For DB2, change the &&XXSSID. to the four-character SSID or driver used when DB2 links to data. For CA Datacom, the &&XXSSID. needs to equal the owner’s ID. The &&WHATSQL. needs to reflect the numeric value associated with the database system. These values are:

- 2 SQL/OS
- 3 DB2
- 4 CA Datacom/DB

If you are using DB2, be sure to also change &&PLAN. to CAISSQL3.

B. Customize CLIST:

Edit member PMACBC in CAI.CAJRCLS0 to reflect the appropriate high level qualifiers. Remove the CAI.CAIRCPCNC library from the concatenations.

Note: The library CAI.VPOINT.PANEL is a part of CA Common Services (Viewpoint).

C. Allocate Libraries for PMACBC CLIST:
The following load libraries must be allocated during the execution of the PMACBC CLIST in this order:

- CA JARS RA load library CAI.CAJRLOAD
- CA Common Services load library
- If you use CA Datacom, its load library (CAILIB or CABDLOAD) and custom load library (CUSLIB)
- If you use DB2, its load library (SYS2.DSNLOAD)

We recommend that you use the ISPEEXEC facility to temporarily create a TASKLIB that will be available during the execution of the CLIST. Here is an example:

```plaintext
FREE DDN(PMALIB)
ALLOC F(PMALIB) DA('CAI.CAJRLOAD' + 'CA.COMMON.SERVICE.CAILIB' + 'CA.DATACOM.DB.LIBRARY') SHR REUSE
   . PMACB CLIST statements
   . ISPEEXEC LIBDEF ISPLLIB LIBRARY ID(PMALIB)
CBASEX NEWCB
ISPEEXEC LIBDEF ISPLLIB LIBRARY
```

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

D. Set European DB2 (optional):

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

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

Note: For more information about CAIKSPAR customization, see the chapter "Batch Processing and Reporting" in the JARS/OLF User Guide.

**Step 25. Invoke JARS/OLF Online**

A.

Log on executing the TSOPROC.
Step 26. Prepare for Live Data

In order to complete the IVP process, the JARS/OLF tables were committed to TESTTEST. Processing of the JARS/OLF IVP resulted in updating the CCTAB. The following steps are required to remove IVP data:

A. Delete the CCCTAB:
   CAJRJCL member CAKRDEL1 deletes the IVP data records from the CCCTAB.
   
   Edit this member to conform to your installation's standards using the previously completed worksheet. Submit the job and review the output to verify processing completed with a return code of 0.

   **Note:** Processing of this member will result in the deletion of the JARS/OLF IVP data.

B. Delete JARS/OLF Definitions (Optional):
   CAJRJCL member CAKRDEL2 deletes the CBdefs that were used to process the JARS/OLF IVP.
   
   Edit this member to conform to your installation's standards using the previously completed worksheet. Submit the job and review the output to verify processing completed with a return code of 0.

Step 27. Grant Access to Additional Users

This step outlines the tasks necessary to grant additional userids access to the JARS/OLF tables.

A. Authorize userid:
   If you have installed the system using DB2, the new user must be granted EXECUTE access on the plans created when the bind procedure was run for DB2. The plan names are CAISSQL2, CAISSQL3, and CAISSQL9. The following SQL statement grants execute access to userid C0001:
   
   ```sql
   GRANT EXECUTE ON PLAN CAISSQL2, CAISSQL3, CAISSQL9 TO C0001;
   ```
If you installed the system using CA Datacom, you must create a schema for the new user. Member CAKRSCSCH can be used. Be sure to customize CAKRSCMA; the userid will need to be changed to the new userid.

B. Grant access to userid:

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

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

C. Establish synonyms:

Important! This step must be executed by the userid requiring the synonyms.

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

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

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

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

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

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

---

**Step 28. Implement Security**

Security of JARS/OLF tables is implemented by protection of dialogs.

Note: For more information, see the chapter "Security and Audit" in the JARS/OLF User Guide.
Step 29. Update Existing IRD/ORD Tables

Updates to the IRD/ORD table definitions are provided periodically.

More Information

Update Database Tables (see page 181)

Step 30. Add New IRD/ORD Record Definitions

Member CAKRTBLP will load new IRD/ORD record definitions. Select only the members you want to add new.

Note: For a list of all available IRD/ORD record definitions, see Appendix C, Predefined CA JARS History Records, in the OLF User Guide.

CAJRSQL library members distributed with the product that are used as input to program CAKRINST include SQL "COMMIT" statements after every one hundred inserts. The commits will cause all work to that point to be committed to the database and held storage will be freed. It is very important to note that this removes the "ROLLBACK" capability if the job fails for any reason. It will be necessary for users to create BACK-UPS for tables that will be modified after initial installation before using CAKRINST.

Complete the steps listed below to add the new IRD/ORD record definitions.

1. From CAJRJCL, customize member CAKRTBLP to conform to your organization's standards.

2. The JCL mentioned in step 1 requires the use of the CAKRTAB proc. Point to a library that already has this member customized from the initial product installation, or customize the CAKRTAB PROC from the CAJRPROC on this tape.

3. Comment out all DD names except those pointing to members that contain IRD/ORD sets that you want to add to your database.

4. Submit the CAKRTBLP member. This will load the requested definitions. A condition code of 0 should be received.
Chapter 7: Migration Information

This section contains the following topics:

Update Database Tables (see page 181)

Update Database Tables

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

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

This section contains the following topics:

- Verifying the Problem (see page 183)
- Collecting Diagnostic Data (see page 183)
- Interpreting Diagnostic Data (see page 186)

Verifying the Problem

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

1. Examine the procedure that you used and compare it to the documented procedure for performing the required activity.

2. If you find no discrepancies between your procedures and the documented procedures, repeat the activity under conditions similar to those that existed when the problem first appeared. (If you no longer get unsatisfactory results, an inadvertent error may have caused the problem.)

3. If the same error occurs when you repeat a given activity, and you can find nothing in the documentation to suggest that your procedure is flawed, check with others at your site to determine if they have had the same or similar problem and how they handled it.

Collecting Diagnostic Data

In the table below, use the left column to categorize the problem your site has encountered. Then, follow the instructions in the corresponding right column to generate useful diagnostic data.

<table>
<thead>
<tr>
<th>Type of Problem</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interfaces</td>
<td>- Check that the Interface data was input as history input (DDNAME=CAIJSHST).</td>
</tr>
<tr>
<td></td>
<td>- Check that all processing by the Interface programs completed successfully prior to inputting Interface data to CA JARS RA.</td>
</tr>
</tbody>
</table>
## Collecting Diagnostic Data

### Type of Problem | Procedure
---|---
**Exits** | - Check that your library concatenation includes the library that contains the exit.  
- If this product abends with the exit yet runs successfully without it, the problem is probably in the exit itself. Make sure control is returned to this product correctly.

**SMF/E** | - Check that the target library, CAJRLOAD, is a linklist and an APF-authorized library.  
- CAIRIM processing completed successfully.  
- For SMF/E routine failures, an SVC dump is created and written to a dump data set (SYS1.DUMPxx).

**Execution** | - Check that sufficient space is allocated to the account file and work files to process all the input data provided (ddnames are: CAIJSACT, CAIJSCTL1, CAIJSCTL2, and the SORTWKxx files).  
- Check that the SELECT statement specifies the same input defined in the JCL and calls for at least one output report to be generated.  
- Check that the elements to be displayed on the report are available at the level of reporting specified. For example, Step Name and Program Name are only available for display if step records are printed, and cannot be displayed at the job or summary level.  
- Check that all control statements are coded correctly and each field begins in the proper columns.  
- Check that the desired SMF records are being collected as specified through SMFPRMxx.  
- Check that sequence numbers are not specified on any control statement.

**Grouping** | - Check that essential records have not been eliminated by the selection/rejection specifications coded on the GROUP or GROUPC or CRITERIA or DEVADDR or DEVNMB control statements.

**SNAPDUMP** | - Make sure the CAIJSNAP data definition statement is coded to produce a dump of records snapped.  
- See the section Interpreting SNAPDUMP Output in the "Special Usage Considerations" chapter of the Systems Programmer Guide. Records are snapped because of errors in the SMF record. A REASON CODE is provided for the snapped records.
JARS/OLF Online Facility

In the JARS/OLF Online Facility, if you encounter the following problems, perform the corresponding procedures listed below:

To bring up the online facility

1. Verify that member NEWCB in CAJRCTMP is correctly customized as outlined in the step Customize JARS/OLF Online in the chapter "Installation Steps."
2. Verify that member PMACBC in CAJRCLS0 has been changed to reflect the appropriate high level qualifiers.
3. Verify that the CAJRLOAD library is allocated and available to the TSO session.
4. Verify that the user CAIKRPAR (CAIKRPAR DD statement) correctly defines your database environment.
5. Verify that the step Grant Access to Additional Users has been completed as outlined in the section Installing CA JARS RA with JARS/OLF in the chapter "Installation Steps."

Error in definition

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

1. Verify that the JARS/OLF version specified using the Option facility reflects the version with which the ORD Type was committed.
2. If the ORD Types definition exists in the Development version of JARS/OLF, you must process the commit before these ORD Types can be used by JARS/OLF definition.

Period Functions - Forecasting

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

1. Exit the Forecasting panel
2. Select Options, then select item 2 (Versions) from the Options pull-down
3. Change the JARS/OLF Version to match the version specified during generation of the forecast

Batch Processing Error

If you encounter a Batch Processing Error, see the JARS/OLF Messages and Codes Guide to determine appropriate reason and action for the error message(s) received.
Interpreting Diagnostic Data

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

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

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

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

A
access
  login • 33
acquiring the product • 9, 34
acquisition
  download • 24, 35
adding
  custom data set • 105
  data destination • 79
  FTP locations • 74
  product • 103
  system • 131
aggregated package, viewing • 51
AJR prefix • 151
allocate and mount • 141
allocating
  CAIKRPAR • 174
  CAIKSPAR • 171
authorization
  modes • 65
AWF prefix • 151

C
CA Auditor for z/OS • 168
CA Datacom
  AD • 20, 172
  database • 173
  DB • 171
  schema creation • 173
  with SQL • 20
CA JARS Wizard • 16
CA LMP • 15
CA MSM usage scenarios • 24
CA SMF Director • 167
CA TCC (CA Total Client Care) • 163
CA-C Runtime • 15
CAI.SAMPJCL
  library • 157
  sample jobs • 157
CAIKRPAR
  allocation • 174
  customization • 174
CAIKSPAR
  allocation • 171
customization • 171
CAIRIM • 15
CAISSF • 15
CAKRDEL • 178
CAKRTBLZ • 181
catalog, update • 34
cBASE Link-Edit • 170
CCCTAB • 178
Common Services requirements • 15
concurrent releases • 21
configuration worksheet • 168
confirming deployment • 101
contact system • 71
contacting technical support • iii
copy files to USS directory • 143, 144, 147
creating
  data destination • 78
  deployment • 88
  methodology • 113
  monoplex • 63
  shared DASD cluster • 64
  staging • 65
  sysplex • 63
CSIs (consolidated software inventories)
  creation • 43
  migration • 24
custom data sets
  add • 105
  edit • 108
  remove • 111
  view • 105
customer support, contacting • iii
customizing
  CAIKRPAR • 174
  CAIKSPAR • 171
  JARS/OLF online • 176

D
DASD requirements • 16
data class • 130
data set name mask • 116
data sets, file systems
data destinations
  add • 79
  create • 78
delete • 82
edit • 80
maintain • 80
set default • 82
database table updates • 181
DB2
   BIND procedure • 170
   European • 176
default
data destination • 82
FTP location • 76
defining database environment • 171
deleting deployment objects
data destination • 82
development • 99
system registry • 73
delivery, product acquisition • 9
deployments
   confirm • 101
   create • 88
current state • 86
delete • 99
maintain • 95
preview • 92
reset status • 99
select a product • 103
select a system • 130
summary • 132
validation, failed • 69
view • 92
diagnostic data • 183
distribution
   libraries • 18, 19
tape • 9
download • 24, 35
   files using ESD • 136
   installation packages • 24, 35
LMP keys • 46
maintenance packages • 24, 48, 49
options • 143
overview • 135
to mainframe through a PC • 147
using batch JCL • 144

E
Earl Service • 15
edit
   custom data set • 108
edit, data destination • 80
methodology • 126
ESD (Electonic Software Delivery) • 9
European DB2 • 176
external HOLDDATA • 156
external packages
   installation • 37, 40
   migration • 37, 50
F
failed validation • 69
free space • 140
FTP locations
   add • 74
   edit • 75
   remove • 76
   set default • 76
G
GIMUNZIP utility • 149
Granting access to additional users • 178
GROUPEXTEND mode • 56
H
hash setting • 149
high-level qualifier • 149
HOLDDATA • 156
I
IEBCOPY • 157
implementation • 179
installation • 24, 40
   create tables • 173
   load tables • 173
installation packages
   download • 35
   migration • 37
installing
   from Pax-Enhanced ESD • 135
   from tape • 157
Integrated Cryptographic Services Facility (ICSF) • 149
internal HOLDDATA • 156
investigating failed validation • 69
IRD/ORD
   record definitions • 180
   tables • 180
   ISPF interface • 166
IVP data • 178

J

JARS/OLF
- customize online • 176
- Distribution Libraries • 19
- invoking online facility • 177
- IVP data • 178
- parameter file • 20
- requirements • 20
Java version support • 149

L

Libraries
- authorization • 14
- distribution • 18
- permanent (target) • 16
- live data • 178
- LMP keys • 46, 163

M

maintain
- data destinations • 80
- deployment • 95
- maintain by list, system register • 72
- system registry • 66
- maintenance • 155
  - application • 24, 52
  - backout • 60
  - GROUPEXTEND mode • 56
  - USERMODs • 56
- maintenance packages
  - backout • 60
  - download • 24, 48, 49
  - installation • 24, 52, 55
  - migration • 50
  - USERMODs • 56
  - viewing status • 55
- methodology
  - create • 113
  - remove • 129
  - symbolics qualifiers • 116
- migrations
  - installation packages • 37
  - maintenance packages • 50
- monoplex
  - create • 63

N

native SMP/E JCL • 151
- nested packages • 51

P

parameter files for JARS/OLF • 20
- pax ESD procedure
  - copy product files • 143
  - create product directory • 148
  - download files • 136
  - set up USS directory • 140
- pax file
  - copy files to USS directory • 143, 144, 147
- PMACBC CLIST • 176
- process overview • 135
- product
  - acquisition • 9
  - product download window • 137
  - product-level directory • 148
- products
  - acquired externally • 37, 50
  - add • 103
  - download • 24, 35
  - installation • 24, 40
  - maintenance • 24, 52, 60
  - remove from deployment • 104

R

read me • 135, 149
- remote credentials
  - add • 83
  - delete • 85
  - edit • 84
- remove
  - custom data sets • 111
  - FTP locations • 76
  - methodologies • 129
  - product • 104
  - system • 131
- Report Writer • 14
- requirements • 11
- reset status • 99
- RMF records processed • 11

S

sample JCL • 157
- sample jobs • 144, 148