

# **CA NetMaster® File Transfer Management**

## **Installation Guide**

**r12**



This documentation and any related computer software help programs (hereinafter referred to as the "Documentation") are for your informational purposes only and are subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be used or disclosed by you except as may be permitted in a separate confidentiality agreement between you and CA.

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

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

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

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

The manufacturer of this Documentation is CA.

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

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

## CA Product References

This document references the following CA products:

- CA NetMaster® File Transfer Management (CA NetMaster FTM)
- CA NetMaster® Network Management for TCP/IP (CA NetMaster NM for TCP/IP)
- CA NetMaster® Network Management for SNA (CA NetMaster NM for SNA)
- CA NetMaster® Network Automation (CA NetMaster NA)
- CA SOLVE:FTS
- CA NetSpy™ Network Performance (CA NetSpy)
- CA SOLVE:Operations® Automation (CA SOLVE:Operations Automation)
- CA SOLVE:Access™ Session Management (CA SOLVE:Access)
- CA Network and Systems Management NetMaster® Option (CA NSM NetMaster Option)
- CA Network and Systems Management (Unicenter NSM)
- CA NetMaster® CONNECT:Direct Agents
- CA NetMaster® Socket Management for CICS (CA NetMaster SM for CICS)
- CA SOLVE:Central™ Service Desk for z/OS (CA SOLVE:Central), which includes CA SOLVE:Problem
- CA XCOM™ Data Transport®
- CA Common Services™ for z/OS (CA Common Services for z/OS)
- CA Common Inventory Service
- CA Auditor for z/OS (CA Auditor)
- CA TCPaccess™ Communications Server for z/OS (CA TCPaccess CS)
- CA TCPaccess™ FTP Server
- CA ACF2™ for z/OS (CA ACF2 for z/OS)
- CA Top Secret® for z/OS (CA Top Secret for z/OS)

## Contact CA

### Contact Technical Support

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

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

### Provide Feedback

If you have comments or questions about CA product documentation, you can send a message to [techpubs@ca.com](mailto:techpubs@ca.com).

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

# Contents

---

<b>Chapter 1: Overview</b>	<b>13</b>
Audience Qualifications .....	13
How the Installation Process Works .....	14
Remaining Documentation .....	14
CA Mainframe Network Management Family of Products .....	15
 <b>Chapter 2: Preparing for Installation</b>	 <b>17</b>
Multiple Product Installation and Setup .....	17
Software Requirements .....	17
Operating Environment .....	17
WebCenter Requirements .....	18
Additional Product Requirements .....	18
Migration Mode .....	19
CA Common Services Requirements .....	19
Security Requirements .....	20
Storage Requirements .....	21
How CA LMP Statements Are Coded .....	21
KEYS Member—Add Execution Key .....	21
CA LMP Key Certificate .....	23
Preparation Worksheets .....	24
Installation .....	24
Region Setup .....	28
TCP/IP Setup .....	32
File Transfer Setup .....	34
Startup Tasks .....	37
Post-installation Worksheet .....	37
Migration Preparation .....	39
Parameter Group Values .....	39
How to Migrate Your Initialization File .....	40
Knowledge Base .....	40
Multisystem Considerations .....	41
 <b>Chapter 3: Installing Your Product Using CA MSM</b>	 <b>43</b>
CA MSM Documentation .....	43
Getting Started Using CA MSM .....	44
How to Use CA MSM: A Scenario .....	44

---

Access CA MSM Using the Web-Based Interface .....	52
Acquiring Products .....	53
Update Software Catalog .....	53
Download Product Installation Package .....	54
Migrate Installation Packages Downloaded External to CA MSM .....	55
Download Multiple Product Installation Packages .....	56
Add a Product .....	57
Delete a Product .....	59
Installing Products .....	59
Install a Product .....	59
Create a CSI .....	63
Download LMP Keys .....	64
Maintaining Products .....	65
How to Apply Maintenance Packages .....	65
Download Product Maintenance Packages .....	66
Download Maintenance Packages for Old Product Releases and Service Packs .....	66
Manage Maintenance Downloaded External to CA MSM .....	68
Manage Maintenance .....	69
GROUPEXTEND Mode .....	73
Back Out Maintenance .....	76
Setting System Registry .....	77
About System Registry .....	77
Create Non-Sysplex System .....	78
Create Sysplex or Monoplex .....	80
Create Staging System .....	82
Create Shared DASD Cluster .....	83
Authorization .....	84
Maintain a System Registry .....	84
Delete a System Registry .....	92
Data Destinations .....	92
FTP Locations .....	100
Remote Credentials .....	103
Deploying Products .....	105
About Deployments .....	105
Create a Deployment using the Product Wizard .....	106
View a Deployment .....	113
Maintain Deployments .....	114
Delete a Deployment .....	119
Delete a Completed Deployment .....	120
Confirm a Deployment .....	120
Products .....	122
Custom Data Sets .....	123

---

Methodologies .....	132
Systems .....	146
Deployment Summary .....	148
 <b>Chapter 4: Installing Your Product From Pax-Enhanced ESD</b>	 <b>151</b>
How to Install a Product Using Pax-Enhanced ESD .....	151
How the Pax-Enhanced ESD Download Works .....	153
ESD Product Download Window .....	153
USS Environment Setup .....	156
Allocate and Mount a File System .....	157
Copy the Product Pax Files into Your USS Directory .....	158
Download Using Batch JCL .....	159
Download Files to Mainframe through a PC .....	162
Create a Product Directory from the Pax File .....	163
Example Job to Execute the Pax Command (Unpackage.txt) .....	164
Copy Installation Files to z/OS Data Sets .....	164
Unload the Install Utility .....	165
Additional Features .....	166
Installation JCL .....	166
Generate the Installation JCL .....	167
Clean Up the USS Directory .....	169
Maintenance .....	170
Product Maintenance .....	170
Apply Maintenance .....	171
Update VSAM Data Sets .....	174
Individual RAMDB Maintenance .....	176
 <b>Chapter 5: Installing Your Product From Tape</b>	 <b>183</b>
Unload the Install Utility .....	183
Additional Features .....	183
Unload into a New Data Set from Tape .....	184
Unload into an Existing Data Set from Tape .....	185
Installation JCL .....	186
Generate the Installation JCL .....	186
Maintenance .....	189
Product Maintenance .....	189
Apply Maintenance .....	189
Update VSAM Data Sets .....	193
Individual RAMDB Maintenance .....	195

---

<b>Chapter 6: Configuring Your Product</b>	<b>201</b>
How Region Setup Works .....	201
Region Contents .....	202
SOLVE SSI as Common Component .....	202
Specify the SOLVE SSI Region .....	203
Specify the Product Region .....	204
Specify the NMFTP Monitor Region .....	207
 <b>Chapter 7: Creating VTAM Definitions and Tables</b>	 <b>209</b>
Create VTAM Definitions and Tables .....	209
 <b>Chapter 8: Preparing the IBM Communications Server</b>	 <b>211</b>
Define UNIX Authorization for Your Started Task User IDs .....	211
User Functionality Authorization .....	211
Example: Authorization in a CA ACF2 System that Protects Operator Commands .....	212
Example: Authorization in a CA Top Secret System .....	212
Example: Authorization in a RACF System .....	212
Set Up the SNMP Agent .....	213
Generate SMF Records for FTP Event Flow .....	214
Generate FTP Post-Processing Transfer Failures Event Flow .....	215
NMFTP Monitor Access to NMI API SMF Records .....	217
SERVAUTH .....	217
BPX.SUPERUSER .....	218
 <b>Chapter 9: Preparing CA TCPaccess CS</b>	 <b>219</b>
Generate SMF Records for FTP Event Flow .....	219
Set Up DNR Members .....	220
Enable Access to SNMP Data .....	221
Restart CA TCPaccess .....	221
 <b>Chapter 10: Setting Up File Transfer Resources</b>	 <b>223</b>
Customize Managed CA XCOM Regions .....	223
How CA SOLVE:FTS Regions Work .....	224
Define the Link to the Product Region .....	225
Install the CA SOLVE:FTS Message Handler .....	226
How Managed CONNECT:Direct Regions Work .....	226
Implement Statistics Exits in the Managed CONNECT:Direct Regions .....	226
Customize CONNECT:Direct Initialization Parameters .....	230
Define the Region as CONNECT:Direct User .....	231
Customize Managed CONNECT:Mailbox Regions .....	232



---

How to Set Up SAF Access for TCPAccess Policy Rule Sets .....	233
How to Define \$SOLVE.FTP.CONTROL to Your Security System .....	233

## **Chapter 11: Preparing to Start Your Product** **235**

Started Task JCL Setup .....	235
TESTEXEC Data Set .....	236
Started Task Product Region Parameter Member .....	237
SOLVE SSI Started Task Parameter Member .....	238
Review and Copy the Product Region Started Task .....	239
Review and Copy the SOLVE SSI Started Task .....	239
Review and Copy the NMFTP Monitor Started Task .....	240
Subsystem Identifier Setup .....	240
Load Libraries .....	240
Authorization of the Load Libraries .....	241
Assign Consoles .....	241
Activate VTAM Applications .....	242
Enable Auditing by CA Auditor .....	242

## **Chapter 12: Performing Initial Migration** **243**

NPF and SAF Security Members .....	243
SYSPARMS Usage .....	243
New Commands that Replace SYSPARMS Operands .....	244
Revised SHOW SYSPARMS Output .....	244
Amended SYSPARMS Operand Processing .....	245
\$CACALL Changes .....	245

## **Chapter 13: Starting Up** **247**

Start the SOLVE SSI Region .....	247
Restart the SOLVE SSI Region .....	248
Start the Product Region .....	248
Start the NMFTP Monitor Region .....	248
Perform the Initial Logon .....	249
Add the Initial Administrator User ID .....	249
Perform Subsequent Logon .....	250

## **Chapter 14: Customizing Your Product** **253**

Initial Customization Requirements .....	253
Customizer Setup Types .....	254
Customize Parameter Values .....	255
Interrupted Customization .....	255

---

Update and Review the Fast Setup Customization Parameters .....	255
Web Browser Settings .....	258
Additional Parameter Groups .....	259
Implement Additional File Transfer Mechanism Parameters .....	259
Customize Region for FTP Events .....	260
Define File Transfer Resources to Your Region .....	261
Define the Region as a CA SOLVE:FTS User .....	261
Initialization Failures .....	261
Resolve Initialization Failures .....	262
Parameter Group Actions .....	263
Perform Additional Customization .....	263

## **Chapter 15: Completing Migration** **265**

NetMaster : Primary Menu .....	265
Knowledge Base Migration .....	266
Migrate Your Existing Knowledge Base .....	267
How to Copy Multi-Object Components .....	268
How to Copy Single-Object Components .....	268
Apply Updated Templates .....	268
MODS Migration .....	270
MODS File .....	270
Copy MODS Definitions .....	271
Panel Migration .....	271
Installation-Defined Panel Library .....	272
Individual Panels .....	272
Copy Panel Definitions .....	273
OSCNTL File Migration .....	274
PSM Default Values Migration .....	274
Region Links to a Multisystem Network .....	274
Important Considerations Prior to Linking .....	275
Link in Migration Mode .....	275
Migrate Subsequent Regions .....	276
Migrate a Multisystem Network .....	276
Scenario: Run Your Old Region in Parallel with the New Region .....	278

## **Appendix A: Defining UNIX System Services Authorization** **279**

USS Authorization Requirements .....	279
Set Up OMVS Segment .....	279

## **Appendix B: Tape Format** **283**

FMID Descriptions .....	283
-------------------------	-----

---

Format of Cartridge VOLSER C2D66A .....	284
Format of Cartridge VOLSER C2D66B .....	285

<b>Index</b>	<b>287</b>
--------------	------------



# Chapter 1: Overview

---

This guide describes how to install and implement CA NetMaster FTM.

This section contains the following topics:

[Audience Qualifications](#) (see page 13)

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

[Remaining Documentation](#) (see page 14)

[CA Mainframe Network Management Family of Products](#) (see page 15)

## Audience Qualifications

Readers of this book require knowledge in the following areas:

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

You work with the following personnel:

- Systems programmer for z/OS, VTAM, and TCP/IP definitions
- Security administrator, for library and started task access authority
- Storage Management Subsystem (SMS) or storage administrator, for direct access storage device (DASD) allocations

## How the Installation Process Works

The following steps describe the installation process:

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

## Remaining Documentation

The CA Technical Support site provides access to instructional documents that showcase your software and provide detailed explanations about its comprehensive, feature-rich components.

From the Documentation link, you can download the guides associated with your product individually or as a zip file. The zip file contains a bookshelf and index that let you access, search, and navigate the documentation.

### **More information:**

[Contact CA](#) (see page iv)

## CA Mainframe Network Management Family of Products

Your product is a member of the CA Mainframe Network Management family of products, which, collectively, are designed to address the management issues of mixed SNA and TCP/IP environments by providing monitoring, diagnostic, and performance management capabilities for mainframe-based TCP/IP and SNA networks.

The CA Mainframe Network Management family consists of the following products:

- CA NetMaster NM for TCP/IP provides mainframe-based TCP/IP network management.
- CA NetSpy is a network performance application for SNA networks.
- CA NetMaster NM for SNA provides mainframe-based SNA network management.
- CA NetMaster NA provides SNA resource automation.
- CA SOLVE:FTS provides a mainframe-to-mainframe file transmission service.
- CA NetMaster FTM provides management of file transfer activity, and the associated environment and infrastructure.
- CA NetMaster SM for CICS manages CICS socket-based connections by focusing on CICS usage, thereby providing an enhanced understanding of these connections to enable better diagnosis of CICS connection problems.
- CA NSM NetMaster Option manages mainframe network services from the CA NSM platform. Mainframe-based TCP/IP, SNA, and file transfer resources can be monitored and controlled using the standardized CA NSM presentations.

You can use your product in conjunction with any of these products, thereby letting you manage your networks with maximum efficiency and flexibility.





# Chapter 2: Preparing for Installation

---

This chapter provides the following:

- An overview of the processes required to get started
- Instructions about how to prepare your system installation
- Advice about how to prepare for migration

This section contains the following topics:

[Multiple Product Installation and Setup](#) (see page 17)

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

[CA Common Services Requirements](#) (see page 19)

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

[Storage Requirements](#) (see page 21)

[How CA LMP Statements Are Coded](#) (see page 21)

[Preparation Worksheets](#) (see page 24)

[Post-installation Worksheet](#) (see page 37)

[Migration Preparation](#) (see page 39)

## Multiple Product Installation and Setup

You can install multiple CA Mainframe Network Management products based on what you have purchased. You can also set up multiple products in one region.

Therefore, you can perform the steps in the *Installation Guides* for these products concurrently as you install and set them up.

**Note:** You cannot set up multiple products with CA NetSpy.

## Software Requirements

You must verify your system is set with the requirements described in this section.

### Operating Environment

Ensure that you have the appropriate operating environment. Your system must have:

- A currently-supported version of z/OS.

- If you intend to implement Secure Sockets Layer (SSL) for the web interface:
  - SMP/E V3R5.0.
  - IBM's 31-bit SDK for z/OS, Java 2 Technology Edition for the libjvm.x side deck. IBM's 64-bit SDK is *not* supported.
- If you intend to use CA TCPaccess CS version 6.0, ensure you are using Service Pack 3 (SP3) or later. If SP3 is not applied, the Packet Analyzer feature, if used with FTP policies, does not analyze or report on the packets that flow through a CA TCPaccess CS stack.

## WebCenter Requirements

Ensure all WebCenter users have the following minimum levels of third-party products installed on their PCs:

- Internet Explorer: 6.0 with SP1 *or* Firefox: 2.0
- Java Runtime Environment (JRE): 1.4.1\_03

### Notes:

- If you are using WebCenter over an IPv6 network, your WebCenter users need JRE 1.5.0\_12.
- If you are using a 64-bit browser, review the JRE support and minimum system requirements for 64-bit browsers on the Sun Java website.

## Additional Product Requirements

Ensure that you have these recommended levels of products:

- CA TCPaccess FTP Server: 2.0 or later
- CA XCOM Data Transport for Windows Family Professional: 3.0, maintenance level 3.00.0105d
- CA XCOM Data Transport for z/OS: 3.0, 3.1, 11.0, or 11.5
  - With 3.0, use the following maintenance level:  
Generation level 0109 - SP3  
PTF Q005474  
PTF Q005475  
PTF Q005476
  - With 11.0, use maintenance level PTF Q071170.

- CONNECT:Direct for OS/390:
  - 4.4 with maintenance level PUT4401
  - 4.5 with maintenance level PUT4501
  - 4.6 with maintenance level PUT4601
  - 4.7 with maintenance level PUT4701
- CONNECT:Direct for UNIX: 3.4
- CONNECT:Direct for Windows NT: 1.3, 3.3, 4.0, 4.1, or 4.2
- CONNECT:Mailbox: 3.1, with maintenance level CUM 3107, F18254, and F18361
- CA SOLVE:FTS: r11 or later

## Migration Mode

If you intend to use [migration mode](#) (see page 41) to link an r12 product region to a multisystem network at the following releases, ensure that you have applied the following APARs:

- r11.6: NY810AS (SP1)
- r11.5: RO12222 and NZ39503 (prerequisite fix NY710AS (SP1))
- r11.0: NZ39505 (prerequisite fixes NY604AS (SP2) and NZ29512)

## CA Common Services Requirements

Your system must have a currently supported version of CA Common Services for z/OS. The CA Common Services load library must be accessible to your product's address space and the SOLVE SSI address space through the JCL STEPLIB or system LNKLIST.

**Note:** The latest version of CA Common Services for z/OS is included in your package.

The following CA Common Services are used with CA NetMaster FTM:

- CAIRIM
- CA LMP
- CAISDI Service

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

## Security Requirements

While you are preparing your product for startup, you need access to the following security-controlled data sets or libraries on your system:

1. Ensure that you have READ authority to data sets with a prefix of CAI.\*. All tape data sets use this prefix.
2. Ensure that you have UPDATE authority to the following data sets or libraries:
  - Started task PROCLIB that stores the run-time JCL, for example, SYS1.PROCLIB
  - SYS1.PARMLIB
  - SYS1.VTAMLST or the library that stores VTAM application definitions and VTAM initialization parameters
  - SYS1.VTAMLIB for terminal mode table definitions
  - Master catalog, a requirement if you intend to define alias entries for data set prefixes
3. Update the following initialization parameter data set members if necessary:
  - SYS1.PARMLIB(IEFSSNxx) to add subsystem IDs
  - SYS1.PARMLIB(IEAAPFxx) to APF-authorize your load libraries
  - SYS1.PARMLIB(CONSOLxx) if your system does not use extended MCS consoles
  - SYS1.PARMLIB(LPALSTxx) if you want to use the SOLVE SSI task as the PPI provider
  - SYS1.PARMLIB(PROGxx) if you want CA Auditor for z/OS or CA Common Inventory Service to know of your products for your auditors
4. Ensure that the following conditions are met:
  - The user IDs associated with your started tasks have access to the run-time data sets created by the installation and setup processes (UPDATE authority required).
  - The user ID associated with the product region started task is authorized to issue system commands.
  - The user IDs associated with the product and SOLVE SSI region must have authority to use [UNIX System Services](#) (see page 279).

## Storage Requirements

CA NetMaster FTM has the following 3390 DASD space requirements:

- If you are using ESD, the following spaces are required:
  - 340 MB of z/OS UNIX file system space for downloading files
  - 530 cylinders for the unpacked files
- For installation and setup, the following spaces are required:
  - Installation = 1220 cylinders
  - IBM System Modification Program Extended (SMP/E) libraries = 280 cylinders
  - Region setup = 1510 cylinders
  - Setup temporary work area = 1400 cylinders

## How CA LMP Statements Are Coded

Before starting this product, you must code CA LMP statements for product license authorization.

To code CA LMP statements, do the following:

1. Install CAIRIM.
2. Activate LMP.
3. Add your product license codes to the LMP statements.
4. Place the LMP statements in the KEYS member of the PPOPTION data set.

**Note:** The KEYS member of the PPOPTION data set is specified in the CAS9 JCL procedure. For more information, see the *CA Common Services Administrator Guide*.

## KEYS Member—Add Execution Key

You must add the CA LMP execution key, provided on your product key certificate, to the CAIRIM parameters to ensure proper initialization. To define a CA LMP execution key to the CAIRIM parameters, modify the KEYS member in CAI.PPOPTION (CA Common Services for z/OS r11) or CAI.CAIOPTN (CA Common Services for z/OS r12).

This sample parameter structure for KEYS member has the following format:

```
PROD(pp) DATE(ddmmyy) CPU(tttt-mmmm/ssssss)
LMPCODE(kkkkkkkkkkkkkkkk)
```

Parameter definitions are as follows:

**PROD(pp)**

Specifies the two-character product code. This code agrees with the product code already in use by the CAIRIM initialization parameters for any earlier releases of this product (if applicable).

X3 is the value for your product.

**DATE(ddmmmyy)**

Specifies the CA LMP licensing agreement expiration date, for example, 13MAR12.

**CPU(tttt-mmmm/ssssss)**

**tttt**

Specifies the CPU type on which CA LMP is to run, for example, 3090.

**-mmm**

Specifies the CPU model on which CA LMP is to run, for example, 600.

**Note:** If the CPU type and or model require fewer than four characters, blank spaces are inserted for the unused characters.

**/ssssss**

Specifies the serial number of the CPU on which CA LMP is to run.

**LMPCODE(kkkkkkkkkkkkkkkkk)**

Specifies the execution key (kkkkkkkkkkkkkkkk) needed to run CA LMP. The key certificate shipped with each CA LMP software solution provides this CA LMP execution key.

**Example: Add CA LMP Execution Key**

This example shows a control statement for the CA LMP execution software parameter.

```
PROD(X3) DATE(27JUN12) CPU(3090-600/370623)
LMPCODE(52H2K06130Z7RZD6)
```

In this example, with your product running on the specified CPU, the CA LMP licensing agreement will expire on June 27, 2012. The product code and execution key values are different when you install your product at your site.

**Note:** For a full description of the procedure for defining the CA LMP execution key to the CAIRIM parameters and further details about the features and associated utilities of CAIRIM, see the *CA Common Services for z/OS Administrator Guide*.

## CA LMP Key Certificate

Examine the CA License Managed Program (CA LMP) key certificate. Your certificate contains the following information:

### **Product Name**

Defines the trademarked or registered name of your product as licensed for the designated site and CPUs.

### **Product Code**

Defines a two-character code that corresponds to the product.

### **Supplement**

Defines the reference number of your license for a particular facility and has the following format:

*nnnnnn-nnn*

This format differs slightly inside and outside North America and, in some cases, the reference number may not be provided at all.

### **CPU ID**

Defines the code that identifies the specific CPU for which installation of this product is valid.

### **Execution Key**

Defines an encrypted code required by CA LMP for installing your product. During installation, it is referred to as the LMP code.

### **Expiration Date**

Defines the date your license expires and has the following format:

*ddmmmyy*

**Example:** 21Mar12

### **Technical Contact**

Defines the name of the designated technical contact at your site who is responsible for the installation and maintenance of your product. CA addresses all CA LMP correspondence to this person.

### **MIS Director**

Defines the name of the Director of MIS or the person who performs such a function at your site. If the title but not the name of the individual is indicated on the certificate, supply the actual name when correcting and verifying the certificate.

### **CPU Location**

Defines the address of the building in which the CPU is installed.

## Preparation Worksheets

During the installation and setup process, you enter values that are used to do the following:

- Allocate data sets.
- Set initial parameters.
- Prepare for the use of your product.

You can print out the worksheets in this section to record the values needed for your site when installing the product.

**Note:** For information about data sets, see the *Reference Guide*.

## Installation

Gather the installation information in the following worksheet:

### JOB CARD Information

Gather the following JOB CARD information:

#### **Batch job class**

Record the value that your site uses here:

Class = \_\_\_\_\_

**Default:** A

#### **Batch job class for tape mounts**

(Not required for ESD) Record the value that your site uses here:

Class = \_\_\_\_\_

#### **Instructions to operator**

Record any instructions here:

---

---

---



## Unload Tape

(Optional) If you are installing from tape, gather the following information related to tape unloading:

### **Tape unit**

Record the value that your site uses here:

?device-in = \_\_\_\_\_

### **More information:**

[Tape Format](#) (see page 283)

## Unload DASD

Gather the following information related to unload DASD:

### **Data set prefix**

Do not include the name of your planned product region.

**Limits:** Maximum 29 characters

Record the value that your site uses here:

?dsnpref = \_\_\_\_\_

### **DASD unit**

Record the value that your site uses here:

?device-out = \_\_\_\_\_

### **DASD volume serial number**

Record the value that your site uses here:

?volser = \_\_\_\_\_

## Installation Parameters

Gather the following information related to installation parameters:

### **Prefix used for ESD Unzipped Data Sets**

(Optional) If your product or maintenance was delivered using ESD, record the data set prefix that your site uses here:

Data set prefix= \_\_\_\_\_

### **Tape information**

(Optional) If you are installing from tape, record the values that your site uses here:

Unit = \_\_\_\_\_

**Default:** CART

Expiry Date = \_\_\_\_\_

**Default:** 98000

### **Allocation Parameters**

Use these prefixes for high-level qualifiers for the different data set groups.

Record the values that your site uses here:

#### **SMP/E Target**

Data Set Prefix = \_\_\_\_\_

Management class = \_\_\_\_\_

Storage class = \_\_\_\_\_

Volume serial number = \_\_\_\_\_

Unit = \_\_\_\_\_

#### **SMP/E Distribution**

Data Set Prefix = \_\_\_\_\_

Management class = \_\_\_\_\_

Storage class = \_\_\_\_\_

Volume serial number = \_\_\_\_\_

Unit = \_\_\_\_\_

#### **SMP/E Libraries**

Data Set Prefix = \_\_\_\_\_

Management class = \_\_\_\_\_

Storage class = \_\_\_\_\_

Volume serial number = \_\_\_\_\_

Unit = \_\_\_\_\_

#### **SMP/E CSI**

Data Set Prefix = \_\_\_\_\_

Management class = \_\_\_\_\_

Storage class = \_\_\_\_\_

Volume serial number = \_\_\_\_\_

**SMPTLIB**

Data Set Prefix = \_\_\_\_\_

Volume serial number = \_\_\_\_\_

Unit = \_\_\_\_\_

**Language Environment Parameters**

Record these language environment values:

**Language Environment library**

Record the value that your site uses here:

SCEELKD = \_\_\_\_\_

**Default:** CEE.SCEELKD**Language Environment link-edit input**

Record the value that your site uses here:

SCEELIB = \_\_\_\_\_

**Default:** CEE.SCEELIB**Language Environment link-edit input 2**

Record the value that your site uses here:

SCEEBND2 = \_\_\_\_\_

**Default:** CEE.SCEEBND2**System Programmer C routines**

Record the value that your site uses here:

SCEESPC = \_\_\_\_\_

**Default:** CEE.SCEESPC**IBM Macros**

Record the value that your site uses here:

MODGEN=\_\_\_\_\_

**Default:** SYS1.MODGEN**Data set that contains the GIMZPOOL member**

Record the value that your site uses here:

\_\_\_\_\_

**Default:** SYS1.MACLIB

## Region Setup

Gather the region setup information in the following worksheet:

### SOLVE Subsystem Interface Region

Gather the following information related to the SOLVE Subsystem Interface region:

**Name of the SOLVE SSI started task (*ssiname*)**

Record the value that your site uses here:

\_\_\_\_\_

**Default:** SOLVESSI

**Name of the SOLVE SSI SYSIN member**

This member contains control statements for starting the SOLVE SSI.

Record the value that your site uses here:

SYSIN = \_\_\_\_\_

**Default:** SSISYSIN

**Name of the optional SOLVE SSI parameter member**

This member contains startup parameters for the SOLVE SSI. If omitted, startup parameters are included in the SOLVE SSI SYSIN member previously described.

Record the value that your site uses here:

PARAMETER = \_\_\_\_\_

**Subsystem ID for a SOLVE SSI started task**

Record the value that your site uses here:

SSID = \_\_\_\_\_

**Default:** SOLV

**Prefix for SOLVE SSI data sets**

Record the value that your site uses here:

\_\_\_\_\_

**Default:** *dsnpref*

## Product Region

Gather the following information related to the product region:

### Product region started task name (*rname*)

Record the value that your site uses here:

\_\_\_\_\_

**Default:** NM

### Product region SYSIN member name

Record the value that your site uses here:

SYSIN = \_\_\_\_\_

**Default:** RUNSYSIN

### Primary VTAM ACB name for the product region

Record the value that your site uses here:

PRI = \_\_\_\_\_

**Default:** NM

### Mixed case passwords

Specifies whether case is preserved (YES) or forced to uppercase (NO):

XOPT = \_\_\_\_

**Default:** NO

### Security exit setting (**NO**|PARTSAF|NMSAF|*lname*)

Record the value that your site uses here:

SEC = \_\_\_\_\_

**Default:** NO

**Note:** For more information about setting your security exit, see the *Security Guide*.

### Prefix for VSAM data sets local to the product region

Record the value that your site uses here:

\_\_\_\_\_

**Default:** *dsnpref.rname*

### Prefix for sequential data sets local to the product region

Record the value that your site uses here:

\_\_\_\_\_

**Default:** *dsnpref.rname*

**Prefix for TESTEXEC**

Record the value that your site uses here:

\_\_\_\_\_

**Default:** *dsnpref.rname*

**Prefix for UAMS or full name of existing UAMS**

Record the value that your site uses here:

\_\_\_\_\_

**Default:** *dsnpref*

**Prefix for shareable VSAM data sets**

Record the value that your site uses here:

\_\_\_\_\_

**Default:** *dsnpref.NMCO*

**Prefix for shareable PARMLIB data sets**

Record the value that your site uses here:

\_\_\_\_\_

**Default:** *dsnpref.NMCO.PARMLIB*

**AOM subsystem interface ID**

Record the value that your site uses here:

AOMSSID = \_\_\_\_\_

**Default:** *Domain ID*

**Note:** Ensure that this value does not conflict with other subsystems. The AOM subsystem interface enables system message flow to the region.

**AOM message suppression character**

Record the value that your site uses here:

\_\_\_\_\_

**Default:** */*

**AOM SSI command prefix string**

Record the value that your site uses here:

\_\_\_\_\_

**Default:** *DomainId>*

**Note:** If you use a command string prefix for other tasks, ensure that this value is not in conflict with them.

**External application ACB pool names****Full-screen terminal prefix**

Record the value that your site uses here:

\_\_\_\_\_

**Default:** NMMAF

**LU1 terminal prefix**

Record the value that your site uses here:

\_\_\_\_\_

**Default:** NMMAV

**NMFTP Monitor**

Gather the following NMFTP Monitor information:

**Name of the NMFTP Monitor started task(*nmftname*)**

Record the value that your site uses here:

\_\_\_\_\_

**Default:** NMFTPMON

**Name of the NMFTP Monitor SYSIN member**

Record the value that your site uses here:

SYSIN = \_\_\_\_\_

**Default:** FTPSYSIN

**Name of the NMFTP Monitor parameter member**

This member contains startup parameters for the NMFTP monitor. If omitted, startup parameters are included in the NMFTP Monitor SYSIN member previously described.

Record the value that your site uses here:

PARAMETER = \_\_\_\_\_

**Subsystem ID for an NMFTP Monitor started task**

Record the value that your site uses here:

SSID = \_\_\_\_\_

**Default:** NFTP

**Prefix for NMFTP Monitor data sets**

Record the value that your site uses here:

\_\_\_\_\_

**Default:** *dsnpref*

## VTAM Definitions

Gather the following information related to VTAM definitions:

### **VTAM major node name**

Record the value that your site uses here:

\_\_\_\_\_

**Default:** VTAMAPPL

### **System macro library**

Record the value that your site uses here:

\_\_\_\_\_

**Default:** SYS1.MACLIB

### **VTAM network definitions library**

Record the value that your site uses here:

\_\_\_\_\_

**Default:** SYS1.VTAMLST

### **VTAM macro library**

Record the value that your site uses here:

\_\_\_\_\_

**Default:** SYS1.SISTMAC1

### **VTAM load library**

Record the value that your site uses here:

\_\_\_\_\_

**Default:** SYS1.VTAMLIB

### **(Optional) External Interface Package (EIP) ACB Prefix**

Record the value that your site uses here:

\_\_\_\_\_

**Default:** NMTSO

## TCP/IP Setup

Gather the TCP/IP setup information in the following worksheet:

### **Name and release of the TCP/IP software**

Record the value that your site uses here:

\_\_\_\_\_



## IBM Communications Server

Gather the following information related to the IBM Communications Server:

**Started task user ID for product region**

Record the value that your site uses here:

\_\_\_\_\_

**Started task user ID for SOLVE SSI**

Record the value that your site uses here:

\_\_\_\_\_

**Started task user ID for NMFTP Monitor region**

Record the value that your site uses here:

\_\_\_\_\_

**PW.SRC data set name**

Record the value that your site uses here:

\_\_\_\_\_

**Default:** /etc/pw.src

**Stack IP address**

Record the value that your site uses here:

\_\_\_\_\_

**PROFILE.TCPIP data set name**

Record the value that your site uses here:

\_\_\_\_\_

**TCPIP.DATA data set name**

Record the value that your site uses here:

\_\_\_\_\_

**Name of the FTP startup JCL procedure**

Record the value that your site uses here:

\_\_\_\_\_

## CA TCPaccess CS

Gather the following information related to the CA TCPaccess CS:

### **IJTCFGxx member**

Record the value that your site uses here:

---

### **DNRALCxx member**

Record the value that your site uses here:

---

### **DNRHSTxx member**

Record the value that your site uses here:

---

### **DNRCFGxx member**

Record the value that your site uses here:

---

### **SNMCFGxx member**

Record the value that your site uses here:

---

### **CA TCPaccess CS subsystem ID**

Record the value that your site uses here:

---

**Default:** ACSS

### **CA TCPaccess CS Job Name**

Record the value that your site uses here:

---

### **PARM data set name**

Record the value that your site uses here:

---

## File Transfer Setup

Gather the File Transfer setup information in the following worksheet:

**CA XCOM****Name of the CA XCOM Data Transport startup JCL procedure**Record the value that your site uses here:  
  
\_\_\_\_\_**Name of the Default Options Table**Record the value that your site uses here:  
  
\_\_\_\_\_**CONNECT:Direct****CONNECT:Direct for OS/390 user ID and password for the region**Record the value that your site uses here:  
  
\_\_\_\_\_**Concatenation of CONNECT:Direct PROCESS files**Record the value that your site uses here:  
  
\_\_\_\_\_**Name of the CONNECT:Direct startup JCL procedure**Record the value that your site uses here:  
  
\_\_\_\_\_**CONNECT:Direct for OS/390 initialization parameter****STATISTICS.EXIT**Record the value that your site uses here:  
  
\_\_\_\_\_**Name of user exit, if you are using an existing exit**Record the value that your site uses here:  
  
\_\_\_\_\_

## **CONNECT:Mailbox**

### **Name of the CONNECT:Mailbox VSAM administration file**

Record the value that your site uses here:

\_\_\_\_\_

### **Name of the CONNECT:Mailbox startup JCL procedure**

Record the value that your site uses here:

\_\_\_\_\_

### **CONNECT:Mailbox for MVS initialization parameters**

#### **Name of user exit, if you are using an existing exit**

Record the value that your site uses here:

\_\_\_\_\_

#### **Name of the ODF file**

Record the value that your site uses here:

\_\_\_\_\_

## **FTP**

### **SAF qualifier for access control**

Record the value that your site uses here:

\_\_\_\_\_

## Startup Tasks

Gather information related to the startup tasks in the following worksheet:

### **Initial administrator user ID**

Record the value that your site uses here:

---

### **Initial administrator password**

Record the value that your site uses here:

---

### **Port number for inbound connections (if you intend to use TCP/IP as a transport method for INMC links)**

Record the value that your site uses here:

---

**Default:** 2636

### **Port number for WebCenter**

Record the value that your site uses here:

---

**Default:** NONE

## Post-installation Worksheet

After you have completed the installation and setup processes, you can record the data set names generated by the Install Utility for future reference.

You can print out the following worksheet now, and record this information as you progress through the remaining chapters in this guide.

### **Installation data set**

Record the value generated by the Install Utility here:

---

**Default:** *dsnpref.NMC0.CAIJCL*

### **Installation JCL data set**

Record the value generated by the Install Utility here:

---

**Default:** *dsnpref.NMC0.INSTALL.JCL*

**More information:**

[Generate the Installation JCL](#) (see page 167)

**SOLVE SSI setup JCL data set**

Record the value generated by the Install Utility here:

\_\_\_\_\_

**Default:** *dsnpref.NMC0.ssiname.JCL*

**More information:**

[Specify the SOLVE SSI Region](#) (see page 203)

**Product region setup JCL data set**

Record the value generated by the Install Utility here:

\_\_\_\_\_

**Default:** *dsnpref.NMC0.rname.JCL*

**More information:**

[Specify the Product Region](#) (see page 204)

**NMFTP Monitor region setup JCL data set**

Record the value generated by the Install Utility here:

\_\_\_\_\_

**Default:** *dsnpref.NMC0.nmftname*

**More information:**

[Specify the NMFTP Monitor Region](#) (see page 207)

**VTAM JCL data set**

Record the value generated by the Install Utility here:

\_\_\_\_\_

**Default:** *dsnpref.NMC0.VTAM.JCL*

**More information:**

[Create VTAM Definitions and Tables](#) (see page 209)

## Migration Preparation

Some migration tasks require actions on the region that you are migrating from. If you are planning to reuse resources for your new product region, such as access control block (ACB) name and started task name, make sure that you perform these tasks before you shut down your existing region for the last time.

**More information:**

[Performing Initial Migration](#) (see page 243)

[Completing Migration](#) (see page 265)

## Parameter Group Values

If you do not use a region initialization (INI) file and want to migrate your previous parameter group values to your r12 product region, record these values now because you will need them to customize the product region.

## How to Migrate Your Initialization File

If you have an existing region INI file from r11 onwards, you can migrate the file for use in this release.

**Important!** You must review and update the file to ensure that names such as ACBs, data sets, and interfaces are suitable for the new region.

The process of migrating your INI file consists of the following steps:

1. If you have not already generated your INI file, generate the INI file in the previous region.
2. Configure the file by updating the data set names used, and checking the ACB and various interface names. Alternatively, you can delete the configuration section for a whole parameter group to let the defaults for the new region be used.

**Note:** During region initialization, the INI file is applied by passing all parameter values to the INI file procedure and letting the procedure overwrite the values as needed. If you do not want to overwrite the settings for a parameter group or individual parameter, comment out or delete the statements in the INI file that contains the group or parameter. Setting the value of a parameter to null sets the parameter value to null, which may not be what you wanted.

3. Start the new region using the INI file by editing your RUNSYSIN.

After you start the region, you can check it and regenerate the INI if necessary.

**Important!** Generation of the INI file replaces custom code, such as code that includes MVS system symbols, with the actual values. If you regenerate the file, you need to reapply the custom code.

**Note:** For more information about setting up the initialization file, see the *Administration Guide*.

## Knowledge Base

If you want to migrate your knowledge base, consider the following:

- To keep a copy of an old distributed ResourceView template (for example, you might have modified it), copy this template to a new template image version above 0009. You can copy a template image from the Template System Image List panel (/RADMIN.T.I).
- To keep a copy of an old distributed EventView rule set (for example, you might have modified it), make a copy of this rule set under a different name. (If the rule set is associated with a system image, update the association accordingly.) You can copy a rule set from the Ruleset List panel (/EADMIN.R.R).



## Multisystem Considerations

You cannot link and synchronize a new region with a region running an earlier release of the product.

### How Migration Mode Works

You can use migration mode to assist in the migration of an existing multisystem network.

Migration mode gives the new product region the same level of visibility as normal synchronization, but a slightly reduced command capability. The main difference between migration mode and normal synchronization is that the databases are not synchronized, and single point database maintenance is not possible in migration mode.

Migration mode works as follows:

1. You unlink an existing region from the multisystem network.
2. You migrate this region to the latest release.
3. You link the newly-migrated region back into the multisystem network.
4. After the new region is linked back, you can monitor all resources for all linked regions from the new region.
5. When the next region is unlinked and migrated to the latest release, it can be linked and synchronized in the standard way to the first migrated region.

Each region can be migrated as required without losing the benefits of multisystem monitoring.

#### **More information:**

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

## How to Prepare for Multisystem Network Migration

If you are upgrading multiple synchronized regions to r12, perform the following steps to plan for it.

1. Ensure your existing multisystem network has at least two focal regions. If you have only one focal region, unlink a subordinate region and relink it as a focal region.
2. Choose a focal region and unlink it from the multisystem network.
3. Upgrade the focal region to r12 and perform migration tasks.
4. After you have completed all of the steps in the remaining chapters in this guide, [link your new focal region in migration mode](#) (see page 274) to an existing focal region.
5. Select the next product region to upgrade and unlink it.
6. Upgrade this product region and then synchronize it to the focal region that you upgraded in Step 3.
7. Continue until all regions are upgraded.

### Notes:

- You only need to perform knowledge base migration for the first region because the focal knowledge base contains details of all linked regions.
- You only need to link the first new focal region in migration mode.

# Chapter 3: Installing Your Product Using CA MSM

---

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

**Note:** If you do not have CA MSM, you can download it from the Download Center at CA Support Online. Follow the installation instructions in the *CA Mainframe Software Manager Product Guide*, available on the Documentation page of <https://support.ca.com/>.

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

This section contains the following topics:

- [CA MSM Documentation](#) (see page 43)
- [Getting Started Using CA MSM](#) (see page 44)
- [Acquiring Products](#) (see page 53)
- [Installing Products](#) (see page 59)
- [Maintaining Products](#) (see page 65)
- [Setting System Registry](#) (see page 77)
- [Deploying Products](#) (see page 105)

**Important!** During installation, use the CAIT66 target zone and the CAID66 distribution zone. The setup process requires that these zone names have been used.

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

## CA MSM Documentation

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

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

## Getting Started Using CA MSM

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

### How to Use CA MSM: A Scenario

Your organization recently deployed CA MSM to simplify the installation of CA products and unify their management. The organization has also licensed a new CA product. In addition, you have a number of existing CSIs from previously installed products. The first scenario shows how you can use CA MSM to acquire and install the new product; The second scenario shows how you can use CA MSM to deploy the product to your target systems; and the third scenario shows how you can use CA MSM to maintain products already installed in your environment.

#### Acquire and Install a New Product

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

1. To use CA MSM to acquire or download a product, you must have a CA Support Online account. If you do not have an account, you can create one through the CA Support website.
2. To [access CA MSM](#) (see page 52), you require its URL. You can get the URL from your site's CA MSM administrator and log in using your z/OS credentials. When you log in for the first time, you are prompted to create a CA MSM account with your CA Support Online credentials. This account enables you to download product packages from CA.
3. After you log in to CA MSM, you can see the products to which your organization is entitled on the Software Catalog tab. If you cannot find the product you want to acquire, [update the catalog](#) (see page 53). CA MSM refreshes the catalog through CA Support Online using the site IDs associated with your CA Support Online credentials.
4. After you find your product in the catalog, you can [download the product installation packages](#) (see page 54). CA MSM downloads (acquires) the packages (including any maintenance packages) from the CA FTP site.
5. After you acquire the product installation packages, you can find the packages at the product gen level you want. From there, you can [install your product](#) (see page 59). A wizard guides you through the installation process. A CSI is created for the installed product as part of the installation process. You also can install a product to an existing CSI.

## Deploy a Product using the Wizard

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

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

1. Find out what systems you have at your enterprise.
2. Add systems to system registry and validate them.
3. [Create remote credentials](#) (see page 103) for those systems in CA MSM.
4. [Add FTP](#) (see page 100) information along with data destination information to each system registry entry.
5. [Create a methodology](#) (see page 132).
6. Use the [deployment wizard](#) (see page 106) to build a deployment.
7. If you need to deploy other products to the systems defined above using the same methodologies, repeat step 6.

## System Registration

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

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

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

### 1. Remote Credentials

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

- remote user ID
- remote system name
- password
- authenticated authorization before creating a remote credential.

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

## 2. System Registry

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

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

### Non-Sysplex Systems

The *Non-Sysplex* is a stand-alone z/OS system that is not part of a sysplex system.

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

### Sysplex or Monoplex Systems

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

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

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

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

### Shared DASD Clusters

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

### Staging Systems

A *Staging system* is a CA MSM deployment services term. It is a virtual system. A Staging system deploys the deployment to the computer where the CA MSM driving system is located. To use a Staging system, the CA MSM driving system must be registered in the CA MSM System Registry.

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

#### 3. FTP Location Information

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

#### 4. Data Destinations

A data destination must be defined for every system. The data destination is how you tell CA MSM which technique to use to transport the deployment data to the remote system. The two choices are FTP and Shared DASD. When FTP is selected as the transport mechanism, the deployment data is shipped to the target system through FTP. It is temporarily placed on the target system at the landing directory specified in the FTP Location information section of the system Registry.

When shared DASD is specified, CA MSM uses a virtual transport technique. That is, it does not actually copy the data from one system to the other. Because the two systems share DASD, there is no need to do this. All of the deployment data is kept in USS file systems managed by CA MSM. The remote system, even though the DASD is shared, may not be able to find the deployment data in the USS file system. Therefore, CA MSM temporarily unmounts the file system from the CA MSM driving system and mounts it in read-only mode on the remote system. For CA MSM to determine where to mount the file system on the remote system, you must specify a mount point location in the data destination. In addition, you can provide allocation information for the creation of the deployment file system, so that when the file system is created on the CA MSM driving system, it will be on the DASD that is shared.



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

The remote allocation information is used by the deployment process on the remote system, letting you control where the deployed software is placed. By specifying the GIMUNZIP volser, CA MSM adds a "volume=" parameter to the GIMUNZIP instructions on the remote system. The list of zFs volsers is only needed if (1) the software you are deploying contains USS parts, and (2) you select a "container" copy option during the deployment process.

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

#### 5. Registered Systems

You need to register each system by validating that it exists. You should validate your Non-Sysplex Systems first, and then your Sysplex or Shared Cluster Systems.

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

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

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

You are now ready to set up your products to be deployed.

### Deploying Products using the Wizard

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

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

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

1. Deployment Name and Description

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

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

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

2. CSI Selection

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

3. Product Selection

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

4. Custom Data Set

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

- For a z/OS data set, you need to provide a data set name that is the actual existing z/OS data set and a mask that names the data set on the target system. This mask may be set up using [symbolic qualifiers](#) (see page 135) 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 135) 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 123).

## 5. Methodology

Methodology is the process by which data sets are named on the target system.

A methodology provides the how of a deployment, that is, what you want to call your data sets. It is the named objects with a description that are assigned to an individual deployment.

To add a methodology, you need to specify the following:

- Data set name mask (which lets you choose symbolic variables that get resolved during deployment)
- Disposition of the target data sets:
  - If you select Create, the target data sets cannot exist, and if they do, the deployment will fail.
  - If you select Create or Replace and the target data sets do not exist, they will be created. If they do exist, this new deployment will overwrite existing target data sets.

You can [create a methodology](#) (see page 132).

## 6. System Selection

Select the system for this deployment.

## 7. Preview

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

Use this option to review your deployment before deploying.

## 8. Deploy

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

## 9. Confirm

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

## 10. Summary

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

## Maintaining Existing Products

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

1. To maintain an existing CSI in CA MSM, you first migrate the CSI to CA MSM. During the migration, CA MSM stores information about the CSI in the database.
2. After the CSI is migrated, you can [download the latest maintenance](#) (see page 66) 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 66).
3. After you download the latest maintenance, you can [apply the maintenance](#) (see page 69).

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

## Access CA MSM Using the Web-Based Interface

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

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

### To access CA MSM using the web-based interface

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

The login page appears.

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

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

The initial page appears. If you log in for the first time, you are prompted to define your CA Support Online account.

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

3. Click New.

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

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

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

You are prompted to review your user settings.

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

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

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

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

## Acquiring Products

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

### Update Software Catalog

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

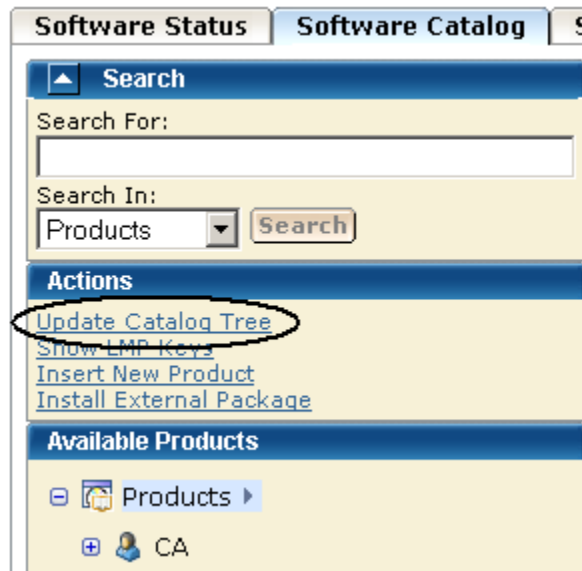
If you update the catalog tree and some changes are missing, check your CA Support Online user settings.

#### To update your software catalog

1. Click the Software Catalog tab.

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

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 view the details of the actions. Click Close to return to the previous page.

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

## Download Product Installation Package

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

### To download a product installation package

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

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

The product releases are listed.

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

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

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

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

The product packages are downloaded.

**Note:** You can expand the tree in the right panel by selecting a product and clicking the vendor link in the right panel, but if you use this method and select multiple products, be aware that if one of the selected products cannot be downloaded, the remaining products will not be processed. If this happens, remove the checks from the ones that were processed and repeat the update catalog request.

## Migrate Installation Packages Downloaded External to CA MSM

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

Migrating these packages to CA MSM enables you to have a complete view of all your product releases. After a package is migrated, you can use CA MSM to [install the product](#) (see page 59).

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

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

The packages for the gen level are listed.

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

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

## Download Multiple Product Installation Packages

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

### To download multiple product installation packages

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

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

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

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

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

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

The product packages are downloaded.

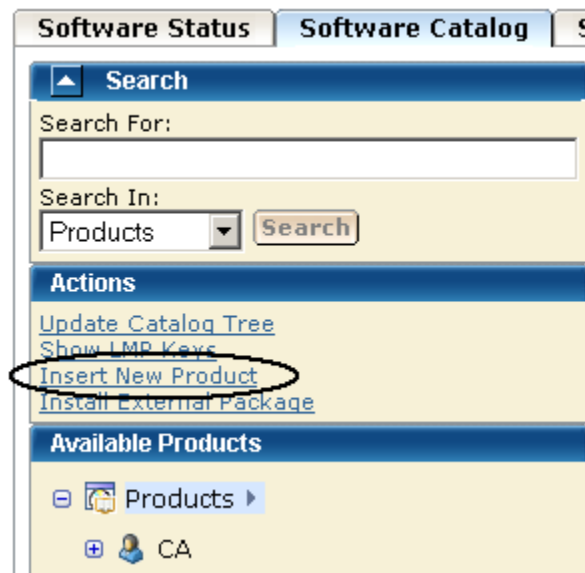


## Add a Product

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

### To add a product package to CA MSM

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



You are prompted to supply information about the product.

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

**Note:** If you need to add several packages from the same location, you can use [masking](#) (see page 58).

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

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

## Masking for External Packages

Masking lets you to add more than one package (or set of maintenance files) from the same location based on a pattern (mask). You can use masking for components, maintenance in USS, and maintenance in data sets. You can use masking for files only, not for directories.

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

- For PDS and PDSE, you can mask members using asterisks.
- For sequential data sets, use the following characters:

**?**

Match on a single character.

**\***

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

**\*\***

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

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

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

### Example 1

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

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

### Example 2

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

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

### Example 3

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

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

### Example 4

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

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

## Delete a Product

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

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

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

You are prompted to confirm the action.

3. Click OK.

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

**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.

## 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.

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:

The screenshot shows the 'Software Catalog' tab selected. On the left, the 'Available Products' tree is expanded to 'CA Panvalet - MVS' > '14.5' > 'SP1'. The main area displays 'Base Install Packages' for 'SP1'. A table lists the following packages:

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

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

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

The Introduction tab of the wizard appears.

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

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

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

You are prompted to select the type of installation.

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

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

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

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

- If no prerequisites exist, click Next.

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

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

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

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

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

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

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

If you select Create a New SMP/E CSI, you are prompted to [specify the CSI parameters](#) (see page 63).

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

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

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

After a CSI is selected or a new CSI is specified, you are prompted for the target zone to use.

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

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

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

After a target zone is selected or specified, you are prompted for the distribution zone to use.

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

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

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

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

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

9. Review the summary, and click Install.

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

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

## Create a CSI

You can create a CSI while you are [installing a product](#) (see page 59). During the process, you are asked to specify data set allocation parameters, which you can then customize for each data set, as well as parameters for DDDEF allocation.

### To create a CSI

1. Click Create a New SMP/E CSI from the product installation wizard.  
You are prompted to define a CSI.
2. Specify a name for the environment represented by the CSI, and the following VSAM and data set allocation parameters. You can leave the other parameters at their defaults.
  - Specify the prefix for the name of the CSI VSAM data set.
  - Specify the prefix for the names of the SMP/E data sets.
  - Select whether to use SMS, and complete the appropriate fields.

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

3. Click Next.

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

4. 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.

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

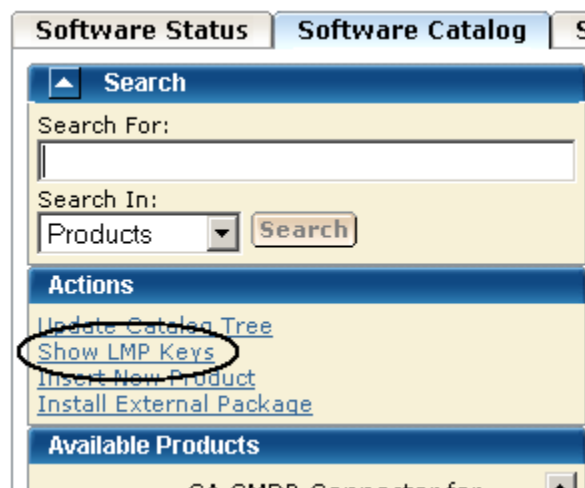
You are prompted to specify any additional parameters. A new CSI is specified.

## Download LMP Keys

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

### To retrieve and list the LMP keys for your products

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



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

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

The list is refreshed for the selected site ID.

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



3. Click Update Keys.

You are prompted to confirm the update.

4. Click OK.

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

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

## Maintaining Products

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

### How to Apply Maintenance Packages

Use this process to download and apply product maintenance packages.

1. Identify your download method. This section details the steps to use three download methods:

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

Contact your system administrator, if necessary.

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

**Note:** This section also details the procedure to back out maintenance that has been applied but not yet accepted.

## Download Product Maintenance Packages

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

### To download product maintenance packages

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

CA MSM uses the credentials to access CA Support Online.

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

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

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

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

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

The maintenance packages are downloaded.

### More information:

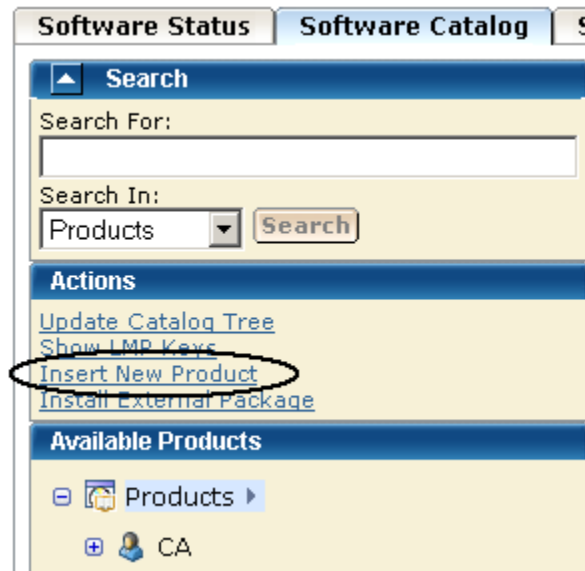
[Download Maintenance Packages for Old Product Releases and Service Packs](#)  
(see page 66)

## Download Maintenance Packages for Old Product Releases and Service Packs

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

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

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



You are prompted to supply information about the product release.

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

**Note:** Use the same product name that appears on the product tree, and use the release and gen level values as they appear for Published Solutions at CA Support Online.

The product release is added to the software catalog.

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

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

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

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

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

## Manage Maintenance Downloaded External to CA MSM

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

Adding these maintenance packages to CA MSM provides you with a complete view of all the maintenance for a product release. After a package is migrated, you can use CA MSM to [apply the maintenance](#) (see page 69).

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 58).

4. Click OK.

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

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

### View Aggregated Package Details

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

#### To view aggregated package details

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

The maintenance packages for the release are listed.

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

The Maintenance Package Details dialog opens.

3. Click the Nested Packages tab.

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

### Manage Maintenance

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

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

The following installation modes are available:

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

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

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

### To manage maintenance for a product

1. Click the Software Catalog tab, and select the product from the tree at the left.

Maintenance information appears at the right for the releases you have.

2. Click Update Catalog Release for the release on which you want to apply maintenance.

The maintenance information is updated.

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

The maintenance packages are listed, for example:

Software Status		Software Catalog	SMP/E Environments	Deployments	System Registry	Tasks	Settings																																																																													
<div><div><div><div>Search</div><div>Search For:</div><div>Search In:</div><div>Products</div><div>Search</div></div><div>Actions</div><div><div>Update Catalog Tree</div><div>Show SMP Keys</div><div>Insert New Product</div><div>Install External Package</div></div><div>Available Products</div><div><div><div><div>CA Panvalet - MVS</div><div>14.4</div><div>14.5</div><div>SP1</div></div><div><div>CA Panvalet Option for ISPF MVS</div><div>CA Panvalet Option for TSO MVS</div><div>CA Partition Expert for DB2 for z/OS - MVS</div><div>CA PDSMAN PDS Library Management ALL 5 COMPONENTS - MVS</div><div>CA PDSMAN PDS Library Management All Extensions and Performance - MVS</div></div></div></div></div></div>			<div>14.5</div> <div>Products &gt; CA &gt; CA Panvalet - MVS &gt; 14.5</div> <div><div>Maintenance Packages</div><div>Add External Maintenance</div><div>Refresh</div></div> <div>show: AllAll for current releaseAll source IDs</div> <div>Select and: Install1 - 10 of 70 &gt;&gt;</div> <table><tr><th><input type="checkbox"/> Select</th><th><input type="checkbox"/> Fix #</th><th>Description</th><th>Confirmed Date</th><th>Type</th><th>Installed</th><th>Actions</th></tr><tr><td><input type="checkbox"/></td><td>Q185660</td><td>* PRODUCT DOCUMENTATION CHANGE</td><td>Jan 29, 2007</td><td>PEA/PDC</td><td>Not installable</td><td>Actions</td></tr><tr><td><input type="checkbox"/></td><td>Q089243</td><td>* PRODUCT ERROR ALERT *</td><td>Jun 20, 2007</td><td>PEA/PDC</td><td>Not installable</td><td>Actions</td></tr><tr><td><input type="checkbox"/></td><td>R012055</td><td>0607: MSM INST. ADD SUPPORT FOR SAMPJCL UNDER SMP/E</td><td>Oct 7, 2009</td><td>PTF</td><td>No (0/1)</td><td>Actions</td></tr><tr><td><input type="checkbox"/></td><td>Q088256</td><td>14.5-SP00: PANO/PAN#1 INPUT STREAM INVALID COMMAND</td><td>May 11, 2007</td><td>PTF</td><td>No (0/1)</td><td>Actions</td></tr><tr><td><input type="checkbox"/></td><td>Q088259</td><td>14.5-SP01: PANO/PAN#1 INPUT STREAM INVALID COMMAND</td><td>May 11, 2007</td><td>PTF</td><td>No (0/1)</td><td>Actions</td></tr><tr><td><input type="checkbox"/></td><td>Q086490</td><td>14.5-SP00: DOING ++WRITE, LNG FMT CHANGED AFTER</td><td>Mar 6, 2007</td><td>PTF</td><td>No (0/1)</td><td>Actions</td></tr><tr><td><input type="checkbox"/></td><td>Q090975</td><td>14.5-SP00/SP01: PAM DIRECTORY AVERAGE BYTES</td><td>Sep 4, 2007</td><td>PTF</td><td>No (0/1)</td><td>Actions</td></tr><tr><td><input type="checkbox"/></td><td>Q081764</td><td>14.5-SP00: PAN#1 ++CONTROL WITH NO CODE GIVES ERROR</td><td>Aug 25, 2006</td><td>PTF</td><td>No (0/1)</td><td>Actions</td></tr><tr><td><input type="checkbox"/></td><td>Q081765</td><td>14.5-SP00: PV071 DOING ++SCANS OF ZTYPE1-8 MEMBERS</td><td>Aug 25, 2006</td><td>PTF</td><td>No (0/1)</td><td>Actions</td></tr><tr><td><input type="checkbox"/></td><td>Q086868</td><td>14.5-SP00: ZTYPE7 NOT FORMATTED CORRECTLY ON TSO</td><td>Mar 19, 2007</td><td>PTF</td><td>No (0/1)</td><td>Actions</td></tr></table>					<input type="checkbox"/> Select	<input type="checkbox"/> Fix #	Description	Confirmed Date	Type	Installed	Actions	<input type="checkbox"/>	Q185660	* PRODUCT DOCUMENTATION CHANGE	Jan 29, 2007	PEA/PDC	Not installable	Actions	<input type="checkbox"/>	Q089243	* PRODUCT ERROR ALERT *	Jun 20, 2007	PEA/PDC	Not installable	Actions	<input type="checkbox"/>	R012055	0607: MSM INST. ADD SUPPORT FOR SAMPJCL UNDER SMP/E	Oct 7, 2009	PTF	No (0/1)	Actions	<input type="checkbox"/>	Q088256	14.5-SP00: PANO/PAN#1 INPUT STREAM INVALID COMMAND	May 11, 2007	PTF	No (0/1)	Actions	<input type="checkbox"/>	Q088259	14.5-SP01: PANO/PAN#1 INPUT STREAM INVALID COMMAND	May 11, 2007	PTF	No (0/1)	Actions	<input type="checkbox"/>	Q086490	14.5-SP00: DOING ++WRITE, LNG FMT CHANGED AFTER	Mar 6, 2007	PTF	No (0/1)	Actions	<input type="checkbox"/>	Q090975	14.5-SP00/SP01: PAM DIRECTORY AVERAGE BYTES	Sep 4, 2007	PTF	No (0/1)	Actions	<input type="checkbox"/>	Q081764	14.5-SP00: PAN#1 ++CONTROL WITH NO CODE GIVES ERROR	Aug 25, 2006	PTF	No (0/1)	Actions	<input type="checkbox"/>	Q081765	14.5-SP00: PV071 DOING ++SCANS OF ZTYPE1-8 MEMBERS	Aug 25, 2006	PTF	No (0/1)	Actions	<input type="checkbox"/>	Q086868	14.5-SP00: ZTYPE7 NOT FORMATTED CORRECTLY ON TSO	Mar 19, 2007	PTF	No (0/1)	Actions
<input type="checkbox"/> Select	<input type="checkbox"/> Fix #	Description	Confirmed Date	Type	Installed	Actions																																																																														
<input type="checkbox"/>	Q185660	* PRODUCT DOCUMENTATION CHANGE	Jan 29, 2007	PEA/PDC	Not installable	Actions																																																																														
<input type="checkbox"/>	Q089243	* PRODUCT ERROR ALERT *	Jun 20, 2007	PEA/PDC	Not installable	Actions																																																																														
<input type="checkbox"/>	R012055	0607: MSM INST. ADD SUPPORT FOR SAMPJCL UNDER SMP/E	Oct 7, 2009	PTF	No (0/1)	Actions																																																																														
<input type="checkbox"/>	Q088256	14.5-SP00: PANO/PAN#1 INPUT STREAM INVALID COMMAND	May 11, 2007	PTF	No (0/1)	Actions																																																																														
<input type="checkbox"/>	Q088259	14.5-SP01: PANO/PAN#1 INPUT STREAM INVALID COMMAND	May 11, 2007	PTF	No (0/1)	Actions																																																																														
<input type="checkbox"/>	Q086490	14.5-SP00: DOING ++WRITE, LNG FMT CHANGED AFTER	Mar 6, 2007	PTF	No (0/1)	Actions																																																																														
<input type="checkbox"/>	Q090975	14.5-SP00/SP01: PAM DIRECTORY AVERAGE BYTES	Sep 4, 2007	PTF	No (0/1)	Actions																																																																														
<input type="checkbox"/>	Q081764	14.5-SP00: PAN#1 ++CONTROL WITH NO CODE GIVES ERROR	Aug 25, 2006	PTF	No (0/1)	Actions																																																																														
<input type="checkbox"/>	Q081765	14.5-SP00: PV071 DOING ++SCANS OF ZTYPE1-8 MEMBERS	Aug 25, 2006	PTF	No (0/1)	Actions																																																																														
<input type="checkbox"/>	Q086868	14.5-SP00: ZTYPE7 NOT FORMATTED CORRECTLY ON TSO	Mar 19, 2007	PTF	No (0/1)	Actions																																																																														

Red asterisks identify HIPER maintenance packages.

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

The Maintenance Package Details dialog appears, identifying any prerequisites.

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

5. Select the maintenance packages you want to install, and click the Install link.

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

The Introduction tab of the wizard appears.

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

The packages to install are listed.

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

The SMP/E environments that contain the product to maintain are listed. Only environments in your working set are listed.

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

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

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

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

- If prerequisites exist and are available, review them and click Next. CA MSM installs these prerequisites as part of the process. If a prerequisite is *not* available, the wizard cannot continue. You must acquire the prerequisite and restart the process.
- If [HOLDDATA](#) (see page 173) entries exist, review and select them, and click Next.

A summary of the task appears.

11. Review the summary, and click Install.

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

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

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

**More information:**

[Download Product Maintenance Packages](#) (see page 66)

[Download Maintenance Packages for Old Product Releases and Service Packs](#) (see page 66)

## View Installation Status of Maintenance Package

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

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

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

### To view installation status of a maintenance package

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

The maintenance packages for the release are listed.

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

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

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

## USERMODs

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

You can create a USERMOD manually, or CA can provide an unpublished maintenance package as a USERMOD. In this case, the USERMOD file, which contains the ++USERMOD statement and the body of the USERMOD, must be [managed as an externally downloaded package](#) (see page 68).



## GROUPEXTEND Mode

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

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

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

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

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

- Apply check
- Apply
- Apply check and apply

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

## How Maintenance in GROUPEXTEND Mode Works

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

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

3. Run the maintenance in Apply mode, and specify SYSMODs that you want to exclude and HOLDDATA that you want to bypass, if any exist.

The followings options are available for bypassing HOLDDATA:

- HOLDSYSTEM
- HOLDCLASS
- HOLDERERROR
- HOLDUSER

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

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

## Manage Maintenance in GROUPEXTEND Mode

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

### To manage maintenance for a product in GROUPEXTEND mode

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

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

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

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 the Link status for a maintenance package is available, you can click it to review a list of zones where the maintenance package is already received, applied, or accepted. Click Close to return to the wizard.

5. Review the packages, and click Next.

The Prerequisites tab of the wizard appears.

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

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

Installation options appear.

7. Specify installation options as follows, and click Next:

- a. Select the installation mode for the selected maintenance.
- b. Review the GROUPEXTEND options and select those you want to apply to the maintenance:

**NOAPARS**

Excludes APARs that resolve error reason ID.

**NOUSERMODS**

Exclude USERMODs that resolve error user ID.

- c. (Optional) Enter SYSMODs that should be excluded in the Excluded SYSMODs field. You can enter several SYSMODs separated by a comma.

The Bypass HOLDDATA tab of the wizard appears.

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

9. Click Next.

A summary of the task appears.

10. Review the summary, and click Apply GROUPEXTEND.

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

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

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

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

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

## Back Out Maintenance

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

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

### To back out a maintenance package from a product release

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

Products installed in the environment are listed.

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

The features in the component are listed.

**Note:** If you want to back out maintenance from all the products in the environment, you can click the Maintenance tab to list all the maintenance packages for the environment.

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

The maintenance packages for the feature are listed.

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

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

The Introduction tab of the wizard appears.

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

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

The packages to back out are listed.

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

7. 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.

**Note:** If prerequisites exist, review them and click Next. CA MSM will restore these prerequisites as part of the process.

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

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

## Setting System Registry

This section includes information about how to use CA MSM to set the system registry. The system registry contains all systems that can be selected as a target for a deployment.

### About System Registry

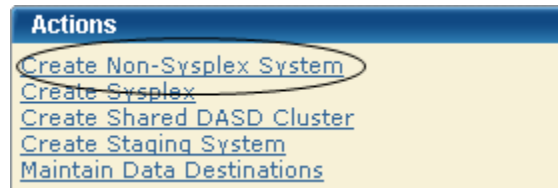
The system registry contains all systems that can be selected as a target for a deployment. You can create Non-SYSPLEX, SYSPLEX, Shared DASD Cluster, and Staging systems as well as maintain, validate, investigate a failed validation, view, and delete a system register.

## Create Non-Sysplex System

You can create a Non-Sysplex System Registry.

### To create a Non-Sysplex system registry

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

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

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

2. Enter the Non-Sysplex System Name.

**Limits:** Maximum 8 characters.

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

3. Enter the Description.

**Limits:** Maximum 255 characters.

4. Enter the CCI System ID:

**Limits:** Maximum 8 characters.

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

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

**Note:** Click Cancel to withdraw this create request.

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

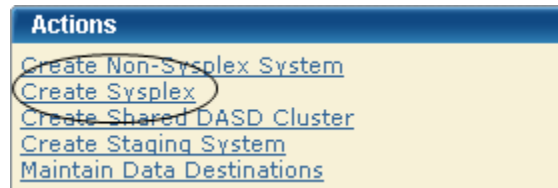
Property Name: z/OS LPAR Name, Value: \*\* Not Applicable \*\*.

## Create Sysplex or Monoplex

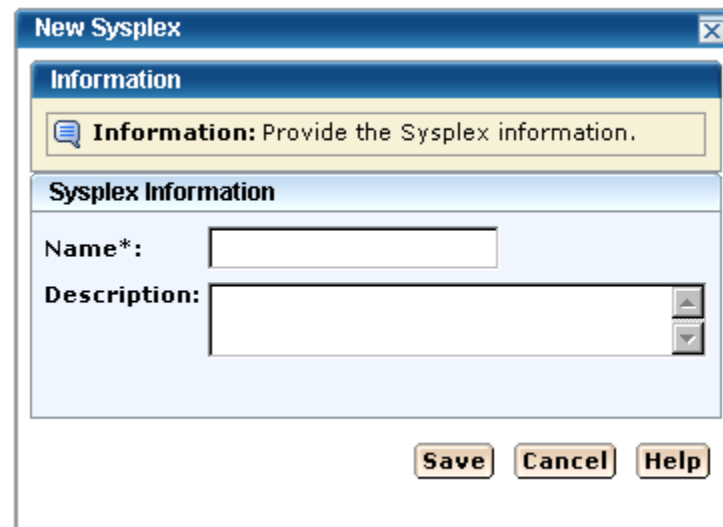
You can create a [Sysplex](#) (see page 80) or Monoplex system registry.

### To create a Sysplex or Monoplex system registry

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



The Sysplex System window appears.

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

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

2. Enter the Sysplex System Name.

**Limits:** Maximum 8 characters.

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

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



This procedure was created to help customers that have Monoplexes with the same Sysplex name (for example: LOCAL). Instead of showing multiple LOCAL Sysplex entries which would need to be expanded to select the correct Monoplex system, the CA MSM System Registry shows the actual Monoplex system name at the top level Sysplex name.

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

3. Enter the Description.

**Limits:** Maximum 255 characters.

4. Click Save to save this new Sysplex System.

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

**Note:** Click Cancel to withdraw this create request.

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

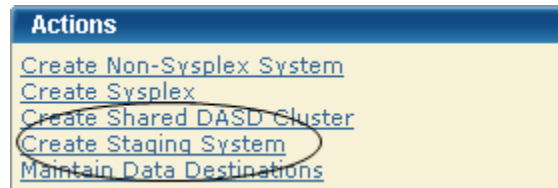
Property Name: z/OS LPAR Name, Value: \*\* Not Applicable \*\*.

## Create Staging System

You can create a Staging System.

### To create a Staging System

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



The New Staging System window appears.

A screenshot of a 'New Staging System' dialog box. The dialog has a title bar with 'New Staging System' and a close button. Inside, there's an 'Information' section with a message icon and the text 'Information: Provide the z/OS system information.' Below this is a 'Staging System Information' section. It contains two fields: 'Name\*' with a text input box, and 'Description:' with a larger text area. At the bottom right of the dialog are three buttons: 'Save', 'Cancel', and 'Help'.

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

2. Enter the Staging System Name.

**Limits:** Maximum 8 characters.

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

3. Enter the Description.

**Limits:** Maximum 255 characters.

4. Click Save to save this new Staging System.

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

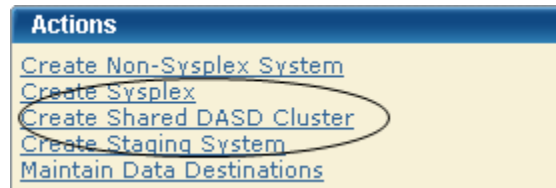
**Note:** Click Cancel to withdraw this create request.

## Create Shared DASD Cluster

You can create a Shared DASD Cluster.

### To create a Shared DASD Cluster

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



The New Shared DASD Cluster window appears.

A screenshot of a dialog box titled 'New Shared DASD Cluster'. It has a blue header bar with the title and a close button. Below the header is an 'Information' section with a yellow background and a message icon, containing the text 'Information: Provide the Shared DASD Cluster information.' Below this is a 'Sysplex Information' section with a light blue background. It contains two labels: 'Name\*:' followed by a text input field, and 'Description:' followed by a larger text area with vertical scrollbars. At the bottom right of the dialog are three buttons: 'Save', 'Cancel', and 'Help'.

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

2. Enter the Shared DASD Cluster Name.

**Limits:** Maximum 8 characters.

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

3. Enter the Description.

**Limits:** Maximum 255 characters.

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

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

**Note:** Click Cancel to withdraw this create request.

## Authorization

There are two authorization modes for the Systems Registry.

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

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

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

## Maintain a System Registry

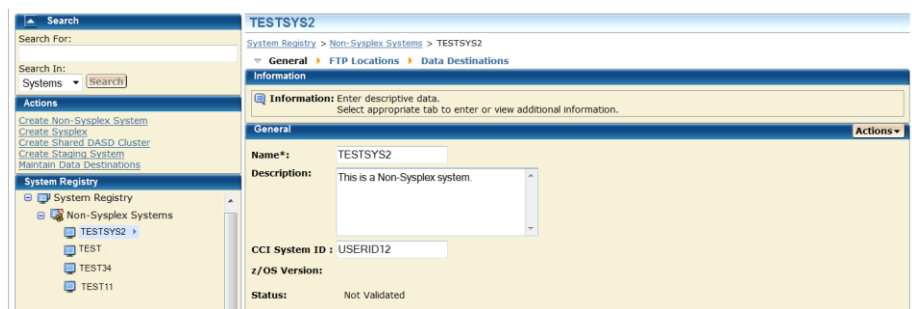
You can maintain the system registry.

### To maintain a system registry

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

The detailed information appears at the right.

2. Select the system to maintain.



3. Update the Name as needed.

**Limits:** Maximum 8 characters.

4. Update the Comments as needed.

**Limits:** Maximum 255 characters.

5. Update the CCI System ID:

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

**Limits:** Maximum 8 characters.

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

For example, assume contact system is set to CO11, FTP location URI is set to XX61 and the remote credentials are set up for CO11.

The deployment could fail because your remote credentials might not be the same on both systems (CO11 and XX61) and you set the Contact System to CO11, but you are contacting to XX61 and it will fail because spawn will be started on CO11 but we will look for the output on XX61 because that is where the FTP location was set.

The screenshot shows the 'General' tab of the 'Data Destinations' configuration window. The 'Name\*' field is set to 'PLEXC1'. The 'Description' field contains 'Test enviornment SYSPLEX'. The 'Contact System' dropdown is set to 'CO11'. The 'z/OS Version' is '01.11.00'. The 'Status' is 'Validated'. The 'Sysplex name' is 'PLEXC1'. The window has tabs for 'General', 'FTP Locations', and 'Data Destinations'. An 'Information' message at the top says: 'Enter descriptive data. Select appropriate tab to enter or view additional information.'

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

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

This procedure was created to help customers that have Monoplexes with the same sysplex name (for example: LOCAL). Instead of showing multiple LOCAL sysplex entries which would need to be expanded to select the correct Monoplex system, the CA MSM System Registry shows the actual Monoplex System name at the top level Sysplex Name.

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

7. For Staging systems, enter the GIMUNZIP volume and/or zFS candidate volumes.

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

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

The screenshot shows a web-based configuration interface for a staging system. At the top, there is a breadcrumb trail: [System Registry](#) > [Staging Systems](#) > Stage1. Below this is a 'General' tab with an 'Information' section containing a message: 'Information: Enter descriptive data.' The main configuration area is titled 'General' and includes an 'Actions' dropdown menu. The fields are as follows:

- Name\*:** Stage1
- Description:** Staging System
- GIMUNZIP Volume:** TSO16A
- zFS Candidate Volumes:** TSO16A, followed by four empty input boxes.

8. Select the Action from the Actions list in the General bar.

#### Cancel

Cancel this maintenance.

#### Save

Save the changes to this maintenance.

#### Validate

Validate authenticates this entry.

**Note:** The validation process is done in steps; each system in this request is validated with the last step summarizing, verifying, and confirming the validation. If the validation fails this steps will show how the validation failed. See [How to Investigate a Failed Validation](#) (see page 87).

#### Validation Rules

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

**Note:** A Staging system is not validated.

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

This table shows the system validation results and actions.

Result	Action
Validated	System is available, status is updated as valid, and system registry is updated with results from validation.
Validation in Progress	System status is updated to in progress.
Validation Error	System status is updated to error. See <a href="#">How to Investigate a Failed Validation</a> (see page 87).
Not Validated	This system has not been validated yet.
Not Accessible	The system has not been validated because it is no longer available or was not found in the CCI Network.
Validation Conflict	System has been contacted but the information entered then different then the information retrieved.

#### Error details

When a validation is in error the Error details button appears. Click this button to find the reason for this conflict. See [How to Investigate a Failed Validation](#) (see page 87).

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

#### Conflict details

When a validation is in conflict, the Error details button appears. Click this button to find the reason for this conflict. See [How to Investigate a Failed Validation](#) (see page 87).

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

### How to Investigate a Failed Validation

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

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

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

### To investigate a failed validation using the Tasks Page

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

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

2. Click the Tasks Tab and then click the Task History link.
3. At the Show bar select All task, or My task to list the tasks by Owner.

**Note:** You can refine the task list by entering USER ID, types, and status.

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

Task History <span>Refresh</span>						
Current date and time is 1/12/2010 03:41:56PM						
Show: <span>USER456</span> <span>All types</span> <span>All status</span> <input type="checkbox"/> Start time <input type="checkbox"/> Stop time <span>Show All</span>						
Owner	Name	Type	Status	Start Time	Stop Time	Task ID
USER456	<a href="#">Validating System: XX60</a>	System Registry	<span>Failed</span>	1/12/2010 02:26:01PM	1/12/2010 02:26:09PM	432

5. The Validate System window appears.

Search

Search For:

Search In:

Search all

Task Steps

Validate System: XX60

Validating System: XX60

messageLog

Validation Results

messageLog

Validate System: XX60 Close

General Download zipped output

Name: Validate System: XX60

Task ID: 447

User ID: USER456

Status: Failed

Status message: Failed to undo command

Steps

#	Name	Description	Status
1	<a href="#">Validating System: XX60</a>	Validating system and retrieving values.	Succeeded
2	<a href="#">Validation Results</a>	Validation results for all the systems that were validated.	Failed



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

**Validation Results** Close

Validate System: XX60 > Validation Results

**General** Download zipped output

Name: Validation Results  
Status: Failed

**MessageLog** Action

System validation was inaccessible for system: XX60, refer to messageLog output in appropriate validation step.

**Explanation**

Validation results for all the systems that were validated.

**Detailed Output**

Show All

Name	Lines	Format	Action
Table does not contain any record.			

### The Message Log.

**messageLog** Close

Validate System: XX60 > Validation System: XX60 > messageLog

Search:  Search Page: 1 / 1

Validation started for system: XX60  
System Validation failed.  
MSMD3001E: The requested system: XX60 is no longer available or was not found in the CCI Network.

### To investigate a failed validation immediately after Validation

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

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

Software Status | Software Catalog | SMP/E Environments | Deployments | **System Registry** | Tasks | Settings

**Search**

Search For:

Search In:  Search

**Actions**

Create Non-Sysplex System  
Create Sysplex  
Create Shared DASD Cluster  
Create Staging System  
Maintain Data Destinations

**System Registry**

System Registry  
Non-Sysplex Systems  
EE20  
EE21  
XX60  
SYS2  
SYSY  
EE12  
CO11  
SEE10

**XX60**

System Registry > Non-Sysplex Systems > XX60

**General** FTP Locations Data Destinations

**Information**

Information: Enter descriptive data.  
Select appropriate tab to enter or view additional information.

**General** Actions

Name\*: XX60

Description: X60 finance system

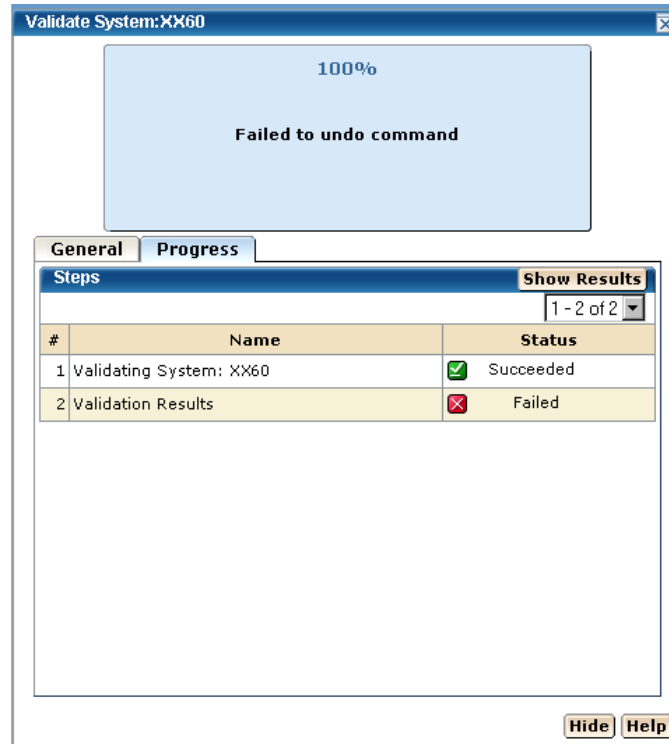
CCI System ID:

z/OS Version:

Status: Not Accessible Details

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

- Click the Progress tab.



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

## Download Message Log

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

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

### To Download as TXT

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

### To Download as ZIP

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

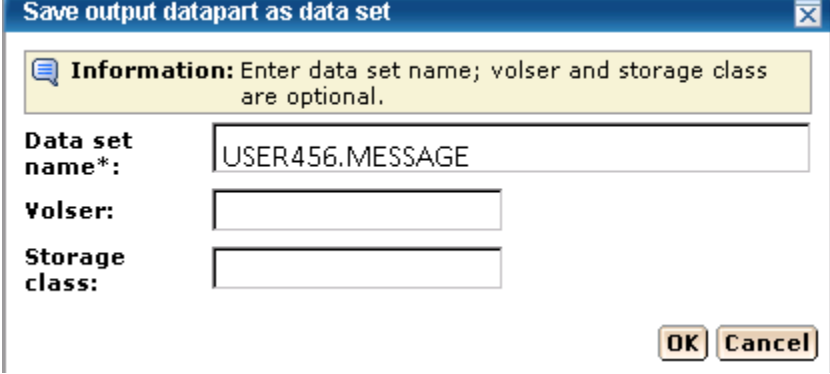
## Save a Message Log as a Data Set

### To save as a data set

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

The Save output as a data set window appears.

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



**Save output datapart as data set**

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

**Data set name\*:** USER456.MESSAGE

**Volser:**

**Storage class:**

**OK Cancel**

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

2. The data set name has been entered by the system.

For Non-SMS data, enter the Volser.

### Example:

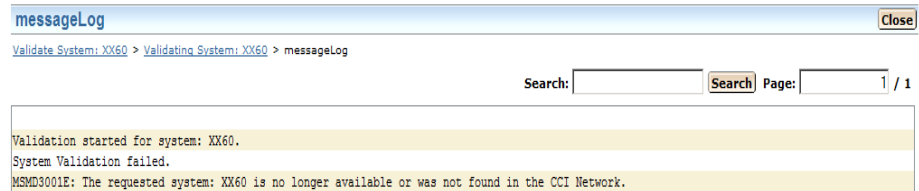
Volsers: SYSP01 and SYSP02

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

## To Show All

### To Show all

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



2. Click Close.

### To Download as TXT

Save the file.

### To Download as ZIP

Save the file.

## Delete a System Registry

You can delete a system registry.

### To delete a system registry

1. Click the System Registry tab.  
The System Registry window appears.
2. On the right, in the System Registry panel, select Non-Sysplex Systems, Sysplexes, Clusters, or Staging Systems link.  
The system list appears.
3. Click the Select box for each system registry you want to delete.
4. Click the Delete link and then click OK to the Delete confirmation window.  
The system is deleted.

## Data Destinations

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

## Create Data Destinations

You can create data destinations.

### To create a data destination

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

**New Data Destination**

**Information**

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

**General**

**Name\*:**

**Description:**

**Transmission Method:** ☒ Shared DASD ☐ FTP

**Mount Point\*:**

**Storage Class:**

**VOLSER:**

**Remote Allocation Data**

**GIMUNZIP Volume:**

**zFS Candidate Volumes:**

**Save** **Cancel** **Help**

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

3. Enter a meaningful Name.

**Limits:** Maximum 64 characters.

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

4. Enter the Description.

**Limits:** Maximum 255 characters.

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

**Default:** Shared DASD.

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

Mount point is a directory path that must exist on the target system. The user that is doing the deployment must have write permission to this directory.

The deployment user must have write permissions for the mount directory. The deployment user ID must have mount authorization on the target system.

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

**Limits:** Maximum 120 characters

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

7. Enter the Storage Class,

**Limits:** Maximum 8 characters

**Example:**

Storage Class: SYSPRG

8. Enter the Volser.

**Limits:** Maximum 6 characters

**Example:**

Volsers: SYSP01 and SYSP02

9. Enter the GIMUNZIP volume.

**Limits:** Maximum 6 characters

10. Enter zFS Candidate volumes.

**Limits:** Maximum 6 characters

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

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

**Note:** Click Cancel to withdraw this create request.

12. For FTP, select FTP button.

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

**Transmission Method:** ☐ Shared DASD ☒ FTP

**Information** Please ensure an FTP location is defined for the system.

**Remote Allocation Data**

**GIMUNZIP Volume:**

**zFS Candidate Volumes:**

**Save** **Cancel** **Help**

13. Enter the GIMUNZIP Volume.

**Limits:** Maximum 6 characters

14. Enter the zFS Candidate Volumes.

**Limits:** Maximum 6 characters

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

**Note:** Click Cancel to withdraw this create request.

## Add a Data Destination

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

### To add a current data destination to an existing system

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

The detailed information appears at the right.

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

3. Click the Data Destination tab.

The Data Destination window appears.

4. Click Add.

The Pick data destination window appears.

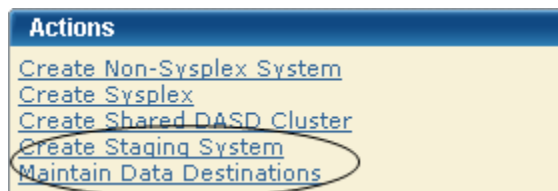
5. Select the data destinations you want to add and click Select.

## Maintain Data Destinations

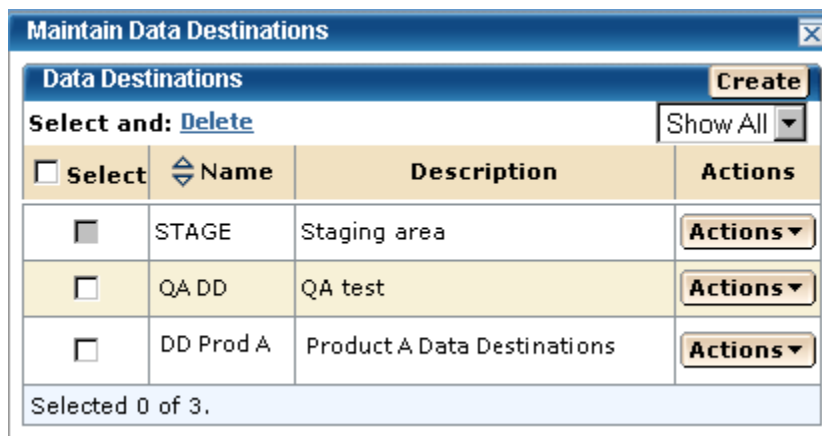
You can maintain, [delete](#) (see page 100), or [create](#) (see page 93) data destinations.

### To maintain current data destinations

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



The Maintains Data Destinations window appears.



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



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

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

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

**Edit Data Destination**

**Information**

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

**General**

**Name\*:** Company DASD

**Description:** allow users to deploy to company dasd using Shared Dasd

**Transmission Method:** ☒ Shared DASD ☐ FTP

**Mount Point\*:** /c/users/ccispns/dep

**Storage Class:** storgage

**VOLSER:** volser2

**Remote Allocation Data**

**GIMUNZIP Volume:** volumzip

**zFS Candidate Volumes:** [ ] [ ] [ ] [ ]

**Save** **Cancel** **Help**

3. Enter a meaningful Name.

**Limits:** Maximum 64 characters.

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

4. Enter the Description.

**Limits:** Maximum 255 characters.

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

**Default:** Shared DASD.

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

Mount point is a directory path that must exist on the target system. The user that is doing the deployment must have write permission to this directory.

The deployment user must have write permissions for the mount directory. The deployment user ID must have mount authorization on the target system.

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

**Limits:** Maximum 120 characters

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

7. Enter the Storage Class, and the Volsers.

**Example:**

Storage Class: SYSPRG

Volsers: SYSP01 and SYSP02

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

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

10. Click Save.

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

**Note:** Click Cancel to withdraw this create request.

11. For FTP, select FTP button.

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

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

12. Enter the GIMUNZIP Volume.
13. Enter the zFS Candidate Volumes.
14. Click Save.

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

**Note:** Click Cancel to withdraw this create request.

## Set a Default Data Destination

You can set a default for a current data destination.

### To set a default for a current data destination

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

The detailed information appears at the right.

2. Click the data destination link.

The data destination window appears.

3. Select the data destination to you want as a default.
4. In the Action box select Set as Default.

The word Default appears in the Default column.

## Delete Data Destinations

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

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

### To delete a data destinations

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

The detailed information appears at the right.

2. Select the system where you want to delete a data destination.
3. Click the Data Destination tab.

The Data Destination window appears.

4. Click the Select box for each data destination you want to remove.
  5. Click the Delete link and then click OK to the Delete confirmation window.
- The data destination is deleted.

## FTP Locations

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

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

## Add FTP Locations

You can add, [edit](#) (see page 101), [set default](#) (see page 102), or [remove](#) (see page 102) FTP locations.

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

### To add FTP locations

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

The detailed information appears at the right.

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

3. Click the FTP Locations tab.  
The FTP Locations window appears.
4. Click Add.  
The New FTP Location window appears.
5. Enter URI.  
**Limits:** Maximum length is 255.
6. Enter Port.  
**Limits:** Maximum Port number is 65535 and must be numeric.  
**Default:** 21
7. Enter Directory Path  
**Limits:** Most start with a root directory, that is /.
8. Click Save.

**More Information:**

[Edit FTP Locations](#) (see page 101)

[Set FTP Location Default](#) (see page 102)

[Remove FTP Locations](#) (see page 102)

## Edit FTP Locations

You can edit FTP locations.

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

**To edit FTP locations**

1. Click the System Registry tab, and select Non-Sysplex Systems, Sysplexes, Shared DASD Clusters, or Staging Systems from the tree at the left.
2. The detailed information appears at the right.
3. Click the system link where you want to create FTP locations.
4. Click the FTP Location tab. The FTP Locations window appears.
5. Select the FTP location and select Edit on the Actions drop down. The Edit FTP Location window appears.
6. Edit the URI.  
**Limits:** Maximum length is 255.

7. Edit the Port.

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

**Default:** 21

8. Edit the Directory Path

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

9. Click Save.

## Set FTP Location Default

You can set an FTP location default.

### To set an FTP location default

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

The detailed information appears at the right.

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

3. Click the FTP Locations tab.

The FTP Locations window appears.

4. Select the FTP locations and select Default on the Actions drop down.

The word Default appears in the Default Column.

## Remove FTP Locations

You can remove FTP locations.

### To remove FTP locations

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

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

3. Click the FTP Locations tab.

The FTP Locations window appears.

4. Click the Select box for each FTP location you want to remove.

5. Click the Remove link and then click OK to the Remove FTP location confirmation window.

The FTP location is removed.

## Remote Credentials

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

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

You can [add](#) (see page 103), [edit](#) (see page 104), or [delete](#) (see page 105) remote credentials.

### Add Remote Credentials

You can add remote credentials.

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

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

#### To add remote credentials

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

**Limits:** Maximum 64 characters.

4. Enter a correct Remote System Name.

**Limits:** Maximum 8 characters.

**Example:** RMinPlex

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

5. Enter a correct password.

**Limits:** Minimum 2 characters and Maximum 63 characters.

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

6. Enter the correct confirm password.

**Limits:** Minimum 2 characters and Maximum 63 characters.

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

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

## Edit Remote Credentials

You can edit remote credentials.

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

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

### To edit remote credentials

1. Click the Setting tab, and select Remote Credentials from the tree at the left. The detailed information appears at the right.
2. In the Actions drop down list, click Edit for the remote credential you want to edit. The Edit Remote Credential window appears.
3. Enter a correct Remote User ID.

**Limits:** Maximum 64 characters.

4. Enter a correct Remote System Name.

**Limits:** Maximum 8 characters.

**Example:** RMinPlex

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

5. Enter a correct password.

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

**Limits:** Minimum 2 characters and Maximum 63 characters.

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



6. Enter the correct confirm password.

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

**Limits:** Minimum 2 characters and Maximum 63 characters.

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

7. Click OK.

The remote credential entry appears on Remote Credentials Accounts List.

8. Click Apply to apply and save your changes.

### Delete Remote Credentials

You can delete remote credentials.

#### To delete remote credentials

1. Click the Setting tab, and select Remote Credentials from the tree at the left.

The detailed information appears at the right.

2. In the Actions drop down list, click Delete for the remote credential you want to delete.

A Delete Confirmation window appears.

3. Click OK.

## Deploying Products

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

### About Deployments

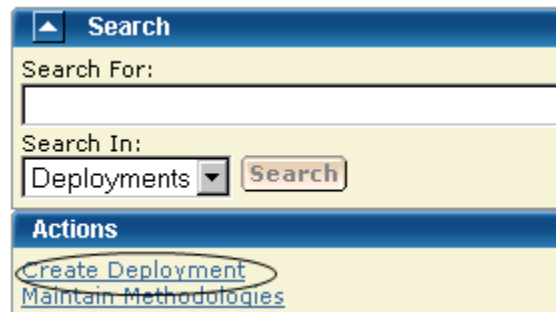
Deployments allow system objects to be deployed across the enterprise. These services enable deployment across both "Shared DASD" environments and networked environments. The objects to be deployed include target libraries defined to SMP/E and user-selected data sets.

## Create a Deployment using the Product Wizard

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

### To create a deployment

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



The Deployment of Products wizard appears.

### Enter Name and Description

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

#### Do the following

1. Enter a meaningful deployment name.

**Limits:** Maximum 64 characters.

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

2. Enter the description of this deployment.

**Limits:** Maximum 255 characters.

3. Click Next.

The CSI Selection window appears.

**Note:** When creating a deployment, you can save this deployment at any step in this wizard. This "under construction" deployment is added to the current deployments list. You can [maintain this deployment](#) (see page 114) until a successful snapshot has been created.

## CSI Selection

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

### To select a CSI


1. Select a CSI, and click Next.

The Product Selection window appears.

**Note:** When creating a deployment, you can save this deployment at any step in this wizard. This "under construction" deployment is added to the current deployments list. You can [maintain this deployment](#) (see page 114) until a successful snapshot has been created.

## Product Selection

### To select a product

1. Select a product from the list.
2. If there is a  text icon in Text column, click the text icon to read the instructions supplied by CA Support for product, data sets, and other necessary information.
3. Click the "I have read the associated text by selecting the text icon from the list about" box. This box appears only if there is a text icon.

**Note:** You will not be able to click Next until you click this box.

4. Click Next.

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

**Note:** When creating a deployment, you can save this deployment at any step in this wizard. This "under construction" deployment is added to the current deployments list. You can [maintain this deployment](#) (see page 114) until a successful snapshot has been created.

Custom Data Sets Selection window appears.

## Custom Data Sets

A *custom data set* contains either an z/OS data set or USS parts paths. For an z/OS data set you need to provide a data set name that is the actual existing z/OS data set and a mask that names the data set on the target system. This mask may be set up using [symbolic qualifiers](#) (see page 135) 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 135) and type of copy. Type of copy can be either a container copy or a file-by-file copy.

**To select a custom data set**

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

**Note:** To add a new custom data set click the Add Data Set button and [enter the custom data set information](#) (see page 123).

The Methodology Selection window appears.

**More Information:**

[Add a Custom Data Set](#) (see page 123)

## Methodology Selection

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

### To select a Methodology

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

**Note:** To create a new methodology click the Create button and [enter the new methodology information](#) (see page 132).

**New Deployment**

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

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

**Methodologies** Create

1 - 5 of 44

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

Save Back Next Deploy Cancel Help

System Selection window appears.

**Note:** When creating a deployment, you can save this deployment at any step in this wizard. This "under construction" deployment is added to the current deployments list. You can [maintain this deployment](#) (see page 114) until a successful snapshot has been created.

### More Information:

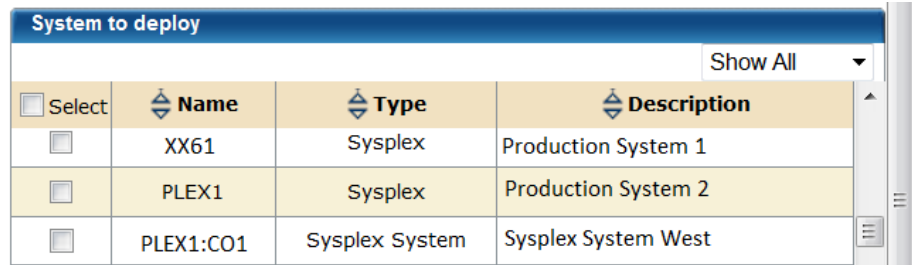
[Create a Methodology](#) (see page 132)

## System Selection

1. Select the systems to be deployed

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

**Note:** Sysplex systems are denoted by Sysplex System:System Name. For example PLEX1:CO11 where PLEX1 is Sysplex name and CO11 is the system name.



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

2. Click Next.

The Preview window appears.

**Note:** When creating a deployment, you can save this deployment at any step in this wizard. This "under construction" deployment is added to the current deployments list. You can [maintain this deployment](#) (see page 114) until a successful snapshot has been created.

## Preview

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

**Note:** Click Cancel to exit this procedure without saving.

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

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

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

### Deployment Preview Sample

This sample shows a deployment ready to be deployed.

**New Deployment**

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

**Preview**

**Identification**  
**Deployment Id:** ???  
**Name:** Deployment Test  
**Style of Deployment** Create only

**Products**  
**Name:** Endevor R14.0 **Source:** Endevor R14 CSI

**Systems**  
**Name:** PRODSTAG

**Transport**  
 to PRODSTAG: No transmission needed

**Target Libraries on PRODSTAG**

<b>Source DDN:</b> CSIQAUTH	<b>DSN:</b> USER456.R14MSM.CSIQAUTH
<b>Target DSN:</b> &SYSUID..D&MSMDID.	
<b>Resolved as:</b> USER456.D???.CSIQAUTH	
<b>Source DDN:</b> CSIQAUTU	<b>DSN:</b> USER456.R14MSM.CSIQAUTU
<b>Target DSN:</b> &SYSUID..D&MSMDID.	
<b>Resolved as:</b> USER456.D???.CSIQAUTU	
<b>Source DDN:</b> CSIQCLS0	<b>DSN:</b> USER456.R14MSM.CSIQCLS0
<b>Target DSN:</b> &SYSUID..D&MSMDID.	
<b>Resolved as:</b> USER456.D???.CSIQCLS0	
<b>Source DDN:</b> CSIQJCL	<b>DSN:</b> USER456.R14MSM.CSIQJCL
<b>Target DSN:</b> &SYSUID..D&MSMDID.	

**Save Back Next Deploy Cancel Help**

**New Deployment**

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

**Resolved as:** USER456.D???.CSIQPJPN  
**Source DDN:** CSIQPRCR **DSN:** USER456.R14MSM.CSIQPRCR  
**Target DSN:** &SYSUID..D&MSMDID.  
**Resolved as:** USER456.D???.CSIQPRCR  
**Source DDN:** CSIQSAMP **DSN:** USER456.R14MSM.CSIQSAMP  
**Target DSN:** &SYSUID..D&MSMDID.  
**Resolved as:** USER456.D???.CSIQSAMP  
**Source DDN:** CSIQSENU **DSN:** USER456.R14MSM.CSIQSENU  
**Target DSN:** &SYSUID..D&MSMDID.  
**Resolved as:** USER456.D???.CSIQSENU  
**Source DDN:** CSIQSRC **DSN:** USER456.R14MSM.CSIQSRC  
**Target DSN:** &SYSUID..D&MSMDID.  
**Resolved as:** USER456.D???.CSIQSRC  
**Source DDN:** CSIQTENU **DSN:** USER.PUBLIC.R14MSM.CSIQTENU  
**Target DSN:** &SYSUID..D&MSMDID.  
**Resolved as:** USER456.D???.CSIQTENU

**SMP/E Environment**  
 Transported to PRODSTAG: no  
 Endeavor R14 CSI has the TR16026 following APARs applied:

**Snapshot**  
**Path:** /u/users/msmserv/msmMP/sdsroot/D???  
**Container:** OMVSUSR.MSM.SDS.D???

**Save Back Next Deploy Cancel Help**

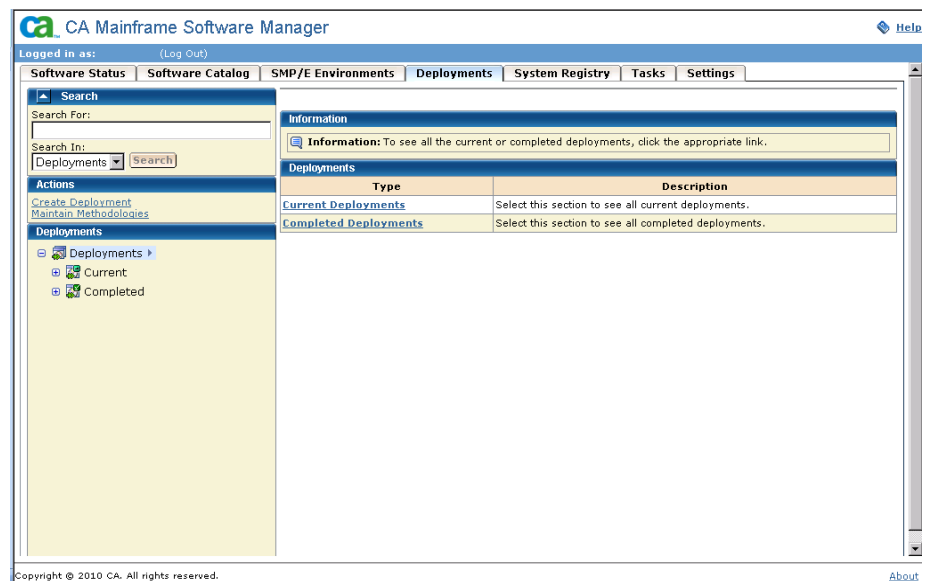


## View a Deployment

You can view a deployment by using the CA MSM.

### To view a deployment

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



## Maintain Deployments

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

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

### To maintain deployments

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

The detailed deployment information appears.

The screenshot shows a software management interface with several tabs: Software Status, Software Catalog, SMP/E Environments, Deployments, System Registry, Tasks, and Settings. The 'Deployments' tab is active. On the left, a search bar and a tree view under 'Deployments' are visible. The tree view shows 'Current' as the selected deployment. The right pane displays the 'Current' deployment details, including an information message and a table of current deployments.

Name	Description	Actions
<a href="#">Test Environment</a>	Authorized development tester only	<a href="#">Actions</a>
<a href="#">QA Environment</a>	Authorized Quality Assurance personnel	<a href="#">Actions</a>
<a href="#">Production_A</a>	Production Alpha System	<a href="#">Actions</a>
<a href="#">Production_B</a>	Production Beta System	<a href="#">Actions</a>

3. Click the Deployment Name link for the Deployment you want to maintain. This deployment's window appears

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

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

There are actions that you can perform based on Deployment State.

**Test Environment 768** Actions ▼

Deployments > Current > Test Environment 768

**Information**

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

**Deployment Details** Save

**Deployment Name\*:** Test Environment 768

**Description:** Only authorized developers and testers

**Current State:** Under Construction

**Methodology\*:**   Edit

**Deployment ID:** 634

**Product List** Add Products

Select and: [Remove](#) Show All ▼

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

**System List** Add Systems

Select and: [Remove](#) Show All ▼

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

Selected 0 of 3.

- To maintain a methodology, select a methodology from the drop down list. To edit the selected methodology click the edit button and the [Edit Methodology window](#) (see page 144) appears.

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

- You can select, [add](#) (see page 122), or [remove](#) (see page 123) a product.
- You can select, [add](#) (see page 147), or [remove](#) (see page 147) a system.
- You can select, [add](#) (see page 123), or [remove](#) (see page 132) a custom data set.
- Click Save on the Deployment Details window.

9. Click Actions button to do one of the following:

**Preview (Summary)**

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

Generates a list of the following current information:

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

**Snapshot**

Takes a snapshot of the current deployment.

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

**Transmit**

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

**Deploy**

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

**Confirm (see page 120)**

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

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

**Delete**

Deletes deployment and its associated containers, folders, and files. This does not including the deployed target libraries on the end systems. See delete a deployment for a list of deleted files.

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

**Reset Status**

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

10. Click Save on the Deployment Details window.

**More Information:**

[Edit a Methodology](#) (see page 144)

[Add a Product](#) (see page 122)

[Remove a Product](#) (see page 123)

[Add a System](#) (see page 147)

[Remove a System](#) (see page 147)

[Confirm a Deployment](#) (see page 120)

**How Investigate a Failed Deployment**

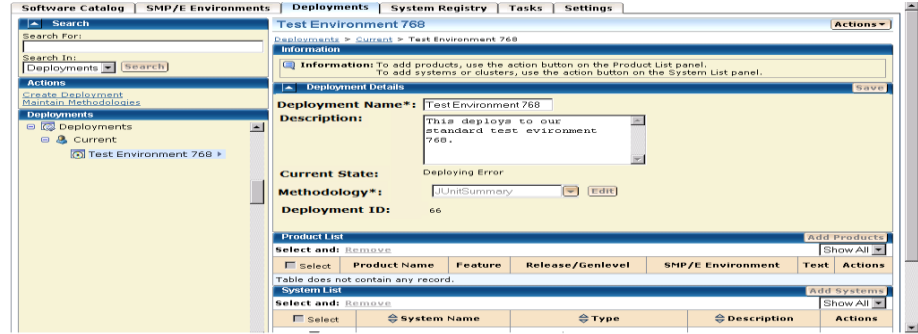
When a deployment fails it can be investigate, corrected, and deployed again. The following procedures are defined.

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

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

### To investigate a failed deployment using the Tasks page

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



2. Click the Tasks Tab and then click the Task History link. Click Refresh button on the right hand side of the Task History Bar to refresh the Task History display.
3. At the Show bar select All task, or My task to list the tasks by Owner.

**Note:** You can refine the task list by entering USER ID, types, and status, and then sort by Task ID.

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

Software Catalog   SMP/E Environments   Deployments   System Registry   Tasks   Settings							
Current Tasks   Task History							
Task History							
Current date and time is 1/26/2010 01:18:12PM							
Show: My tasks   All types   All status   Start time   Stop time							
Show All							
Owner	Name	Type	Status	Start Time	Stop Time	Task ID	
USER456	<a href="#">Deploy Test Environment 768</a>	Deployment	Failed	1/26/2010 12:58:09PM	1/26/2010 12:59:14PM	980	

4. The Task Manager window appears.

Deploy: Deployment Test

Close

General

Download Zipped Output

Name:Deploy: Deployment Test

Task ID:3172

User ID:USER456

Status:Failed

Status Message:Failed

Steps

Show All

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

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

The screenshot shows a window titled "Deployment Lock SIS" with a "Close" button. Below the title bar, there is a breadcrumb "Deploy Test Environment 768 > Deployment Lock SIS". The window has several tabs: "General", "MessageLog", "Explanation", and "Detailed Output". The "General" tab is active, showing "Name: Deployment Lock SIS" and "Status: Failed". There is a "Download zipped output" button. The "MessageLog" tab is also visible, showing a log entry: "SIS Lock command has started. Lock: true 1 CSI repository is being used. Gathering information for lock. Lock exists by USER null for resource Deployment Bernie1". The "Explanation" tab shows "Lock the appropriate SIS database records." The "Detailed Output" tab shows a table with columns "Name", "Lines", "Format", and "Action". The table has one row with "errorLog", "4", "U", and an "Action" button.

Name	Lines	Format	Action
<a href="#">errorLog</a>	4	U	<a href="#">Action</a>

### More Information:

[Download Message Log](#) (see page 90)

[Save a Message Log as a Data Set](#) (see page 91)

[To Show All](#) (see page 92)

## Delete a Deployment

You can delete deployments.

### To delete a deployment

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

## Delete a Completed Deployment

You can delete a completed deployment.

### To delete a completed deployment

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

A list of completed deployments appears.

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

The completed deployment is deleted.

## Confirm a Deployment

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

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

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



### To confirm a deployment

1. Click Confirm and Confirmation Dialog window appears.

Review the confirmation.

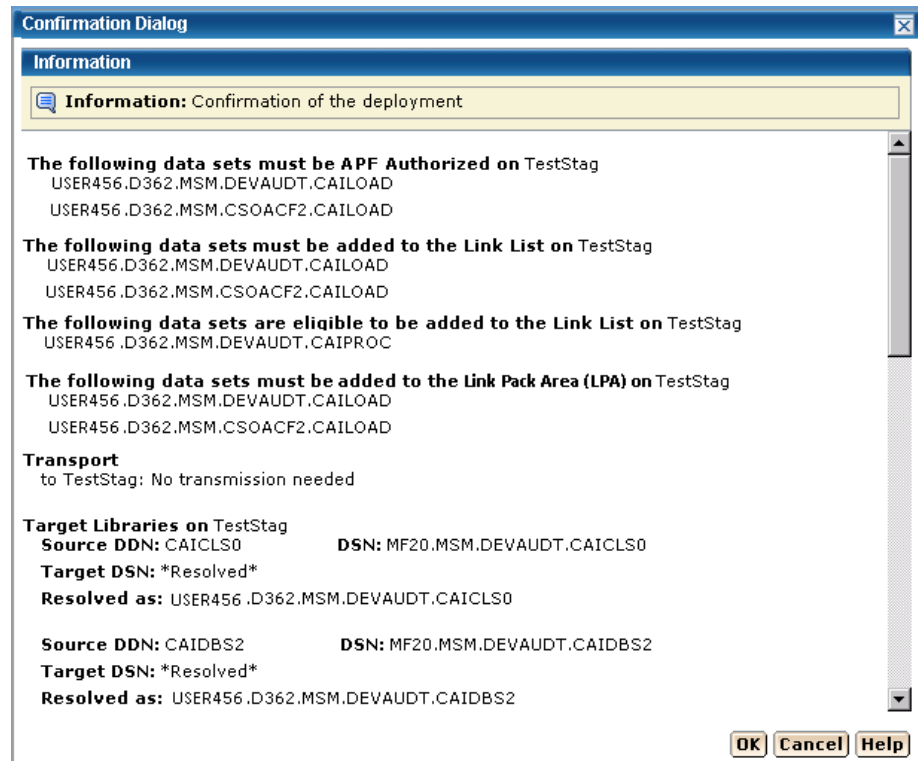
2. Click OK when the deployment is correct.

**Note:** Click Cancel to exit this procedure without confirming.

The Deployment Summary window contains none or any of the following:

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

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




## Products

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

### Add a Product

You can add a product to a deployment.

#### To add a product to a deployment

1. Click the Deployments tab. The Deployments window appears.
2. On the right, in the Deployments panel click the Current Deployment link.  
A list of current deployments appears.
3. Click the deployment name link.
4. In the Product List panel click Add Products.  
The Add Products wizard appears.
5. Select a CSI and click Next.  
The Product Selection appears.
6. Select a Product.
7. If there is a  text icon in Text column, click the text icon to read the instructions supplied by CA Support for product, data sets, and other necessary information.
8. Click the "I have read the associated text by selecting the text icon from the list about" box. This box appears only if there is a text icon.  
**Note:** You will not be able to click Next until you click this box.
9. Click Next.  
The Custom Data Set Selection appears
10. If needed, select or [add a custom data set](#) (see page 123).
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 123), [edit](#) (see page 128), and [remove](#) (see page 132) custom data sets from a deployment.

### Add a Custom Data Set

You can add custom data sets to a deployment.

#### To add custom data sets to deployment

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

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

The Add Custom Data Sets window appears.

**Add Custom Data Set**

Add a Custom data set by selecting the product, entering the Data Set Name, and the Mask.  
Note: The Instructions are required directions supplied by CA Support.

**Product\*:** CA Auditor for z/OS

**Instructions:**

**Data Set Type\*:** ☒ Data Set ☐ USS

**Data Set Name\*:**

**Mask\*:**

OK Cancel Help

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

5. Select a Product from the drop down list.

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

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

**Default:** data set

7. For data set enter the Data Set Name.

**Limits:** Maximum 44 characters.

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

8. Enter the Data Set Name Mask and/or click the file icon and select a [symbolic name](#) (see page 135).

**Mask**

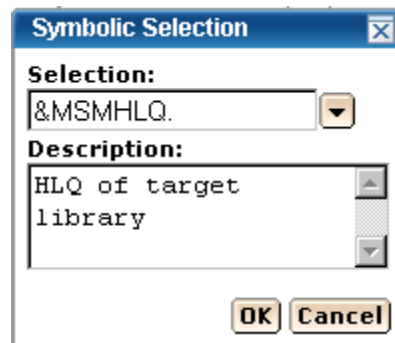
This is the mask that will be used to name the data sets that are being deployed. They can contain [symbolic qualifiers](#) (see page 135). For example, if you enter CAPRODS.&SYSID, the &SYSID is replaced by its values, and if the SYSID that is being deployed to is XX16, the dsn mask will be CAPRODS.XX16

**Limits:** Maximum 64 characters.

**Note:** Each deployed target data set will be named using the resolved content of the Data Set Name Mask followed by the low level qualifier of the source data set. Appending the low level qualifier from the source data set insures uniqueness of the final data set name.

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

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



9. Enter the Mask and click OK.

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

**Limit:** Maximum 255 characters.



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

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

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

11. Enter the Remote Path and/or click the file icon and select a [symbolic name](#) (see page 135). The remote path is the path were the files are to be copied to.

**Limit:** Maximum 255 characters.

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

**Note:** For file-by-file copy the user must make sure the USS path exists on all of the remote systems of this deployment. And has sufficient space to hold these target libraries.

**Default:** File-by-file Copy

13. Click OK.

14. For Container Copy enter the container name and/or click the file icon and select a [symbolic name](#) (see page 135).

**Limit:** Maximum 64 characters.

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

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

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

- c. All of the directories in the mount point will be dynamically created.
- d. The file system will be mounted at the requested mount point

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

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

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

15. Select the Type of Container from the drop down box. Either zFS or HFS.
16. Enter the Mount Point and/or click the file icon and select a [symbolic name](#) (see page 135).

**Limit:** Maximum 255 characters.

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

17. Enter the percentage of Free Space needed.

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

**Limit:** 0 to 1000.

18. Click OK.

The custom data set is added.

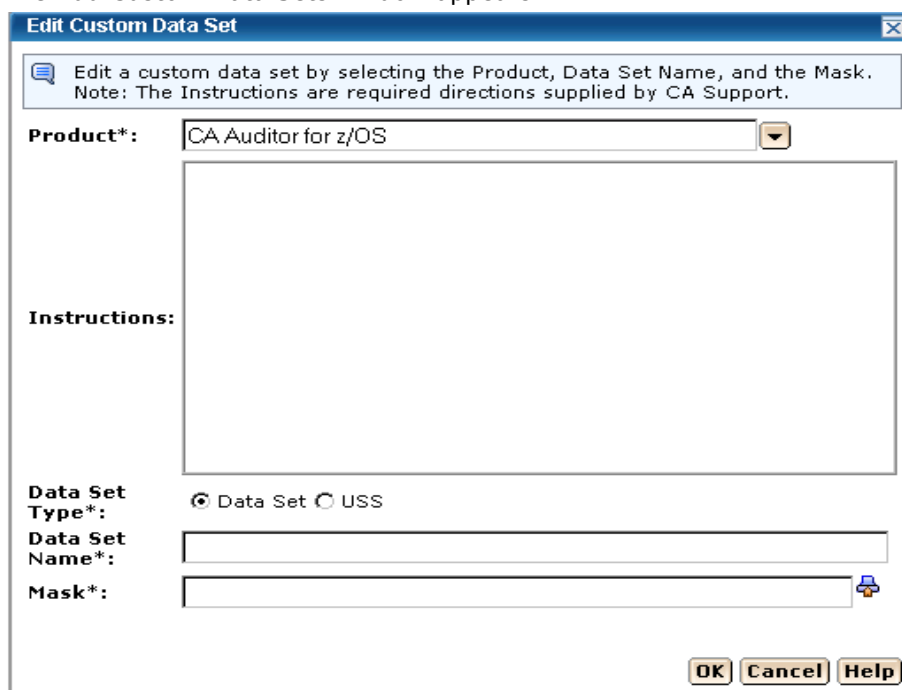
## Edit a Custom Data Set

You can edit a custom data set.

### To edit a custom data set

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

The Add Custom Data Sets window appears.



The screenshot shows a dialog box titled "Edit Custom Data Set". At the top, there is a message box with a speech bubble icon that says: "Edit a custom data set by selecting the Product, Data Set Name, and the Mask. Note: The Instructions are required directions supplied by CA Support." Below this, the "Product\*" field is a dropdown menu showing "CA Auditor for z/OS". The "Instructions:" field is a large, empty text area. The "Data Set Type\*" field has two radio buttons: "Data Set" (which is selected) and "USS". Below this are two text input fields: "Data Set Name\*" and "Mask\*", both of which are empty. At the bottom right of the dialog are three buttons: "OK", "Cancel", and "Help".

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

5. Select a Product from the drop down list.

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



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

**Default:** data set

7. For data set enter the Data Set Name.

**Limits:** Maximum 44 characters.

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

8. Enter the Data Set Name Mask and/or click the file icon and select a [symbolic name](#) (see page 135).

#### Mask

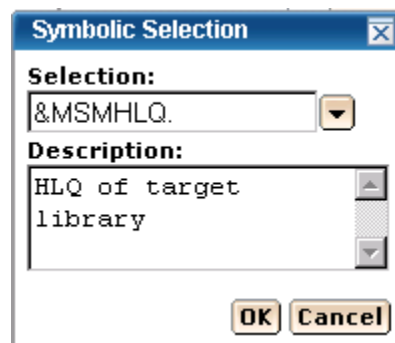
This is the mask that will be used to name the data sets that are being deployed. They can contain [symbolic qualifiers](#) (see page 135). For example, if you enter CAPRODS.&SYSID, the &SYSID is replaced by its values, and if the SYSID that is being deployed to is XX16, the dsn mask will be CAPRODS.XX16

**Limits:** Maximum 64 characters.

**Note:** Each deployed target data set will be named using the resolved content of the Data Set Name Mask followed by the low level qualifier of the source data set. Appending the low level qualifier from the source data set insures uniqueness of the final data set name.

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

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



9. Enter the Mask and click OK.

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

**Limit:** Maximum 255 characters.



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

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

Note: The asterisk indicates that the field is mandatory.

11. Enter the Remote Path and/or click the file icon and select a [symbolic name](#) (see page 135). The remote path is the path where the files are to be copied to.

**Limit:** Maximum 255 characters.

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

**Note:** For file-by-file copy the user must make sure the USS path exists on all of the remote systems of this deployment. And has sufficient space to hold these target libraries.

**Default:** File-by-file Copy

13. Click OK.

14. For Container Copy enter the container name and/or click the file icon and select a [symbolic name](#) (see page 135).

**Limit:** Maximum 64 characters.

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

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

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

- c. All of the directories in the mount point will be dynamically created.
- d. The file system will be mounted at the requested mount point

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

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

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

15. Select the Type of Container from the drop down box. Either zFS or HFS.
16. Enter the Mount Point and/or click the file icon and select a [symbolic name](#) (see page 135).

**Limit:** Maximum 255 characters.

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

17. Enter the percentage of Free Space needed.

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

**Limit:** 0 to 1000.

18. Click OK.

The custom data set is added.

## Remove a Custom Data Set

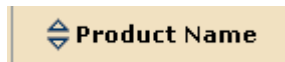
You can remove a custom data set from a deployment.

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

### To remove a custom data set

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

### Product Name Sort Arrows



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

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

## Methodologies

You can [create](#) (see page 132), maintain, [edit](#) (see page 144), and [delete](#) (see page 146) methodologies from a deployment.

### Create a Methodology

You can create a methodology.

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

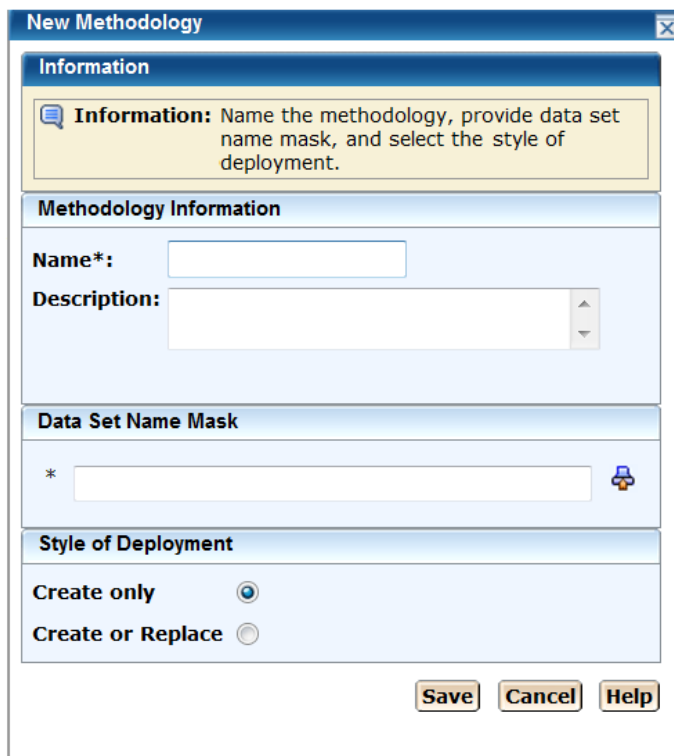
### To create a methodology

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

2. Enter the methodology name.

**Limits:** Maximum 64 characters.

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



The image shows a 'New Methodology' dialog box with a blue title bar and a close button. It contains several sections: 'Information' with a message box, 'Methodology Information' with 'Name\*' and 'Description' fields, 'Data Set Name Mask' with a field and a printer icon, and 'Style of Deployment' with two radio buttons. At the bottom are 'Save', 'Cancel', and 'Help' buttons.

**New Methodology**

**Information**


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

**Methodology Information**

**Name\*:**

**Description:**

**Data Set Name Mask**

\*  

**Style of Deployment**

**Create only** ☒

**Create or Replace** ☐

**Save** **Cancel** **Help**

3. Enter the description of this methodology.

**Limits:** Maximum 255 characters.

4. Enter the data mask name and/or click the file icon and select a [symbolic name](#) (see page 135).

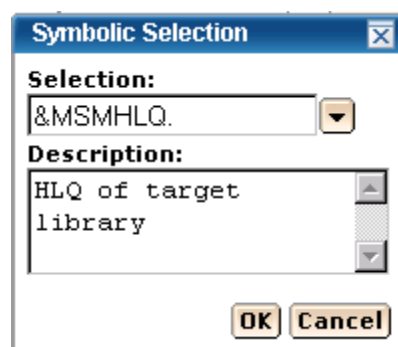
#### Data Set Name Mask

This is the mask that will be used to name the data sets that are deployed. They can contain [symbolic qualifiers](#) (see page 135). For example, assume you enter, CAPRODS.&SYSID. In this case, the &SYSID will be replaced by its values. If the SYSID that is being deployed to is X16, the dsn mask will be: CAPRODS.X16

**Limits:** Maximum 64 characters.

**Note:** Each deployed target data set will be named using the resolved content of the Data Set Name Mask followed by the low-level qualifier of the source data set. Appending the low-level qualifier from the source data set help ensures uniqueness of the final data set name.

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



5. Select a style of Deployment.

#### Create only

Creates new data sets.

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

#### Replace or Create

Creates new data sets and replaces an existing one with the same name.

**Note:** Prior to creating any data sets on the remote system, a check is made, to see if the data sets already exist. If they do exist, the contents are replaced. If they do not exist, new data sets are created.

6. Click Save.

**Note:** Click Cancel to exit this procedure without saving.

## Symbolic Qualifiers

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

### Data Set Name Mask

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

### Directory Path

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

### Symbolic Substitution

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

### Symbolic Variables

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

**Example:** Assume MSMDID is 255.

SYSWORK.D&MSMDID..DATASET

**Note:** The double dots are important, since the first dot is part of the symbolic name, it will not appear in the translated value.

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

### Numeric Values

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

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

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

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

An incorrect specification of the mask would be:

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

### Directory Paths

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

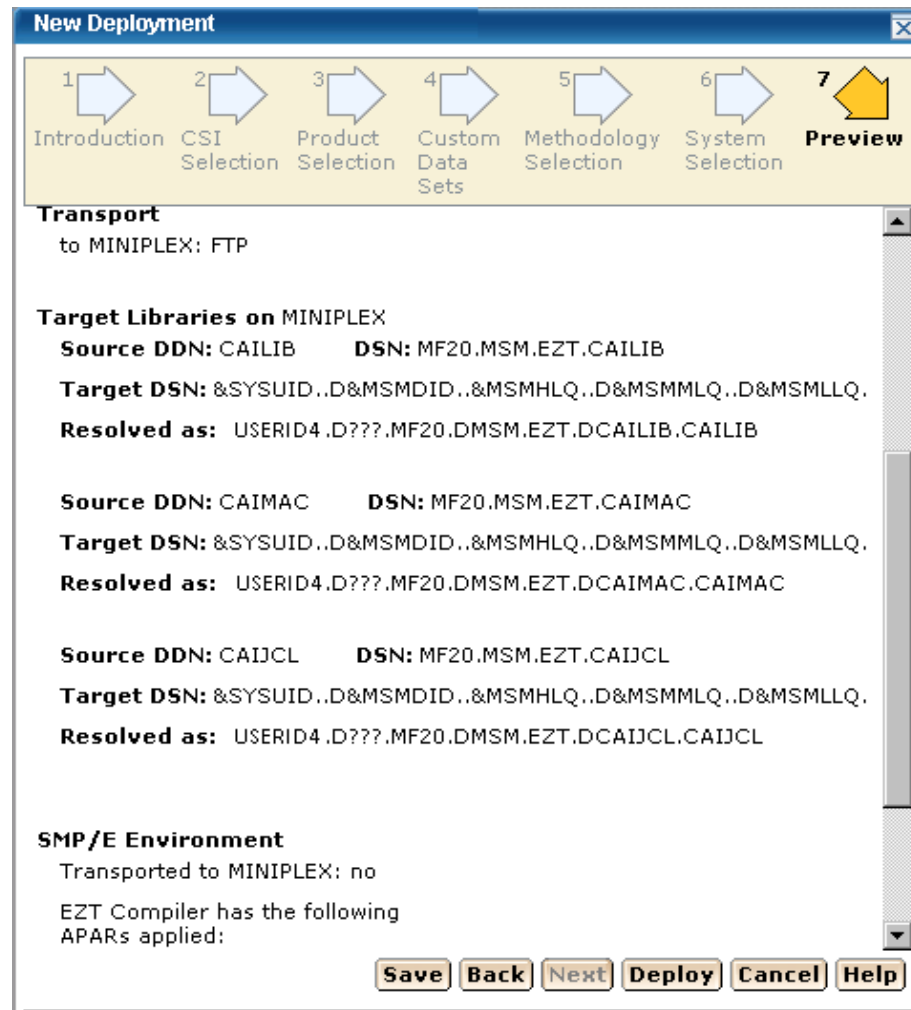
**Example:** Assume the target system is SYSZ.

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



## Preview Example

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



## Symbolic Qualifiers

### ID and System Information

#### MSMDID

This is the MSM Deployment ID.

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

### **MSMMPN**

This is the MSM Mount Point Name. The value is entered into the mount point name field when [adding a custom data set](#) (see page 123) with both the USS radio button and the Container copy radio button set. It is of primary value in remote path.

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

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

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

Remote path: &MSMMPN.

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

### **MSMSYSNM**

This is the MSM system object name.

### **SYSCLONE**

This is the shorthand name of the system.

**Limits:** Maximum 2 characters.

### **SYSNAME**

This is the system name entered when a Non-Sysplex System, Sysplex, Shared DASD Cluster, or Staging System is created.

### **SYSPLEX**

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

**Note:** This symbolic may not be used for a Non-SYSPLEX system.

### **SYSUID**

The current user ID.

## **Target Libraries**

### **MSMHLQ**

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

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

**Example:** For the data set johnson.finance.division.script, the high-level qualifier is johnson.

**MSMMLQ**

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

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

**Example:** For the data set johnson.finance.division.script, the middle-level qualifier is finance.division.

**MSMLLQ**

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

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

**Example:** For the data set johnson.finance.script, the low-level qualifier is script.

**MSMSLQ**

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

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

**Example:** For the data set johnson.finance.second.script, the low-level qualifier is second.

**MSMPREF**

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

**Example:** For the data set johnson.finance.division.script the prefix is johnson.finance.division

### **MSMDLIBN**

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

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

DSN = USER456.LIBR473.CAIPROC

DSN = USER456.LIBR473.CAILOAD

DSN = USER456.LIBR473.CAIEEXEC

Assume the methodology specified a mask of:

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

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

Deployed library = USER789.D877.LIB1.CAIPROC

Deployed library = USER789.D877.LIB2.CAILOAD

Deployed library = USER789.D877.LIB3.CAIEEXEC

### **Local Date and Time**

#### **LYYMMDD**

This is the local two-digit year.

**YY** two-digit year

**MM** two-digit month (01=January)

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

**Example:** 100311

#### **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

## Edit a Methodology

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

### To edit a methodology

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

The Maintain Methodologies select window appears.

**Edit Methodology**

**Information**

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

**Methodology Information**

**Name\*:** USER456

**Description:** MSMETHODOLOGY

**Data Set Name Mask**

\* &MSMHLQ.

**Style of Deployment**

**Create only** ☒

**Create or Replace** ☐

**Save** **Cancel** **Help**

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

As with Add a Methodology, all fields are available to be edited and the details for each field are listed.

3. Enter the Methodology Name.

**Limits:** Maximum 64 characters.

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

4. Enter the Description of this Methodology.

**Limits:** Maximum 255 characters.



5. Enter the Data Set Name Mask and/or click the file icon and select a [symbolic name](#) (see page 135).

#### Data Set Name Mask

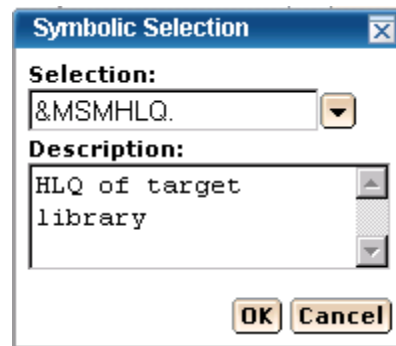
This is the mask that will be used to name the data sets that are deployed. They can contain [symbolic qualifiers](#) (see page 135).

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

**Limits:** Maximum 64 characters.

**Note:** Each deployed target data set will be named using the resolved content of the Data Set Name Mask followed by the low level qualifier of the source data set. Appending the low level qualifier from the source data set insures uniqueness of the final data set name.

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



6. Select a Style of Deployment.

#### Create only

Creates new data sets.

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

#### Replace or Create

Creates new data sets and replaces an existing one with the same name.

**Note:** Prior to creating any data sets on the remote system, a check is made, to see if the data sets already exist. If they do exist, the contents are replaced. If they do not exist, new data sets are created.

7. Click Save.

**Note:** Click Cancel to exit without saving your changes.

**More Information:**

[Symbolic Qualifiers](#) (see page 135)

**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.

**Search**

Search For:

Search In:

Deployments Search

**Actions**

[Create New Deployment](#)

[Maintain Methodologies](#)

**Maintain Methodologies**

**Information:** You can create, edit or delete methodologies.

**Methodologies**

Select and: [Delete](#) Show All

Select	Name	Description	DSN Mask	Actions
<input checked="" type="checkbox"/>	Method1	Method1	&SYSUID.	Action
<input type="checkbox"/>	Method2	Method2	&SYSUID..D&MSMDID..&MSMSLQ	Action
<input type="checkbox"/>	Another1	Method3	&SYSUID..D&MSMDID.	Action
<input type="checkbox"/>	myMeth	Test Method	&SYSUID..D&MSMDID..&SYSNAME.	Action

Save Cancel Help

2. Select the methodology that you want to delete.

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

3. Click Delete and then OK to the Delete Methodologies confirmation window.  
The methodology is deleted.

**Systems**

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

## Add a System

You can add a system to a deployment.

### To add a system

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

3. Click the deployment name link.
4. In the System List panel, click Add Systems.  
The Add Systems window appears.

5. Select a system to add.

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

**Note:** Sysplex systems are denoted by Sysplex System:System Name. For example PLEX1:CO11 where PLEX1 is Sysplex name and CO11 is the system name.

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

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

## Remove a System

You can remove a system from a deployment.

### To remove a system

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

3. Select the deployment that you wish to remove the product from.

#### System Name Sort Arrows



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

#### Type Sort Arrows



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

#### Description Sort Arrows



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

4. In the System List panel, select a system you want to remove.
5. Click Remove and then OK to the Remove Products confirmation window.  
The system is removed.

## Deployment Summary

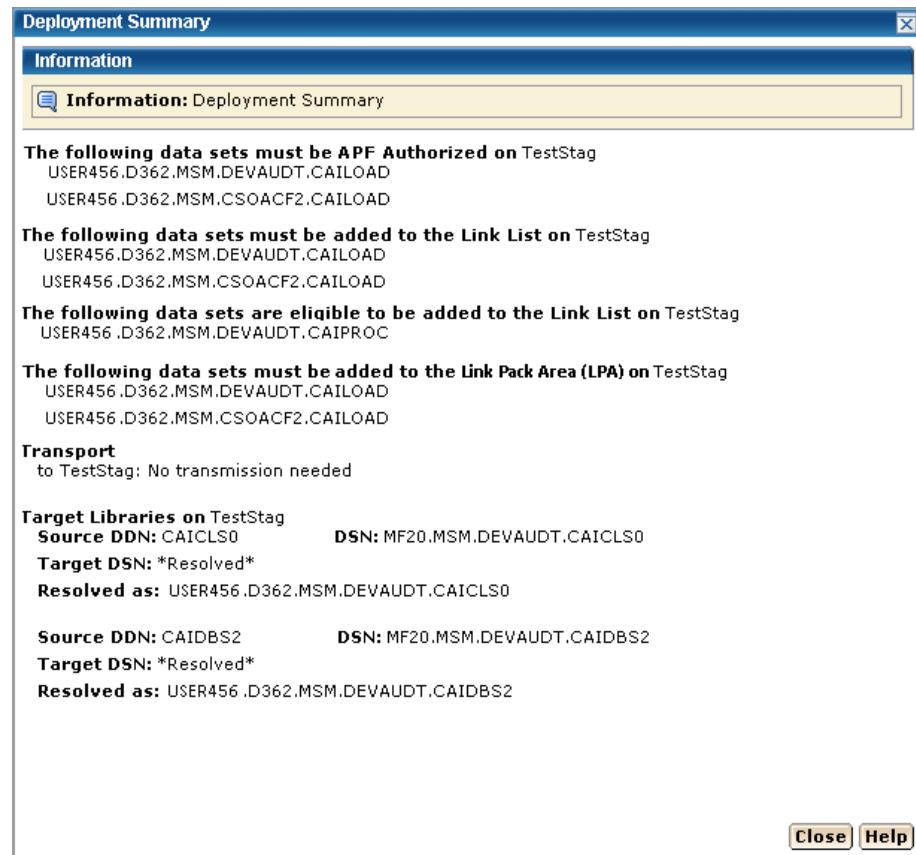
This Action button is available after a successful deployment.

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

The Deployment Summary window contains none or any of the following:

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

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



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



# Chapter 4: Installing Your Product From Pax-Enhanced ESD

---

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

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

This section contains the following topics:

[How to Install a Product Using Pax-Enhanced ESD](#) (see page 151)

[Allocate and Mount a File System](#) (see page 157)

[Copy the Product Pax Files into Your USS Directory](#) (see page 158)

[Create a Product Directory from the Pax File](#) (see page 163)

[Copy Installation Files to z/OS Data Sets](#) (see page 164)

[Unload the Install Utility](#) (see page 165)

[Installation JCL](#) (see page 166)

[Clean Up the USS Directory](#) (see page 169)

[Maintenance](#) (see page 170)

## How to Install a Product Using Pax-Enhanced ESD

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

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

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

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

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

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

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

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

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

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

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

**More Information:**

[USS Environment Setup](#) (see page 156)

[Allocate and Mount a File System](#) (see page 157)

[Copy the Product Pax Files into Your USS Directory](#) (see page 158)

[Create a Product Directory from the Pax File](#) (see page 163)

[Copy Installation Files to z/OS Data Sets](#) (see page 164)



## How the Pax-Enhanced ESD Download Works

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

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

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

The CA Support Online web page appears.

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

The CA Product Download window appears.

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

For both options, [The ESD Product Download Window](#) (see page 153) topic explains how the download interface works.

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

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

The product is installed on the mainframe.

## ESD Product Download Window

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

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

**CA Earl - MVS**

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

If you have comments or suggestions about CA product documentation, send a message to [techpubs@ca.com](mailto:techpubs@ca.com).

[View Download Cart](#)

☐ Add All to cart

Product Components				Add to cart	Download
<b>CA COMMON SERVICES PROD PKG</b> 11SP08AW000.pax.Z	11.0 /SP08	03/31/2010	407MB	<input type="checkbox"/>	<a href="#">Download</a>
<b>CA EARL PRODUCT PACKAGE</b> 610106AEO00.pax.Z	6.1 /0106	03/31/2010	1MB	<input type="checkbox"/>	<a href="#">Download</a>
<b>EARL PIPPACK</b> AEO61010600.pdf	6.1 /0106	03/31/2010	93KB	<input type="checkbox"/>	<a href="#">Download</a>
<b>EARL INSTALL GUIDE MANUAL</b> I2J2ED610NE.pdf	6.1 /0000	03/31/2010	361KB	<input type="checkbox"/>	<a href="#">Download</a>
<b>CA COMMON SERVICES COVER LTR</b> QI92742.pdf	11.0 /SP08	03/31/2010	46KB	<input type="checkbox"/>	<a href="#">Download</a>

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

### Download Method

---

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

---

#### HTTP via Download Manager


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

[Download](#)

---

#### HTTP via Internet Browser

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

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

---

#### FTP

This method allows you to download your file(s) via FTP from CA's content delivery network or via native FTP servers.

**Note:** Processing is required and an email notification will be sent when your request is ready for downloading.

[FTP Request](#)

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

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

### Download Method

---

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

---

#### HTTP via Download Manager

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

[Download](#)

---

#### Create a Zip File

This method allows you to bundle your download files into one or more zip files of up to 3.5 GB each. These zip files can then be downloaded via HTTP or FTP.

**Note:** Processing is required and an email notification will be sent when your request is ready for downloading.

[Create Zip](#)

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

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

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

### Review Download Requests

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

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

#### Today's Downloads

Order #	Status	Description	Date Placed	Download Options
<a href="#">10000961</a>	Ready	FTP Download Request	04/30/2010	<a href="#">Preferred FTP</a> ▼   <a href="#">Alternate FTP</a> ▼

#### Previous 6 day Download History

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

## USS Environment Setup

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

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

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

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

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

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

## Allocate and Mount a File System

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

This procedure details how to perform the following tasks:

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

**Important!** USS commands are case-sensitive.

### To allocate and mount the file system

1. Allocate the HFS. For example:

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

The HFS is allocated.

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

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

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

The mount point is created.

3. Mount the file system. For example, from TSO, enter the following command:

```
MOUNT      FILESYSTEM('yourHFS dataset name')  
           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 product installation procedure, copy the product's pax file into the USS directory you set up. Use one of the following methods:

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

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

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

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

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

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

**More Information:**

[How the Pax-Enhanced ESD Download Works](#) (see page 153)  
[ESD Product Download Window](#) (see page 153)

## Download Using Batch JCL

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

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

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

**To download files using batch JCL**

1. Supply a valid JOB statement.
2. Replace *yourTCPIP.PROFILE.dataset* with the name of the TCPIP profile data set for your system. Consult your local network administrators, if necessary.  
The job points to your profile.
3. Replace *YourEmailAddress* with your email address.  
The job points to your email address.

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

The job points to your USS directory.

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

You have identified the product component to download.

6. Click Download for the applicable file.

**Note:** You may also add files to a cart for multiple downloads.

The Download Method window opens.

7. Click FTP Request.

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

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

8. Select one of the following methods:

#### **Preferred FTP**

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

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

#### **Alternate FTP**

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

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

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

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

9. Submit the job.

**Important!** If your FTP commands are incorrect, this job may fail and still return a zero condition code. You must read the messages in the job DDNAME SYSPRINT to verify the FTP succeeded.

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



**Example: CAtoMainframe.txt, JCL**

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

```
//GETPAX JOB (ACCOUNTNO),'FTP GET ESD PACKAGE',
// MSGCLASS=X,CLASS=A,NOTIFY=&SYSUID
//*****
/* This sample job can be used to download a pax file directly from *
/* CA Support Online to a USS directory on your z/OS system. *
/* *
/* This job must be customized as follows: *
/* 1. Supply a valid JOB statement. *
/* 2. Replace "yourTCPIP.PROFILE.dataset" with the name if the TCPIP *
/* profile data set for your system. *
/* 3. Replace "Host" based on the type of download method. *
/* 4. Replace "YourEmailAddress" with your email address. *
/* 5. Replace "yourUSSESDdirectory" with the name of the USS *
/* directory used on your system for ESD downloads. *
/* 6. Replace "FTP Location" with the complete path *
/* and name of the pax file obtained from the FTP location *
/* of the product download page. *
//*****
//GETPAX EXEC PGM=FTP,REGION=0K
//SYSTCPD DD DSN=yourTCPIP.PROFILE.dataset,DISP=SHR
//SYSPRINT DD SYSOUT=*
//OUTPUT DD SYSOUT=*
//INPUT DD *
Host
anonymous YourEmailAddress
lcd yourUSSESDdirectory
binary
get FTP location
quit
```

## Download Files to Mainframe through a PC

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

### To upload files to the mainframe through a PC

1. Follow the procedures in [How to Download Files Using ESD](#) (see page 153) to download the product pax or zip file to your PC. If you download a zip file, first unzip the file to use the product pax files.

The pax or zip file resides on your PC.

2. Open a Windows command prompt.

The command prompt appears.

3. Customize and enter the FTP commands with the following changes:

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

The pax file is transferred to the mainframe.

### Example: FTP Commands

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

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

## Create a Product Directory from the Pax File

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

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

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

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

The job points to your specific directory.

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

The job points to your specific pax file.

4. Submit the job.

The job runs and creates the product directory.

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

## Example Job to Execute the Pax Command (Unpackage.txt)

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

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

## Copy Installation Files to z/OS Data Sets

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

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

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

You have identified product-specific installation details.

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

The job is edited.

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

Your view is of the product-specific directory.

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

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

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

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

6. Submit the UNZIPJCL job.

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

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

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

## Unload the Install Utility

The installation utility software lets you generate and run the JCL required to install your product. The installation utility software is delivered electronically with ESD.

The installation software unloads into the *dsnpref.CAI.NMC0.CAIJCL* data set; *dsnpref* is a prefix you specify for your product data sets.

After you unzip the data sets, do *one* of the following:

- Rename *dsnpref.CAI.NMC0.CAIJCL* to *dsnpref.NMC0.CAIJCL*
- Copy the members in *dsnpref.CAI.NMC0.CAIJCL* into *dsnpref.NMC0.CAIJCL*

## Additional Features

The Install Utility provides an option to install the following additional features:

- SSL support
- ReportCenter
- WebCenter SDK

You should install, set up, and customize your product region completely before installing ReportCenter or WebCenter SDK.

**Note:** For information about installing these features, see the *ReportCenter Guide* and the *WebCenter SDK Developer Guide*.

## Installation JCL

The installation process creates the *dsnpref.NMC0.INSTDB* database to store details of each installation that you perform. If you are also installing other products in the Mainframe Network Management family of products, this database manages those installations. These details include the products you install and the installation values that you specify.

**Note:** During this task, the INSTALLATION JCL Library Creation panel lets you specify your installation JCL library. The default library name is *dsnpref.NMC0.INSTALL.JCL*, where *dsnpref* is the same data set prefix you used for the *dsnpref.NMC0.CAIJCL* data set.

If your installation JCL library exists, do *one* of the following:

- Specify a new data set name at that panel.
- Delete the existing library by issuing a TSO DELETE command.

**Note:** If you leave the Install Utility at any stage, you can return to it from the ISPF/PDF TSO Command Shell prompt. Execute the following command:

```
EXEC 'dsnpref.NMC0.CAIJCL(INSTALL)'
```

## Generate the Installation JCL

During the installation process, you provide the [site-specific installation information that you previously collected](#) (see page 24). This information is used to generate the installation JCL.

### To generate the installation JCL

1. At the ISPF/PDF TSO Command Shell prompt, execute the following command:

```
EXEC 'dsnpref.NMC0.CAIJCL(INSTALL)'
```

The Install Utility panel appears.

**Note:** On each of the Install Utility panels, you can use the following keys:

- Enter to proceed to the next panel
- F1 to display help
- F3 to return to the previous panel
- F4 to exit and return to the main menu

2. Press Enter.

The Install Utility Primary Menu panel appears.

3. Enter **1** (Set Installation Parameters).

The Software Delivery Method panel appears.

4. Complete each of the panels as they open. Press Enter at the completion of each panel. You must complete all five parameter panels before you can install the product. You can take the default options or specify site-specific values. For information about the fields, press F1 (Help).

5. Enter **2** (Install Products).

The INSTALLATION Primary Menu panel appears.

6. Enter **1** (Select Products to Install).

The INSTALLATION Product Selection panel appears with previously installed products unavailable.

7. Enter **S** next to the product name and press Enter.

The INSTALLATION Product Confirmation panel appears, confirming your selections.

If you have already installed another product in the product family, the INSTALLATION Components Already Installed panel appears, confirming your selections.

**Note:** You can enter S next to multiple products to install multiple products at one time. You must be licensed for any products you install.

8. Press Enter to confirm your selection and complete each of the INSTALLATION panels as they open. You must complete all the panels before you can set up your regions. You can take the default options or specify site-specific values. For information about the fields, press F1 (Help).
9. Record the data set name into which the JCL was generated in your [post-installation worksheet](#) (see page 37). Jobs can be submitted from the panel or directly from this data set after exiting the panel.
10. Submit and run the following installation jobs in sequence. Do not proceed with any job until the previous job has completed successfully. Each job should complete with return code 0 unless otherwise indicated.

**I01ALLOC**

Allocates the data sets.

The I01ALLOC member allocates CC2DLOAD as a load library of the PDS type. Do not change it to a PDS/E type because the type is not supported.

**I02INSMP**

Initializes the SMP/E data sets.

**I03RCSMP**

Performs an SMP/E RECEIVE.

**I04AKSMP**

Performs an SMP/E APPLY CHECK. This job is listed only if maintenance exists for previously installed products.

**I05RSSMP**

Performs an SMP/E RESTORE. This job is listed only if maintenance exists for previously installed products.

**I06APSMP**

Performs an SMP/E APPLY.

**I07ACSM**

Performs an SMP/E ACCEPT.



11. If you selected SSL Support as an additional feature to install, the following jobs are also generated. Submit and run them in sequence as for the previous jobs.

- I21ALLME
- I22INIME
- I23RECME
- I26APPME
- I27ACCME

**Notes:**

- If you installed and set up your regions without SSL support, and then later install SSL support, you must add the installed *dsnpref.NMC0.CC2DPLD* data set to the region's STEPLIB or in the system linklist.
- You must have SMP/E V3R5.0 to implement SSL.

12. Press F3.

You are returned to the Primary Menu panel.

## Clean Up the USS Directory

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

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

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

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

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

### To delete the pax files and product-specific directories

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

Your view is of the applicable USS directory.

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

```
rm paxfile
```

#### ***paxfile***

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

The pax file is deleted.

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

```
rm -r product-specific-directory
```

#### ***product-specific-directory***

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

The product-specific directory is deleted.

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

## Maintenance

Maintenance includes program temporary fixes (PTFs) that supersede all authorized program analysis reports (APARs) that were created up to that time. Details of the superseded APARs are available as comments within the PTFs.

### Product Maintenance

**Important!** The *dsnpref.NMC0.CAILINK* data set must be in your system linklist before you start maintenance. You can also create a STEPLIB to the data set name (DSN) in your TSOPROC (that is, allocate it to ISPLLIB). If you installed the product using CA MSM, you must use CA MSM to apply maintenance.

Product maintenance is provided as system modification program (SMP) fixes. The fixes consist of PTFs applied using the IBM System Modification Program Extended (SMP/E) tool.

**Note:** If an installed SMP fix contains maintenance for the VSAM data sets, you must update those data sets for each region you have set up.

RAMDB maintenance is provided as SMP/E PTFs. However, this is only the delivery and recordkeeping methodology. You must apply the maintenance using \$RMDB04D.

## Apply Maintenance

This section describes how to apply individual SMP fixes using the Install Utility.

**Note:** Individual SMP fixes are only available from the [CA Technical Support site](#) (see page iv).

When you receive SMP fixes, unload them into one of the following:

- A sequential data set
- A member of a partitioned data set

Multiple SMP fixes can be appended into a single data set or member.

### To apply SMP fixes

1. Access the ISPF/PDF Primary Menu.
2. Select the COMMAND option.  
The ISPF Command Shell panel appears.
3. At the command prompt, enter the following command:  
`EXEC 'dsnpref.NMC0.CAIJCL(INSTALL)'`
4. At the Install Utility title panel, press Enter.  
The Install Utility Primary Menu panel appears.
5. At the Install Utility Primary Menu panel, enter **8** (Maintain Products).  
The MAINTENANCE Primary Menu panel appears.
6. Enter **3** (Apply individual SMP fixes from a DASD data set).  
The MAINTENANCE DASD Fixes Dataset Name panel appears.
7. Enter the data set name that contains the SMP fixes to be applied and press Enter.
8. Complete the fields on the following MAINTENANCE panels as they open.

9. At the MAINTENANCE JCL Library Creation panel, review your fix JCL library. The default library name is:

*dsnpref.NMC0.FIX.DASD.JCL*

***dsnpref***

The same data set prefix you used for the *dsnpref.NMC0.CAIJCL* data set.

**Note:** Each time you apply maintenance, use a new output data set. A new data set ensures that the only jobs in your maintenance JCL library are the jobs required for the maintenance you are installing now. To use a new data set:

- Delete the library by issuing a TSO DELETE command and the library name, at the command prompt.
- Specify a new data set name.

10. Press Enter to proceed with the generation of the maintenance JCL.

When the JCL generation is complete, a list of generated jobs and a description of what each member does appears.

11. Note the name of the data set into which the JCL was generated.

12. Submit and run the following jobs in sequence. Do not proceed with any job until the previous job has completed successfully. Each job should complete with return code 0 unless otherwise indicated.

**Important!** If there is maintenance for additional features, the SMP/E apply job must be run on a system that has the z/OS UNIX file system used during installation and mounted for read/write access.

**F11RCSMP**

SMP/E receives maintenance and lists existing HOLDDATA and SOURCEIDs that are already applied. If a job step returns condition code 04, there is no HOLDDATA present.

Review the information. For any held APARs that you want to apply, add the correct BYPASS HOLDx operands to the corresponding APPLY control statement for those APARs. Add the operands by manually editing the F12APSMP job that contains the SMP control statements.

**Note:** For information about the BYPASS HOLDx operands, see IBM's *SMP/E Commands* guide.

**F12APSMP**

SMP/E applies maintenance.

13. Press F3.

The Install Utility Primary Menu panel appears.

14. If the installed SMP fix contains maintenance for the VSAM data sets, select maintenance option **V** (Update MODS, PANELS and OSCNTL data sets with installed maintenance).

The VSAM data sets for the regions you set up are updated.

15. Press F4 to exit the Install Utility Primary Menu panel and return to the ISPF Command Shell panel, or continue with the other options.

## HOLDDATA

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

### System HOLDDATA

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

#### **ACTION**

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

#### **DEP**

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

#### **DELETE**

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

#### **DOC**

Indicates a documentation change with this SYSMOD.

#### **EC**

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

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

### **External HOLDDATA**

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

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

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

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

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

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

## **Update VSAM Data Sets**

If an installed SMP fix contains maintenance for the VSAM data sets, maintenance option V of the Install Utility becomes available. To complete maintenance, select the option to update the data sets for the regions you have set up.

**To update the VSAM data sets**

1. Access the ISPF/PDF Primary Menu, and select the COMMAND option.  
The ISPF Command Shell panel appears.
2. At the command prompt, execute the following command:  

```
EXEC 'dsnpref.NMC0.CAIJCL(INSTALL)'
```

  
The Install Utility title panel appears.
3. Press Enter.  
The Install Utility Primary Menu panel appears.
4. Enter **8** (Maintain Products).  
The MAINTENANCE Primary Menu panel appears.
5. Enter **V** (Update MODS, PANELS, OSCNTL and NETINFO data sets with installed maintenance).  
The MAINTENANCE Shared Region Data Sets panel appears.
6. Review the information, and press Enter.
7. At the MAINTENANCE JOBCARD Information panel, specify your JOBCARD details and press Enter.
8. At the MAINTENANCE JCL Library Creation panel, review your fix JCL library.  
The default library name is:  

```
dsnpref.NMC0.FIX.VSAMUPD.JCL
```

  
**dsnpref**  
The same data set prefix used for the *dsnpref.NMC0.CAIJCL* data set.  
**Note:** Each time you apply maintenance, use a new output data set. The new data set ensures that the only jobs in your maintenance JCL library are the jobs required for the maintenance you are installing. To use a new data set:
  - Delete the library by issuing a TSO DELETE command and the library name, at the command prompt.
  - Specify a new data set name.
9. Press Enter to proceed with the generation of the maintenance JCL.
10. Submit and run the job F21RFRSH to update the VSAM data sets.
11. Press F3.  
The Install Utility Primary Menu panel appears.
12. Press F4 to exit the Install Utility Primary Menu panel and return to the ISPF Command Shell panel, or continue with the other options.

## Individual RAMDB Maintenance

**Note:** Individual RAMDB maintenance is also available from the [CA Technical Support site](#) (see page iv).

This section describes how to apply maintenance to the RAMDB and details the command syntax of the \$RMDB04D maintenance utility.

**Important!** The RAMDB data set must not be updated with individual replacement records using the IDCAMS REPRO command.

When applying maintenance, you can [display details of what differences are being added, replaced, or deleted by the maintenance](#) (see page 178).

### Create Backup RAMDB

As a safety precaution, you must create a backup of your RAMDB (herein referred to RAMDBd) before applying maintenance.

#### To create the RAMDBd

1. Allocate RAMDBd in the same way that RAMDB was allocated. The cluster definition is in *dsnpref.NMC0.rname.JCL(S01LCALC)*.
2. Stop the product region.
3. Copy the data from RAMDB to RAMDBd using IDCAMS REPRO command. See the example in *dsnpref.NMC0.rname.JCL(S04LDVSM)*.
4. Restart the product region.



## Apply Maintenance to RAMDB

You can apply maintenance directly to your RAMDB. The maintenance can then propagate to all connected regions, if any. If necessary, you can restore the maintenance using your RAMDBd as input (provided that the maintenance has not yet been applied to RAMDBd).

### To apply maintenance directly to RAMDB

1. Log on to your product region and enter CMD.

The command entry panel appears.

2. Apply-check the RAMDB fix by entering the following command:

```
$RAMDB04D OPT=APPLY FIX=fix-name CHECK=YES
```

#### ***fix\_name***

Is RAM@UPDT for published solutions or TZdddd for test fixes.

When the APPLY CHECK finishes, a report appears that shows whether an APPLY of the fix will be successful, and also exactly what changes will result from the APPLY.

**Note:** Perform this step for the following reasons:

- To see what will happen if a fix is applied to a RAMDB
- To see whether a fix has been applied to a RAMDB

3. Apply the RAMDB fix by entering the following command:

```
$RAMDB04D OPT=APPLY FIX=fix_name
```

**Note:** If a RAMDB fix does not apply correctly or if you want to restore a fix, [restore the RAMDB maintenance](#) (see page 178).

## Restore RAMDB Maintenance

**Note:** This step is optional.

The RESTORE option can be used to remove an applied fix from the RAMDB by using RAMDBd as input. The fix is effectively reversed, that is, any added objects are deleted and any deleted or replaced objects are copied from RAMDBd back to the RAMDB.

To restore the fix, enter the following command:

```
$RMDB04D OPT=RESTORE FIX=fix_name DDBDSN=?RAMDBd-dataset-name DDB=?RAMDBd  
?RAMDBd
```

Specifies the ddname for the backup RAMDB.

**?*RAMDBd-dataset-name***

Specifies the full data set name of the backup RAMDB.

## RAMDB Maintenance Utility Syntax

This section contains descriptions of the RAMDB Maintenance Utility syntax.

### **\$RMDB04D OPT=APPLY**

Use this procedure to apply a fix to a RAMDB or check a fix against a RAMDB.

This procedure has the following format:

```
$RMDB04D OPT=APPLY  
FIX=fix-number  
[DDNAME=ddname | DATASET=dataset-name]  
[CHECK={NO | YES}]  
[DIFF={YES | NO}]  
[FORCE={NO | YES}]  
[CONFIRM={YES | NO}]  
[DB=file-id [DDBSN=db-dataset-name]]
```

**OPT=APPLY**

Specifies that a fix is being applied to a RAMDB.

**FIX=*fix-number***

Specifies the fix number to be applied. This number is used as the member name of the input partitioned data set.

**[DDNAME=*ddname* | DATASET=*dataset-name*]**

Specifies the DDNAME parameter if the data set containing the fix is already allocated to the system; or, specifies the DATASET parameter if the data set containing the fix is to be allocated by this NCL procedure and freed after the fix has been retrieved. These two parameters are mutually exclusive and, therefore, you cannot specify both of them. If neither is specified, the COMMANDS DD concatenation in the region is used.

**[CHECK={NO | YES}]**

Specifies whether the fix is checked. If you specify YES, the fix is checked only for compatibility with the database and is not actually applied to the database. The check phase is always performed regardless of the value specified. However, this parameter determines whether the check phase is the only phase to be performed.

**[DIFF={YES | NO}]**

Specifies whether differences are displayed. If you specify YES (the default), the differences between the target objects and the new objects contained in the fix are displayed for each updated object. This applies to any SET (update) and CREATE (add) actions in the fix member where the target objects already exist.

**[FORCE={NO | YES}]**

Specifies whether the fix is applied regardless of the success or failure of the check phase. However, if CHECK=YES is specified, the FORCE parameter has no effect.

**[CONFIRM={YES | NO}]**

Specifies whether the fix is retrieved and the syntax checked before being presented as a panel for browsing. The panel enables you to view the fix and confirm the application. After you confirm, the fix is applied, and the message log displays another panel for browsing. If you specify NO, the fix is applied without presenting any confirmation panel and the message log is written to the terminal rather than being displayed as a panel.

The message log is always written to the activity log regardless of the options specified.

**[DB=*file-id* [DBDSN=*db-dataset-name*]]**

Specifies the DB parameter to apply the fix to a database other than the currently allocated RAMDB. This parameter specifies the file ID of the target database. If you also specify the DBDSN parameter, the specified data set is allocated a ddname that is the same as the specified file ID, and is opened and started. The database is not freed after the fix is applied. If the database is already allocated, the specified data set name is verified as allocated to the ddname (that is the same as the specified file ID) and opened to the same file ID.

## \$RMDB04D OPT=RESTORE

Use this procedure to reverse the effect of a fix.

This procedure has the following format:

```
$RMDB04D OPT=RESTORE  
FIX=fix-number  
[DDNAME=ddname | DATASET=dataset-name]  
[CONFIRM={YES | NO}]  
[TDB=target-file-id [TDBDSN=target-dataset-name]]  
[DDB=source-file-id [DDBDSN=source-dataset-name]]
```

### **OPT=RESTORE**

Specifies that a fix, which has been applied to the target RAMDB, is being reversed.

### **FIX= *fix-number***

Specifies the fix number to back out of the RAMDB. This number is used as the member name of the fix data set and is verified against the contents of the member for the correct fix.

### **[DDNAME=*ddname* | DATASET=*dataset-name*]**

Specifies the DDNAME parameter if the data set containing the fix is already allocated to the system. Specify the DATASET parameter if the data set is to be allocated by this NCL procedure and freed after the fix has been retrieved. These two parameters are mutually exclusive and, therefore, you cannot specify both of them. If neither is specified, the COMMANDS ddname of the region is used.

### **[CONFIRM={YES | NO}]**

Specifies whether the fix is retrieved and the syntax checked before being presented as a panel for browsing. The panel lets you view the fix and confirm the restoration process. After you confirm, the fix is removed and the original data restored. The message log is presented as another panel for browsing. If you specify NO, the restoration process proceeds without presenting any confirmation panel, and the message log is written to the terminal rather than being displayed as a panel.

The message log is always written to the activity log regardless of the options specified.

### **[TDB=*target-file-id* [TDBDSN=*target-dataset-name*]]**

Reverses a fix in a database other than the currently allocated RAMDB. This parameter specifies the file ID of the target database. If you also specify the TDBDSN parameter, the specified data set is allocated a ddname that is the same as the specified file ID, and is opened and started. The database is not freed after the restoration process. If the database is already allocated, the specified data set name is verified as allocated to the ddname (that is the same as the specified file ID) and opened to the same file ID.

**DDB=source-file-id [DDBDSN=source-dataset-name]**

Specifies the file ID of the source database.

**Note:** Restoration requires the specification of the distribution (source) database through the DDB parameter.

The source database must be a copy of the original database. If you also specify the DDBDSN parameter, the specified data set is allocated a ddname that is the same as the specified file ID, and is opened and started. The database is not freed after the restoration process. If the database is already allocated, the specified data set name is verified as allocated to the ddname (that is the same as the specified file ID) and opened to the same file ID.

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



# Chapter 5: Installing Your Product From Tape

---

This section contains the following topics:

[Unload the Install Utility](#) (see page 183)

[Installation JCL](#) (see page 186)

[Maintenance](#) (see page 189)

## Unload the Install Utility

The installation utility software lets you generate and run the JCL required to install your product. The installation utility software is delivered on tape.

The installation software unloads into the *dsnpref.NMC0.CAIJCL* data set; *dsnpref* is a prefix you specify for your product data sets.

To unload the install utility, do *one* of the following:

- If *dsnpref.NMC0.CAIJCL* does not exist and you are installing from tape, [unload into a new data set from tape](#) (see page 184).
- If *dsnpref.NMC0.CAIJCL* exists from a previous installation and you are installing from tape at the current release level, [unload into an existing data set from tape](#) (see page 185).

## Additional Features

The Install Utility provides an option to install the following additional features:

- SSL support
- ReportCenter
- WebCenter SDK

You should install, set up, and customize your product region completely before installing ReportCenter or WebCenter SDK.

**Note:** For information about installing these features, see the *ReportCenter Guide* and the *WebCenter SDK Developer Guide*.

## Unload into a New Data Set from Tape

If *dsnpref.NMC0.CAIJCL* does not exist and you are installing from tape, you must unload the installation software from tape on to your DASD and into a new data set.

### To unload the software into a new data set

1. Create an unload job by copying the following JCL:

```
//jobname JOB .....
//STEP1 EXEC PGM=IEBCOPY
//SYSPRINT DD SYSOUT=*
//SYSUT1 DD DSN=CAI.SAMPJCL,
//          DISP=OLD,UNIT=?device-in,VOL=SER=?tapeser,
//          LABEL=(1,SL,EXPDT=98000)
//SYSUT2 DD DSN=?dsnpref.NMC0.CAIJCL,
//          DISP=(NEW,CATLG,DELETE),
//          UNIT=?device-out,VOL=SER=?volser,
//          SPACE=(CYL,(10,1,120)),
//          DCB=(RECFM=FB,LRECL=80,BLKSIZE=0)
//SYSIN DD DUMMY
```

**Important!** The *SYSUT2* data set name must end with *NMC0.CAIJCL*.

2. Replace the statements prefixed with a question mark (?) with your own values as follows:

#### **?device-in**

Specifies the tape drive unit to mount the tape.

#### **?tapeser**

Specifies the tape volume serial number in the form C2D66x. The value for this release is C2D66A.

#### **?dsnpref**

Specifies the data set prefix that will be used for the installation, maintenance, and Install Utility data sets. Do not include the name of your planned product region in the prefix; *?dsnpref* can be up to 29 characters long. If the data set high level qualifiers you are using do not exist, define an alias entry in the master catalog.

#### **?device-out**

Specifies the type of the DASD device where you want to place the installation software.

#### **?volser**

Specifies the volume serial number of the DASD.

If allocation is controlled by SMS, replace *UNIT=* and *VOL=SER=* with *STORCLAS=?storclass*.



3. Submit and run the job.
4. Check that the job successfully completed.

## Unload into an Existing Data Set from Tape

If *dsnpref.NMC0.CAIJCL* exists from a previous installation at the current release level and you are installing from tape, unload the installation software from tape into the existing data set.

### To unload the software into an existing data set

1. Create an unload job by copying the following JCL:

```
//jobname JOB .....
//STEP1 EXEC PGM=IEBCOPY
//SYSPRINT DD SYSOUT=*
//SYSUT1 DD DSN=CAI.SAMPJCL,
//          DISP=OLD,UNIT=?device-in,VOL=SER=?tapeser,
//          LABEL=(1,SL,EXPDT=98000)
//SYSUT2 DD DSN=?dsnpref.NMC0.CAIJCL,
//          DISP=OLD
//SYSIN DD *
        COPY I=((SYSUT1,R)),0=SYSUT2
        COPY I=((SYSUT2,R)),0=SYSUT2
/*
```

2. Replace the statements prefixed with a question mark (?) with your own values as follows:

#### **?device-in**

Specifies the tape drive unit to mount the tape.

#### **?tapeser**

Specifies the tape volume serial number in the form C2D66x. The value for this release is C2D66A.

#### **?dsnpref**

Specifies the data set prefix in the previous installation.

3. Submit and run the job.
4. Check that the job successfully completed.

## Installation JCL

The installation process creates the *dsnpref.NMC0.INSTDB* database to store details of each installation that you perform. If you are also installing other products in the Mainframe Network Management family of products, this database manages those installations. These details include the products you install and the installation values that you specify.

**Note:** During this task, the INSTALLATION JCL Library Creation panel lets you specify your installation JCL library. The default library name is *dsnpref.NMC0.INSTALL.JCL*, where *dsnpref* is the same data set prefix you used for the *dsnpref.NMC0.CAIJCL* data set.

If your installation JCL library exists, do *one* of the following:

- Specify a new data set name at that panel.
- Delete the existing library by issuing a TSO DELETE command.

**Note:** If you leave the Install Utility at any stage, you can return to it from the ISPF/PDF TSO Command Shell prompt. Execute the following command:

```
EXEC 'dsnpref.NMC0.CAIJCL(INSTALL)'
```

## Generate the Installation JCL

During the installation process, you provide the [site-specific installation information that you previously collected](#) (see page 24). This information is used to generate the installation JCL.

### To generate the installation JCL

1. At the ISPF/PDF TSO Command Shell prompt, execute the following command:

```
EXEC 'dsnpref.NMC0.CAIJCL(INSTALL)'
```

The Install Utility panel appears.

**Note:** On each of the Install Utility panels, you can use the following keys:

- Enter to proceed to the next panel
- F1 to display help
- F3 to return to the previous panel
- F4 to exit and return to the main menu

2. Press Enter.

The Install Utility Primary Menu panel appears.

3. Enter **1** (Set Installation Parameters).

The Software Delivery Method panel appears.

4. Complete each of the panels as they open. Press Enter at the completion of each panel. You must complete all five parameter panels before you can install the product. You can take the default options or specify site-specific values. For information about the fields, press F1 (Help).

5. Enter **2** (Install Products).

The INSTALLATION Primary Menu panel appears.

6. Enter **1** (Select Products to Install).

The INSTALLATION Product Selection panel appears with previously installed products unavailable.

7. Enter **S** next to the product name and press Enter.

The INSTALLATION Product Confirmation panel appears, confirming your selections.

If you have already installed another product in the product family, the INSTALLATION Components Already Installed panel appears, confirming your selections.

**Note:** You can enter S next to multiple products to install multiple products at one time. You must be licensed for any products you install.

8. Press Enter to confirm your selection and complete each of the INSTALLATION panels as they open. You must complete all the panels before you can set up your regions. You can take the default options or specify site-specific values. For information about the fields, press F1 (Help).
9. Record the data set name into which the JCL was generated in your [post-installation worksheet](#) (see page 37). Jobs can be submitted from the panel or directly from this data set after exiting the panel.

10. Submit and run the following installation jobs in sequence. Do not proceed with any job until the previous job has completed successfully. Each job should complete with return code 0 unless otherwise indicated.

**I01ALLOC**

Allocates the data sets.

The I01ALLOC member allocates CC2DLOAD as a load library of the PDS type. Do not change it to a PDS/E type because the type is not supported.

**I02INSMP**

Initializes the SMP/E data sets.

**I03RCSMP**

Performs an SMP/E RECEIVE.

**I04AKSMP**

Performs an SMP/E APPLY CHECK. This job is listed only if maintenance exists for previously installed products.

**I05RSSMP**

Performs an SMP/E RESTORE. This job is listed only if maintenance exists for previously installed products.

**I06APSMP**

Performs an SMP/E APPLY.

**I07ACSM**

Performs an SMP/E ACCEPT.

11. If you selected SSL Support as an additional feature to install, the following jobs are also generated. Submit and run them in sequence as for the previous jobs.

- I21ALLME
- I22INIME
- I23RECME
- I26APPME
- I27ACCME

**Notes:**

- If you installed and set up your regions without SSL support, and then later install SSL support, you must add the installed *dsnpref.NMC0.CC2DPLD* data set to the region's STEPLIB or in the system linklist.
- You must have SMP/E V3R5.0 to implement SSL.

12. Press F3.

You are returned to the Primary Menu panel.

## Maintenance

Maintenance includes program temporary fixes (PTFs) that supersede all authorized program analysis reports (APARs) that were created up to that time. Details of the superseded APARs are available as comments within the PTFs.

### Product Maintenance

**Important!** The *dsnpref.NMC0.CAILINK* data set must be in your system linklist before you start maintenance. You can also create a STEPLIB to the data set name (DSN) in your TSOPROC (that is, allocate it to ISPLLIB). If you installed the product using CA MSM, you must use CA MSM to apply maintenance.

Product maintenance is provided as system modification program (SMP) fixes. The fixes consist of PTFs applied using the IBM System Modification Program Extended (SMP/E) tool.

**Note:** If an installed SMP fix contains maintenance for the VSAM data sets, you must update those data sets for each region you have set up.

RAMDB maintenance is provided as SMP/E PTFs. However, this is only the delivery and recordkeeping methodology. You must apply the maintenance using \$RMDB04D.

### Apply Maintenance

This section describes how to apply individual SMP fixes using the Install Utility.

**Note:** Individual SMP fixes are only available from the [CA Technical Support site](#) (see page iv).

When you receive SMP fixes, unload them into one of the following:

- A sequential data set
- A member of a partitioned data set

Multiple SMP fixes can be appended into a single data set or member.

### To apply SMP fixes

1. Access the ISPF/PDF Primary Menu.
  2. Select the COMMAND option.  
The ISPF Command Shell panel appears.
  3. At the command prompt, enter the following command:  
`EXEC 'dsnpref.NMC0.CAIJCL(INSTALL)'`
  4. At the Install Utility title panel, press Enter.  
The Install Utility Primary Menu panel appears.
  5. At the Install Utility Primary Menu panel, enter **8** (Maintain Products).  
The MAINTENANCE Primary Menu panel appears.
  6. Enter **3** (Apply individual SMP fixes from a DASD data set).  
The MAINTENANCE DASD Fixes Dataset Name panel appears.
  7. Enter the data set name that contains the SMP fixes to be applied and press Enter.
  8. Complete the fields on the following MAINTENANCE panels as they open.
  9. At the MAINTENANCE JCL Library Creation panel, review your fix JCL library.  
The default library name is:  
`dsnpref.NMC0.FIX.DASD.JCL`  
**dsnpref**  
The same data set prefix you used for the `dsnpref.NMC0.CAIJCL` data set.
- Note:** Each time you apply maintenance, use a new output data set. A new data set ensures that the only jobs in your maintenance JCL library are the jobs required for the maintenance you are installing now. To use a new data set:
- Delete the library by issuing a TSO DELETE command and the library name, at the command prompt.
  - Specify a new data set name.
10. Press Enter to proceed with the generation of the maintenance JCL.  
When the JCL generation is complete, a list of generated jobs and a description of what each member does appears.
  11. Note the name of the data set into which the JCL was generated.

12. Submit and run the following jobs in sequence. Do not proceed with any job until the previous job has completed successfully. Each job should complete with return code 0 unless otherwise indicated.

**Important!** If there is maintenance for additional features, the SMP/E apply job must be run on a system that has the z/OS UNIX file system used during installation and mounted for read/write access.

#### **F11RCSMP**

SMP/E receives maintenance and lists existing HOLDDATA and SOURCEIDs that are already applied. If a job step returns condition code 04, there is no HOLDDATA present.

Review the information. For any held APARs that you want to apply, add the correct BYPASS HOLDx operands to the corresponding APPLY control statement for those APARs. Add the operands by manually editing the F12APSMP job that contains the SMP control statements.

**Note:** For information about the BYPASS HOLDx operands, see IBM's *SMP/E Commands* guide.

#### **F12APSMP**

SMP/E applies maintenance.

13. Press F3.

The Install Utility Primary Menu panel appears.

14. If the installed SMP fix contains maintenance for the VSAM data sets, select maintenance option **V** (Update MODS, PANELS and OSCNTL data sets with installed maintenance).

The VSAM data sets for the regions you set up are updated.

15. Press F4 to exit the Install Utility Primary Menu panel and return to the ISPF Command Shell panel, or continue with the other options.

## HOLDDATA

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

### System HOLDDATA

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

#### **ACTION**

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

#### **DEP**

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

#### **DELETE**

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

#### **DOC**

Indicates a documentation change with this SYSMOD.

#### **EC**

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

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



## External HOLDDATA

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

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

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

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

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

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

## Update VSAM Data Sets

If an installed SMP fix contains maintenance for the VSAM data sets, maintenance option V of the Install Utility becomes available. To complete maintenance, select the option to update the data sets for the regions you have set up.

### To update the VSAM data sets

1. Access the ISPF/PDF Primary Menu, and select the COMMAND option.  
The ISPF Command Shell panel appears.
2. At the command prompt, execute the following command:  

```
EXEC 'dsnpref.NMC0.CAIJCL(INSTALL)'
```

  
The Install Utility title panel appears.
3. Press Enter.  
The Install Utility Primary Menu panel appears.
4. Enter **8** (Maintain Products).  
The MAINTENANCE Primary Menu panel appears.
5. Enter **V** (Update MODS, PANELS, OSCNTL and NETINFO data sets with installed maintenance).  
The MAINTENANCE Shared Region Data Sets panel appears.
6. Review the information, and press Enter.
7. At the MAINTENANCE JOBCARD Information panel, specify your JOBCARD details and press Enter.
8. At the MAINTENANCE JCL Library Creation panel, review your fix JCL library.  
The default library name is:  

```
dsnpref.NMC0.FIX.VSAMUPD.JCL
```

#### ***dsnpref***

The same data set prefix used for the *dsnpref.NMC0.CAIJCL* data set.

**Note:** Each time you apply maintenance, use a new output data set. The new data set ensures that the only jobs in your maintenance JCL library are the jobs required for the maintenance you are installing. To use a new data set:

- Delete the library by issuing a TSO DELETE command and the library name, at the command prompt.
  - Specify a new data set name.
9. Press Enter to proceed with the generation of the maintenance JCL.
  10. Submit and run the job F21RFRSH to update the VSAM data sets.
  11. Press F3.  
The Install Utility Primary Menu panel appears.
  12. Press F4 to exit the Install Utility Primary Menu panel and return to the ISPF Command Shell panel, or continue with the other options.

## Individual RAMDB Maintenance

**Note:** Individual RAMDB maintenance is also available from the [CA Technical Support site](#) (see page iv).

This section describes how to apply maintenance to the RAMDB and details the command syntax of the \$RMDB04D maintenance utility.

**Important!** The RAMDB data set must not be updated with individual replacement records using the IDCAMS REPRO command.

When applying maintenance, you can [display details of what differences are being added, replaced, or deleted by the maintenance](#) (see page 178).

### Create Backup RAMDB

As a safety precaution, you must create a backup of your RAMDB (herein referred to RAMDBd) before applying maintenance.

#### To create the RAMDBd

1. Allocate RAMDBd in the same way that RAMDB was allocated. The cluster definition is in *dsnpref.NMC0.rname.JCL(S01LCALC)*.
2. Stop the product region.
3. Copy the data from RAMDB to RAMDBd using IDCAMS REPRO command. See the example in *dsnpref.NMC0.rname.JCL(S04LDVSM)*.
4. Restart the product region.

## Apply Maintenance to RAMDB

You can apply maintenance directly to your RAMDB. The maintenance can then propagate to all connected regions, if any. If necessary, you can restore the maintenance using your RAMDBd as input (provided that the maintenance has not yet been applied to RAMDBd).

### To apply maintenance directly to RAMDB

1. Log on to your product region and enter CMD.

The command entry panel appears.

2. Apply-check the RAMDB fix by entering the following command:

```
$RAMDB04D OPT=APPLY FIX=fix-name CHECK=YES
```

#### ***fix\_name***

Is RAM@UPDT for published solutions or TZdddd for test fixes.

When the APPLY CHECK finishes, a report appears that shows whether an APPLY of the fix will be successful, and also exactly what changes will result from the APPLY.

**Note:** Perform this step for the following reasons:

- To see what will happen if a fix is applied to a RAMDB
- To see whether a fix has been applied to a RAMDB

3. Apply the RAMDB fix by entering the following command:

```
$RAMDB04D OPT=APPLY FIX=fix_name
```

**Note:** If a RAMDB fix does not apply correctly or if you want to restore a fix, [restore the RAMDB maintenance](#) (see page 178).

## Restore RAMDB Maintenance

**Note:** This step is optional.

The RESTORE option can be used to remove an applied fix from the RAMDB by using RAMDBd as input. The fix is effectively reversed, that is, any added objects are deleted and any deleted or replaced objects are copied from RAMDBd back to the RAMDB.

To restore the fix, enter the following command:

```
$RMDB04D OPT=RESTORE FIX=fix_name DDBDSN=?RAMDBd-dataset-name DDB=?RAMDBd  
?RAMDBd
```

Specifies the ddname for the backup RAMDB.

**?*RAMDBd-dataset-name***

Specifies the full data set name of the backup RAMDB.

## RAMDB Maintenance Utility Syntax

This section contains descriptions of the RAMDB Maintenance Utility syntax.

### \$RMDB04D OPT=APPLY

Use this procedure to apply a fix to a RAMDB or check a fix against a RAMDB.

This procedure has the following format:

```
$RMDB04D OPT=APPLY  
FIX=fix-number  
[DDNAME=ddname | DATASET=dataset-name]  
[CHECK={NO | YES}]  
[DIFF={YES | NO}]  
[FORCE={NO | YES}]  
[CONFIRM={YES | NO}]  
[DB=file-id [DBDSN=db-dataset-name]]
```

#### **OPT=APPLY**

Specifies that a fix is being applied to a RAMDB.

#### **FIX=*fix-number***

Specifies the fix number to be applied. This number is used as the member name of the input partitioned data set.

**[DDNAME=*ddname* | DATASET=*dataset-name*]**

Specifies the DDNAME parameter if the data set containing the fix is already allocated to the system; or, specifies the DATASET parameter if the data set containing the fix is to be allocated by this NCL procedure and freed after the fix has been retrieved. These two parameters are mutually exclusive and, therefore, you cannot specify both of them. If neither is specified, the COMMANDS DD concatenation in the region is used.

**[CHECK={NO | YES}]**

Specifies whether the fix is checked. If you specify YES, the fix is checked only for compatibility with the database and is not actually applied to the database. The check phase is always performed regardless of the value specified. However, this parameter determines whether the check phase is the only phase to be performed.

**[DIFF={YES | NO}]**

Specifies whether differences are displayed. If you specify YES (the default), the differences between the target objects and the new objects contained in the fix are displayed for each updated object. This applies to any SET (update) and CREATE (add) actions in the fix member where the target objects already exist.

**[FORCE={NO | YES}]**

Specifies whether the fix is applied regardless of the success or failure of the check phase. However, if CHECK=YES is specified, the FORCE parameter has no effect.

**[CONFIRM={YES | NO}]**

Specifies whether the fix is retrieved and the syntax checked before being presented as a panel for browsing. The panel enables you to view the fix and confirm the application. After you confirm, the fix is applied, and the message log displays another panel for browsing. If you specify NO, the fix is applied without presenting any confirmation panel and the message log is written to the terminal rather than being displayed as a panel.

The message log is always written to the activity log regardless of the options specified.

**[DB=*file-id* [DBDSN=*db-dataset-name*]]**

Specifies the DB parameter to apply the fix to a database other than the currently allocated RAMDB. This parameter specifies the file ID of the target database. If you also specify the DBDSN parameter, the specified data set is allocated a ddname that is the same as the specified file ID, and is opened and started. The database is not freed after the fix is applied. If the database is already allocated, the specified data set name is verified as allocated to the ddname (that is the same as the specified file ID) and opened to the same file ID.

**\$RMDB04D OPT=RESTORE**

Use this procedure to reverse the effect of a fix.

This procedure has the following format:

```
$RMDB04D OPT=RESTORE
FIX=fix-number
[DDNAME=ddname | DATASET=dataset-name]
[CONFIRM={YES | NO}]
[TDB=target-file-id [TDBDSN=target-dataset-name]]
[DDB=source-file-id [DDBDSN=source-dataset-name]]
```

**OPT=RESTORE**

Specifies that a fix, which has been applied to the target RAMDB, is being reversed.

**FIX= *fix-number***

Specifies the fix number to back out of the RAMDB. This number is used as the member name of the fix data set and is verified against the contents of the member for the correct fix.

**[DDNAME=*ddname* | DATASET=*dataset-name*]**

Specifies the DDNAME parameter if the data set containing the fix is already allocated to the system. Specify the DATASET parameter if the data set is to be allocated by this NCL procedure and freed after the fix has been retrieved. These two parameters are mutually exclusive and, therefore, you cannot specify both of them. If neither is specified, the COMMANDS ddname of the region is used.

**[CONFIRM={YES | NO}]**

Specifies whether the fix is retrieved and the syntax checked before being presented as a panel for browsing. The panel lets you view the fix and confirm the restoration process. After you confirm, the fix is removed and the original data restored. The message log is presented as another panel for browsing. If you specify NO, the restoration process proceeds without presenting any confirmation panel, and the message log is written to the terminal rather than being displayed as a panel.

The message log is always written to the activity log regardless of the options specified.

**[TDB=*target-file-id* [TDBDSN=*target-dataset-name*]]**

Reverses a fix in a database other than the currently allocated RAMDB. This parameter specifies the file ID of the target database. If you also specify the TDBDSN parameter, the specified data set is allocated a ddname that is the same as the specified file ID, and is opened and started. The database is not freed after the restoration process. If the database is already allocated, the specified data set name is verified as allocated to the ddname (that is the same as the specified file ID) and opened to the same file ID.

**DDB=source-file-id [DDBDSN=source-dataset-name]**

Specifies the file ID of the source database.

**Note:** Restoration requires the specification of the distribution (source) database through the DDB parameter.

The source database must be a copy of the original database. If you also specify the DDBDSN parameter, the specified data set is allocated a ddname that is the same as the specified file ID, and is opened and started. The database is not freed after the restoration process. If the database is already allocated, the specified data set name is verified as allocated to the ddname (that is the same as the specified file ID) and opened to the same file ID.

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



# Chapter 6: Configuring Your Product

---

This chapter describes how to use the Install Utility to set up the regions required by this product.

**Important!** You must put the *dsnpref.NMC0.CAILINK* data set in your system linklist before you start setting up regions. You can also create a STEPLIB to the data set name (DSN) in your TSOPROC (that is, allocate it to ISPLLIB).

This section contains the following topics:

[How Region Setup Works](#) (see page 201)

[Region Contents](#) (see page 202)

[SOLVE SSI as Common Component](#) (see page 202)

[Specify the SOLVE SSI Region](#) (see page 203)

[Specify the Product Region](#) (see page 204)

[Specify the NMFTP Monitor Region](#) (see page 207)

## How Region Setup Works

You can have more than one region on a system. Each region runs as a started task.

The Install Utility uses the [site-specific information you collected during preinstallation](#) (see page 24) to generate the jobs that build the regions. If you need additional regions, you can reuse the Install Utility to create them.

**Note:** If you use CA MSM to deploy the software on different systems before you perform the setup, you must use the Install Utility on a target system to perform the setup on that system.

**Important!** After you have run a setup job, you cannot alter the results using the setup software. You can use the setup software to create a region, or you can manually customize the existing region's JCL.

## Region Contents

Your product is comprised of the following regions:

### **SOLVE Subsystem Interface (SOLVE SSI) Region**

Provides communication between the product region and other software on a system. One SOLVE SSI can serve multiple product regions.

### **Product Region**

Specifies where you sign on and use your product. You can have more than one product region on a system.

### **NMFTP Monitor Region**

Specifies that the NMFTP Monitor provides communication between the product region and the SMFAPI on a system. One NMFTP Monitor can serve multiple product regions.

## SOLVE SSI as Common Component

The SOLVE SSI is a common component for multiple CA product families and can serve multiple product regions on a system. The following methods are available:

- One shared SSI to serve all product families.
- A separate SSI for each product family (CA Mainframe Network Management, CA SOLVE:Operations Automation, and CA SOLVE:Access).
- A mix of the first two methods, for example, CA SOLVE:Access has its own SSI and CA Mainframe Network Management and CA SOLVE:Operations Automation share an SSI.

**Note:** If you have already installed another Mainframe Network Management product and set up a SOLVE SSI, you do not need to set up another SOLVE SSI. You must, however, ensure that the SOLVE SSI parameters suit your product and site requirements.

## Specify the SOLVE SSI Region

Use this procedure to provide communication between the product region and other software on a system.

### To specify a SOLVE SSI region

1. At the ISPF/PDF TSO Command Shell prompt, execute the following command:

```
EXEC 'dsnpref.NMC0.CAIJCL(INSTALL)'
```

The Install Utility panel appears.

**Note:** On each of the Install Utility panels, you can use the following keys:

- Enter to proceed to the next panel
- F1 to display the online help
- F3 to return to the previous panel
- F4 to exit and return to the main menu

2. Press Enter.

The Install Utility Primary Menu panel appears.

3. (Optional) If you have installed the product using CA MSM, perform the following steps:

- a. Enter **1**.

The Software Delivery Method panel appears.

- b. Complete the panel:

- Enter **S** next to CA MSM.
- Specify the name of the CSI data set used during product installation in the SMP/E CSI Used field.

- c. Press Enter.

4. Enter **4**.

A panel appears listing several approaches to implement your SOLVE SSI environment.

**Note:** For more information, press F1 (Help).

5. Press Enter.

The SETUP SOLVE SSI Primary Menu panel appears.

6. Enter **1** (Add a Region).

The SETUP Specify SOLVE SSI Name panel appears.

7. Enter the name (*ssiname*) and description of the SOLVE Subsystem Interface region you are setting up. The initial value is SOLVESSI.

The setup software uses the name to generate the started task JCL. For example, if the name is SOLVESSI, your started task JCL is named SOLVESSI.

8. Complete each of the SETUP panels as they appear. You can accept the default values or specify site-specific values. For information about the fields, press F1 (Help).

The Install Utility generates a series of setup jobs into the *dsnpref.NMC0.ssiname.JCL* library.

9. Record the name of the data set into which the JCL was generated in your [post-installation worksheet](#) (see page 37).

**Note:** If you want to set up a new SSI, continue with these steps. Otherwise, skip the remaining steps in this procedure, verify that the required SSI parameters are present in your existing shared SSI, and update them as necessary.

10. Submit and run the following:

**S01LCALC**

Allocates the SOLVE SSI data sets if the value in the Enable the Packet Analyzer field on the SETUP Region Parameters panel is set to YES.

**S02LDPDS**

Copies the PDS members to *dsnpref.NMC0.SSIPARM*.

**S03MIGRT**

Copies data from earlier releases.

This job is only generated if the value in the Enable the Packet Analyzer field on the SETUP Region Parameters panel is set to YES.

11. Press F3.

The Install Utility Primary Menu panel appears.

## Specify the Product Region

The Install Utility lets you set up a region with the products you installed. If you need additional product regions, you can reuse the Install Utility to create them.

**To specify a product region**

1. At the ISPF/PDF TSO Command Shell prompt, execute the following command:

```
EXEC 'dsnpref.NMC0.CAIJCL(INSTALL)'
```

The Install Utility panel appears.

**Note:** On each of the Install Utility panels, you can use the following keys:

- Enter to proceed to the next panel
- F1 to display help
- F3 to return to the previous panel
- F4 to exit and return to the main menu

2. Press Enter.

The Install Utility Primary Menu panel appears.

3. Enter **5** (Setup a NetMaster/SOLVE Product Region).

The SETUP Product Region Primary Menu panel appears.

4. Enter **1** (Add a Region).

The SETUP Specify Product Region Name panel appears.

**Note:** If you want to add this product to an existing region, enter **4** (Add Products and Additional Features to a Region) and select the appropriate region.

5. Enter the name (*rname*) and description of the region you are setting up. The initial value is NM.

The Install Utility uses the name that you entered to generate local data set names and the started task JCL. For example, if you enter REGION01 as the region name, your started task JCL is REGION01 and a local region file, such as the Virtual File System (VFS), is *dsnpref.REGION01.VFS*.

The SETUP Product Selection panel appears.

6. Enter **S** next to the products you are licensed to include in the region.
7. Complete each of the SETUP panels as they open. You can accept the default values or specify site-specific values.

**Note:** For information about the fields, press F1 (Help).

**Note:** On the SETUP Region Information panel, ensure that the value of the Subsystem Interface Identifier matches the value of the SOLVE SSI you intend to use.

The setup software generates a series of setup jobs in the *dsnpref.NMC0.rname.JCL* library.

8. Record the name of the data set into which the JCL was generated in your [post-installation worksheet](#) (see page 37).

9. Submit and run the following jobs in sequence. Do not proceed with any job until the previous job has completed successfully. Each job should complete return code 0 unless otherwise indicated.

**S01LCALC**

Allocates the region-specific (local) data sets. If you are upgrading and have increased the size of a particular file, modify the JCL to increase the space allocation as required.

**S02SHALC**

Allocates the shared run-time data sets.

**S03LDVIP**

Populates the MODS, PANELS, and OSCNTL files.

**S04LDVSM**

Populates the other VSAM files.

**S05LDPDS**

Copies some PDS members to *dsnpref.rname*.TESTEXEC or *dsnpref*.PARMLIB for use by the product region. If this product is being added to an existing region, the RUNSYSIN and IIAPARMS are overwritten.

**Note:** The member names for IIAPARMS and SXPARMS include the domain ID, so they appear as *IIAdmid* and *SXPdmid*.

**S06MIGRT**

Copies site-specific VSAM data from an earlier release.

**Note:** After your product is installed, it monitors the size of your VSAM data sets. For more information about tuning VSAM data sets, see the *Reference Guide*.

10. Press F3.

The Install Utility Primary Menu panel appears.

**Note:** If you want to replicate this product region on another system, certain data sets are required. Copy the data sets listed in *dsnpref*.NMC0.*rname*.JCL(DSLIST) to your target system.

## Specify the NMFTP Monitor Region

**Note:** The NMFTP Monitor is only required if you need to monitor FTP events using an IBM TCP/IP stack.

One NMFTP Monitor (NMFTPMON) can serve multiple product regions on a system.

### To specify an NMFTP Monitor region

1. At the Install Utility Primary Menu panel, enter **6**.  
The SETUP NMFTP Monitor Primary Menu panel appears.
2. Enter 1 (Add a Region).  
The SETUP Specify NMFTP Monitor Name panel appears.
3. Enter the name (*nmftname*) and description of the NMFTP Monitor region you are setting up. The initial value is NMFTPMON.  
The setup software uses the name to generate the started task JCL. For example, if the name is NMFTPSSI, your started task JCL will be called NMFTPSSI.
4. Complete each of the SETUP panels as they appear. You can accept the default values or specify site-specific values. For information about the fields, press F1 (Help).
5. The setup software generates a series of setup jobs into the *dsnpref.NMC0.nmftname.JCL* library.
6. Record the name of the data set into which the JCL was generated in your Installation Values worksheet (see Post-Implementation Record Keeping on page 82).
7. Submit and run the following:
  - S01LCALC
  - S02LDPDSThe PDS members are copied to *dsnpref.NMC0.SSIPARM*.
8. Press F3.  
The Install Utility Primary Menu panel appears.

**Note:** If the required NMFTP Monitor address space is not available, no NMFT normalized File Transfer Events are generated.





# Chapter 7: Creating VTAM Definitions and Tables

---

This chapter describes how to set up your VTAM major node.

This section contains the following topics:

[Create VTAM Definitions and Tables](#) (see page 209)

## Create VTAM Definitions and Tables

The Create VTAM Definitions and Tables facility builds the VTAM major node, which contains application definition statements for all ACBs required by your product regions. Perform this task initially when all product regions have been set up. If changes are made to any regions or if additional regions are added later, perform the task again.

**Note:** You use the major node that you create in this procedure to [activate your VTAM applications](#) (see page 242).

### To create VTAM definitions and tables

1. At the ISPF/PDF TSO Command Shell prompt, execute the following command:

```
EXEC 'dsnpref.NMC0.CAIJCL(INSTALL)'
```

The Install Utility Primary Menu panel appears.

2. Enter **7** (Create VTAM Definitions and Tables).

The VTAM Primary Menu panel appears.

3. Enter **1** (Create VTAM Definitions and Tables).

The VTAM Data Sets panel appears.

4. Enter the VTAM major node name (*vtamname*) and data set names of the requested IBM data sets.

The VTAM NetMaster/SOLVE ACBs panel appears and displays the prefix for External Interface Package (EIP) ACBs and the names of all product regions and the ACBs associated with them.

**Note:** If >>> appears, you can use F10 (right) to display all ACBs.

5. Enter the prefix for EIP ACBs.

6. Complete each of the remaining panels as they appear. You can accept the default values or specify site-specific values. For information about the fields, press F1 (Help).

The Install Utility generates a series of jobs in the *dsnpref.NMC0.VTAM.JCL* library.

7. Record the name of the data set into which the JCL was generated in your [post-installation worksheet](#) (see page 37).
8. Submit and run the following jobs in sequence:

**V01LDVTM**

Copies major node into SYS1.VTAMLST.

**V02ASMOD**

Assembles VTAM MODE table.

This job is required only if you want to provide users with access to external applications. Your product uses VTAM mode tables that are assembled and linked into a load library available to VTAM, and the tables lets users access external applications.

Each job should return condition code 0 unless otherwise indicated.

9. Press F3.

The Install Utility Primary Menu panel appears.

10. Enter **X**.

The Install Utility closes.

**Note:** Press F1 (Help) for information about any panel.

# Chapter 8: Preparing the IBM Communications Server

---

This chapter describes how to prepare IBM's Communications Server to communicate with this product.

If you do not use IBM Communications Server, skip to [Preparing CA TCPAccess CS](#) (see page 219).

## Define UNIX Authorization for Your Started Task User IDs

The product region requires access to sockets interfaces and therefore requires UNIX System Services authorization provided by an OMVS segment security definition.

For the UNIX functions, the SOLVE SSI region requires UNIX System Services authorization provided by an OMVS segment security definition.

Set [UNIX System Services authorization](#) (see page 279) for the following:

- The product region's started task user ID
- The SOLVE SSI region's started task user ID
- NMFTP Monitor region (if defined)

## User Functionality Authorization

**Note:** If you are using CA ACF2 for z/OS, you do not need to perform this task unless it is set up to protect operator commands.

Your product uses z/OS operator VARY commands to drop connections. The user ID associated with your product region must be authorized by your security system to issue these commands.

The OPERCMDS resource to be accessed with UPDATE access level is MVS.VARY.TCPIP.DROP OPERCMDS.

Authorize individual users to the OPERCMDS resources if you:

- Plan to configure your system to use SAF user security
- Are using a partial security exit that returns a SAF UTOKEN, for example NMSAFPX

### Example: Authorization in a CA ACF2 System that Protects Operator Commands

```
$KEY(MVS) TYPE(OPR)  
VARY.TCPIP.- UID(uid_string) SERVICE(UPDATE) ALLOW
```

### Example: Authorization in a CA Top Secret System

```
TSS PER(XXXXXX) OPERCMD(MVS.VARY.) ACCESS(UPDATE)
```

### Example: Authorization in a RACF System

```
PE MVS.VARY.TCPIP.* CLASS(OPERCMDS) ID(uuuuuuu) ACCESS(UPDATE)
```

## Set Up the SNMP Agent

**Note:** Do not perform this task if OSNMPD is already configured.

### To set up the SNMP agent

1. Configure the SNMP agent (OSNMPD) by following the instructions in the *IBM Communications Server IP Configuration Guide*.
2. Locate the PW.SRC data set in the OSNMPD started task JCL. This data set can be:

- A z/OS data set, for example:

```
//SYSPWSRC DD DISP=SHR,DSN=TCPIP.DATA(PWSRC)
```

- A z/OS UNIX file, for example:

```
/etc/pw.src
```

3. In the PW.SRC data set, configure a community name for use by the local host IP address.

**Important!** Community names are case sensitive. The default community name is public in lowercase.

For example, with multiple IP addresses, if the Communications Server has the IP addresses 192.168.8.1 and 192.168.1.2, your PW.SRC data set could contain something like the following:

```
public 192.168.0.0 255.255.0.0
```

With a single IP address, if Communications Server has the IP address 192.168.0.1, your PW.SRC data set could contain something like the following:

```
public 192.168.0.1 255.255.255.255
```

It is not necessary to activate the SNMP Query Engine (SNMPQE) because the functions it performs are done internally by your product.

4. Locate the PROFILE data set.
5. Set up the TCP/IP subagent in the PROFILE data set by following the instructions in the *IBM Communications Server IP Configuration Guide*, for example:  

```
SACONFIG COMMUNITY public AGENT 161 ENABLED
```
6. Activate the SNMP agent (OSNMPD) by following the instructions in the *IBM Communications Server IP Configuration Guide*.

## Generate SMF Records for FTP Event Flow

**Note:** Perform this task only if you want to monitor FTP events.

The Communications Server must be set up to generate the SMF records required for FTP events.

The SMF records are intercepted by the NMFTP Monitor region and are used by the product region to enable the following:

- File Transfer events monitoring
- Event history reporting

**To ensure SMF records are generated**

1. Add the following line to the PROFILE.TCPIP configuration member to enable the SMF API:

```
NETMONITOR SMFSERVICE
```

2. Restart the TCP/IP started task.

**Note:** Alternatively, you can issue this change in an OBEYFILE.

## Generate FTP Post-Processing Transfer Failures Event Flow

**Note:** Perform this task only if you want to monitor FTP events.

You can use this procedure to monitor all FTP failures.

### To generate transfer failures *without* existing user exit

1. Receive and apply the *dsnpref.NMC0.CC2DSAMP*(FTPOSTPR) SMP/E USERMOD.

The FTPPOSTPR exit is created.

2. Do *one* of the following:

- APF-authorize the *dsnpref.NMC0.CC2DLOAD* library, and include it as a STEPLIB for your FTP server started task (typically named FTPD).
- Copy FTPPOSTPR from the *dsnpref.NMC0.CC2DLOAD* library into an existing APF-authorized library that also is included as a STEPLIB to your FTP server job.
- Copy to a link library known to the linklist.

3. If you are using RACF and program control is active, use the following commands to add FTPPOSTPR to program control:

```
RDEFINE PROGRAM FTPPOSTPR ADDMEM('library'//NOPADCHK) UACC(READ)
SETROPTS WHEN(PROGRAM) REFRESH
```

#### ***library***

Identifies the library that contains FTPPOSTPR.

**To generate transfer failures *with* existing user exit**

1. Modify your existing FTP post-transfer processing user exit (FTPOSTPR) by inserting the following code fragment immediately before exiting:

```
*------(NetMaster For File Transfer Management )-----*
*
*      .------.
*      | Call the CA NMFT FTP Post-Transfer Processing module |
*      '------'
*
L      R15,=V(NM000FPX)
O      R15,=X'80000000'
BASSM R14,R15          Call NM000FPX
L      R14,=A(NEXT0000+X'80000000')
BSM    0,R14          Ensure in 31-BIT if required
SPACE 2
NEXT0000 DS    0H
```

These lines are added in the module entry section, and register 1 must point to the parameter list passed to FTPPOSTPR.

2. Modify your existing FTP post-transfer processing user exit (FTPOSTPR) link-edit deck by inserting the following:

```
//AC2DLOAD DD DISP=SHR,DSN=dsnpref.NMC0.AC2DLOAD
//SYSLIN DD *
...
INCLUDE AC2DLOAD (NM000FPX)
INCLUDE AC2DLOAD (NM000Y51)
ORDER          NM000FPX
ORDER          FPXDATA
ORDER          NM000Y51
ENTRY          FTPPOSTPR
MODE           AMODE(31)
MODE           RMODE(ANY)
NAME           FTPPOSTPR(R)
```

3. Submit the modified job to assemble and link edit the exit.
4. Ensure that the user exit load module is in a cataloged data set and placed in an APF authorized library that the FTP server accesses using STEPLIB, linklist, or LPA.

**Note:** The existing FTP Control Customizer parameter group option Enable FTP Event Receiver (for non-TCPaccess FTP server), also controls the FTP Post Processing User Exit event delivery.



## NMFTP Monitor Access to NMI API SMF Records

**Note:** Perform this task only if you want to monitor FTP events.

You can use one of the following methods to grant the NMFTP Monitor region access to Network Management Interface (NMI) API SMF records:

- SERVAUTH
- Access to BPX.SUPERUSER

### SERVAUTH

If you want to ensure the highest level of security, define the SERVAUTH profile name EZB.NETMGMT.sysname.tcpname.SYSTCPSM and grant the NMFTP Monitor user ID READ access to this profile name.

**Important!** After the SERVAUTH facility has been defined to your security system, TCP/IP resource protection will be enabled. This affects the ability of users to access TCP/IP resources other than just SYSTCPSM. For example, it may restrict the ability to open sockets, bind to non-ephemeral ports, use Netstat, and use certain network resources. Before using this method, see IBM's *Communications Server IP Configuration Guide* for more information about TCP/IP resource protection.

**Important!** If your security setup does not distinguish between a resource profile not defined and a user not permitted to that resource, you may need to define profiles for resources other than just SYSTCPSM whenever the SERVAUTH class is active. See IBM's *Communications Server IP Configuration Guide* for more information.

**Note:** We recommend that you use this method.

#### Example: CA ACF2 System

```
SET RESOURCE(SERVAUTH)
COMPILE *
$KEY(EZB) TYPE(SERVAUTH)
NETMGMT.SYSA.TCPIPA.SYSTCPSM UID(USER1) SERVICE(READ) ALLOW
STORE
```

**Note:** Instead of using TSO, you can use the ACFBATCH utility in JCL. If you do this, omit the [ACF] and [END] lines.

#### Example: CA Top Secret System

```
TSS ADD SERVAUTH(EZB.NETMGMT.SYSA.TCPIPA.SYSTCPSM)
TSS PER(nmuser) SERVAUTH(EZB.NETMGMT.SYSA.TCPIPA.SYSTCPSM)
ACCESS(READ)
```

### Example: RACF System

```
RDEFINE SERVAUTH EZB.NETMGMT.SYSA.TCPIPA.SYSTCPSM UACC(NONE)
SETR RACLIST(SERVAUTH) REFRESH
PE EZB.NETMGMT.SYSA.TCPIPA.SYSTCPSM CLASS(SERVAUTH) ID(nmuser)
ACCESS(READ)
```

### BPX.SUPERUSER

If you are less concerned with security, grant the NMFTP Monitor user ID READ access to the BPX.SUPERUSER facility.

### Example: CA ACF2 System

```
SET RESOURCE(FAC)
COMPILE *
$KEY(BPX) TYPE(FAC)
SUPERUSER UID(USER1) SERVICE(READ) ALLOW
STORE
```

**Note:** Instead of using TSO, you can use the ACFBATCH utility in JCL. If you do this, omit the [ACF] and [END] lines.

### Example: CA Top Secret System

```
TSS PER(nmuser) IBMFAC(BPX.SUPERUSER) ACCESS(READ)
```

### Example: RACF System

```
PE BPX.SUPERUSER CLASS(FACILITY) ID(nmuser) ACCESS(READ)
```

# Chapter 9: Preparing CA TCPaccess CS

---

This chapter describes how to prepare CA TCPaccess CS to communicate with your product.

If you do not use CA TCPaccess CS, skip to the next chapter.

This section contains the following topics:

[Generate SMF Records for FTP Event Flow](#) (see page 219)

[Set Up DNR Members](#) (see page 220)

[Enable Access to SNMP Data](#) (see page 221)

[Restart CA TCPaccess](#) (see page 221)

## Generate SMF Records for FTP Event Flow

You must implement the software for the product region to generate SMF Records for the FTP event flow.

### To generate SMF Records for the FTP event flow

1. Check the IJTFCGxx configuration member to ensure that all of the subtypes that you require will be generated.

The SMF TYPE parameter identifies whether or not SMF records are created.

**Note:** If your SMF statement does not specify SUBTYPE or has SUBTYPE(ALL), you can skip this step.

The SMF statement includes a SUBTYPE parameter. This allows specific subtypes to be selected or suppressed. Do the following:

- If the parameter is set to ALL, leave it as it is.
- If the parameter is set to NONE, set it to ALL or a list of the subtypes that you require.
- If the parameter is set to a list of subtypes, set it to ALL or a list of the subtypes that you require.

This product uses SUBTYPE 20, FTP data set transfer completion (RETR, STOR, and APPE).

2. Copy the NMDSPAXS load module supplied in *dsnpref.NMC0.CC2DLOAD* to a library accessible to CA TCPaccess CS, for example a library in the CA TCPaccess CS started task STEPLIB.

3. Define NMDSPAXS as a CA TCPaccess CS exit by adding the following statement to IJTFCGxx member:

```
EXIT PROGRAM (NMDSPAXS)
```

**Note:** Insert the NMDSPAXS definition in the first position of the exit list. This ensures that the exit is always called.

## Set Up DNR Members

You must ensure that your CA TCPaccess CS Domain Name Resolver (DNR) members can translate the CA TCPaccess CS subsystem name into an IP address and a fully-qualified host name.

### To set up DNR members

1. Enable translation from subsystem name to fully-qualified domain name.

For example, if your CA TCPaccess CS subsystem name is ACSS and its fully-qualified domain name is MVS.SITE1.COM, enter a line like the following into your DNRALCxx member:

```
ACSS MVS.SITE1.COM.
```

Specify the domain name (rather than an IP address) and end it with a period (.).

2. Enable local translation of the fully qualified host name to an IP address.

For example, if the IP address of MVS.SITE1.COM. is 172.24.123.112, enter a line like the following into your DNRHSTxx member:

```
MVS.SITE1.COM. 172.24.123.112
```

3. Ensure that the HOSTTABLE statement in the DNRCFGxx member points to the correct DNRHSTxx member.
4. Restart DNR. You do not need to restart CA TCPaccess CS to introduce changes to the DNR tables. For example:

```
F stackname,STOP DNR TASK(n)  
F stackname,START DNR CNFG(xx)
```

TASK(n) is the DNR task number used by the site.

## Enable Access to SNMP Data

Your product accesses information about CA TCPaccess CS by using SNMP.

To enable these functions, you must activate the SNMP Agent by updating the SNMCFGxx member in the CA TCPaccess CS PARM data set. Make sure that you have a community value statement, which includes the community name. The default community name is *public* in lower case. You do not need to restart CA TCPaccess CS.

To activate SNMP, issue **/F stackname,START SNM CNFG(xx)**.

Make sure you update the STARTxx member to include the following:

```
'START SNM CNFG(xx)
```

## Restart CA TCPaccess

If you have made changes to your IJTFCGxx configuration member, you need to restart the server.

### To restart the server

1. Restart the server to bring the changes into effect.
2. Check the job log and the SYSLOG for the presence of the following messages:

```
T00EX004I NMDSPAXS: N6XA01 Activity log message interface initialized
T00EX004I NMDSPAXS: N6XA02 Receiver ID $IPXssid will monitor messages from
TCPaccess
T00EX004I NMDSPAXS: N6XA03 NetMaster AXS exit EP:exit_entry_point
Compiled:compilation_timestamp
```

*ssid* is the SSID of the server job.

These messages are logged during initialization. Their presence indicates that the interface has been set up correctly.



# Chapter 10: Setting Up File Transfer Resources

---

This chapter describes how to define and implement your File Transfer resources.

## Customize Managed CA XCOM Regions

You can use this procedure to customize a CA XCOM Data Transport region to work with this product.

### To customize a managed CA XCOM Data Transport region

1. Ensure that the values of the following parameters in the CA XCOM Data Transport Default Options Table are set as follows:
  - NETMAST=YES
  - RECVRID=*xcom-event-receiver-id*

The value of the RECVRID parameter must match the CA XCOM Data Transport event receiver ID specified in the XCAPI parameter group of CA NetMaster FTM. If the parameter is not specified, it assumes the value \$RFFTEVR.
  - ERRINTV=*error-retry-interval*

Use a low value for the ERRINTV parameter to ensure that accurate transfer request status is displayed on the monitors. You can either use the default parameter or use a lower value.
2. Reassemble and link the Default Options Table.

**Note:** This step only applies if you make changes to the default parameters. The remaining steps are required only if one of the following applies:

  - You have not already applied the CA XCOM Data Transport user modification (USERMOD) for CA NetMaster support (as part of previous installation of CA NetMaster FTM).
  - You are upgrading CA XCOM Data Transport to r11.

3. (This step is for r11.0 and below only.) Copy one of the following job members, depending on your version of CA XCOM Data Transport:
  - If you are managing an Advantage CA XCOM Data Transport 3.1 region (or a previous release), copy the *dsnpref.NMC0.CC17SAMP(XCUSRMOD)* job member to the *dsnpref.NMC0.rname.JCL* data set.

The job applies user modification (USERMOD) to include the exit in the CA XCOM Data Transport region.
  - If you are managing a CA XCOM Data Transport r11 region, copy the *dsnpref.NMC0.CC17SAMP(XCUSRM11)* job member to the *dsnpref.NMC0.rname.JCL* data set.

The job applies user modification (USERMOD) to include the exit in the CA XCOM Data Transport r11 region.
4. (This step is for r11.0 and below only.) Review the comments in the copy, and update the variables that start with a question mark (?).
5. (This step is for r11.0 and below only.) Submit the customized job.
6. Restart the CA XCOM Data Transport region.

## How CA SOLVE:FTS Regions Work

If you are using CA SOLVE:FTS and want to customize a CA SOLVE:FTS region to work with this product, perform the procedures in this section.

This product can manage CA SOLVE:FTS in the same region using the FTSMGR FTSELF template. Links are only required to manage remote regions.



## Define the Link to the Product Region

The CA NetMaster FTM and CA SOLVE:FTS regions communicate with an INMC link.

### To define a link to the product region

1. Log on to the CA SOLVE:FTS region, and select Operator Console Services.
2. Enter the following DEFLINK command to enable the dynamic creation of an INMC link:

```
DEFLINK LUNAME=acb-name LINK=link-name
```

#### ***acb-name***

Specifies the ACB name of the product region to which the CA SOLVE:FTS region is to establish a link.

#### ***link-name***

Specifies a name that identifies the link.

3. Enter SHOW LINK=DYNAMIC to check that the allowed number of dynamic links will not be exceeded.
4. Issue the following command:

```
SYSPARMS DYNLMAX=number
```

#### ***number***

Sets the number of allowed dynamic links.

The number of dynamic links is increased.

5. Ensure that the DEFLINK and the SYSPARMS commands are included in the NMREADY procedure for the CA SOLVE:FTS region to enable the automatic execution of the commands during region startup.

## Install the CA SOLVE:FTS Message Handler

**Note:** If the release of the CA SOLVE:FTS region is at least r11.5, there is no need to install the \$RFAGENT message handler in it because extra data is provided on \$\$FTS events.

The CA SOLVE:FTS message handler, \$RFAGENT, processes CA SOLVE:FTS events before they are sent to the CA NetMaster FTM region. If your CA SOLVE:FTS region is the same as your CA NetMaster FTM region, \$RFAGENT is already available, so you do not need to copy it.

To install the handler, copy *dsnpref.NMC0.CC17EXEC(\$RFAGENT)* to the NCL procedures library (normally *dsnpref.rname.TESTEXEC*) in the CA SOLVE:FTS region.

**Important!** The \$RFAGENT message handler must be present in each pre-r11.5 CA SOLVE:FTS region that you want to monitor.

## How Managed CONNECT:Direct Regions Work

You can use the procedures in this section to implement the flow of CONNECT:Direct events.

## Implement Statistics Exits in the Managed CONNECT:Direct Regions

**Note:** The File Transfer statistics exit in each managed CONNECT:Direct region must be current for the version of CA NetMaster FTM you are running.

### To implement the File Transfer statistics exits in each managed CONNECT:Direct regions

1. Include the supplied APF-authorized CC2DLOAD library in the STEPLIB DD statements of the CONNECT:Direct startup JCL procedure. (The library is set up as *dsnpref.NMC0.CC2DLOAD*.)
2. Depending on your current CONNECT:Direct setup, you might need to update the following statement in the *dsnpref.NMC0.CC17SAMP(NMCDSTEX)* statistics exit:

```
$RFGDSTX  
AMODE=31,USREXIT=NONE,EPSRCVR=$RFFTEVR,  
EXCLUDE=NONE
```

**Important!** If modifications are required, we recommend that you create an SMP/E ++USERMOD to record and control the changes, and then copy the member to TESTEXEC. Alternatively, you can copy the distributed member to the region's TESTEXEC data set for modification.

3. Specify the load module name of your exit in the USREXIT parameter if you are already using a CONNECT:Direct statistics exit.
4. Copy the list of excluded record types to the EXCLUDE parameter and remove STAT.EXCLUDE from the CONNECT:Direct initialization parameter if you are excluding records from the CONNECT:Direct statistics file.
5. Ensure that the value of the EPSRCVR parameter matches the CONNECT:Direct event receiver ID specified in the CDAPI parameter group of CA NetMaster FTM. Multiple CONNECT:Direct regions can use the EPSRCVR ID concurrently.

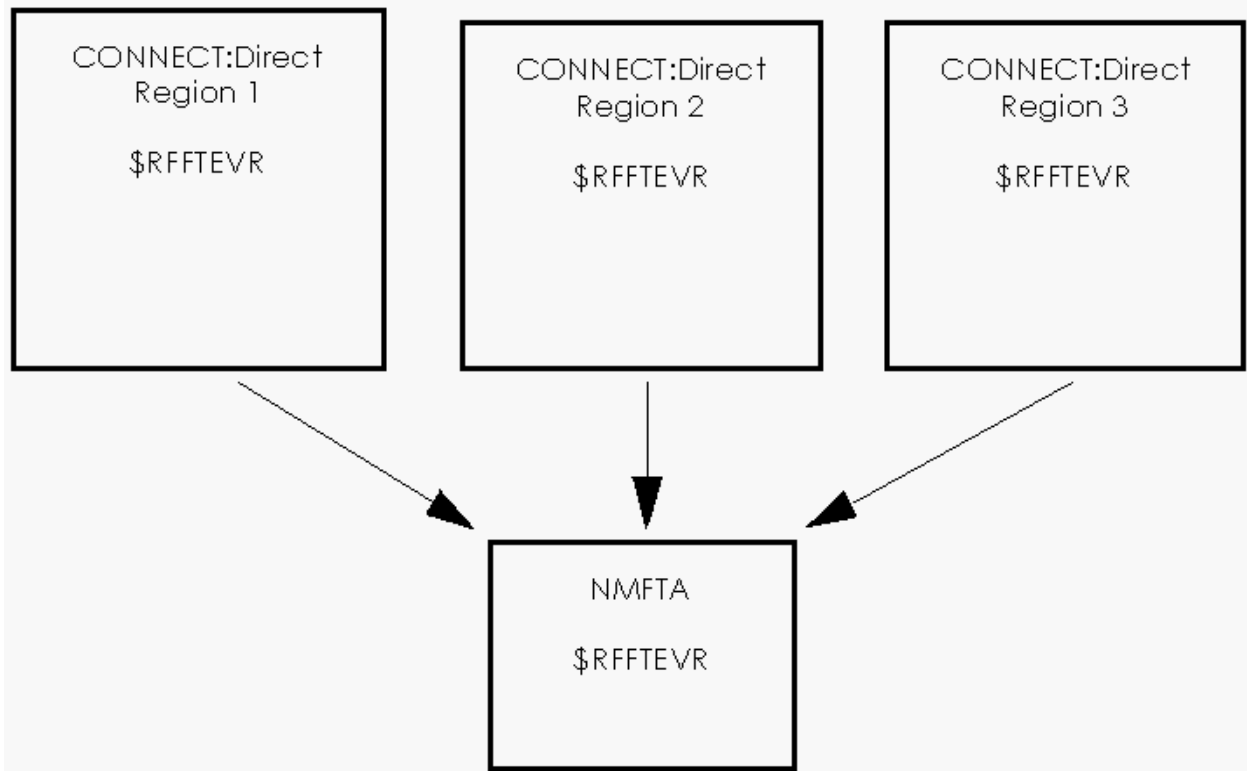
**Note:** The NMCDSTEX member also contains comments that provide additional background information.

6. If you updated the NMCDSTEX statistics exit in TESTEXEC, perform the following steps:
  - a. Copy the ASMCDSTX job from the *dsnpref.NMC0.CC17SAMP* library to the *dsnpref.NMC0.rname.JCL* library.
  - b. Customize the ASMCDSTX job in the *dsnpref.NMC0.rname.JCL* library, following the instructions provided by the comments in the file.
  - c. Submit the customized job to assemble and link edit the exit.
7. Change the value of the CONNECT:Direct initialization parameter, STATISTICS.EXIT, to NMCDSTEX.

NMCDSTEX is the default statistics exit name. If you assemble and link edit the exit manually, the statistics exit name you specify must match the exit name specified in the ASMCDSTX job.

### Example: One Region

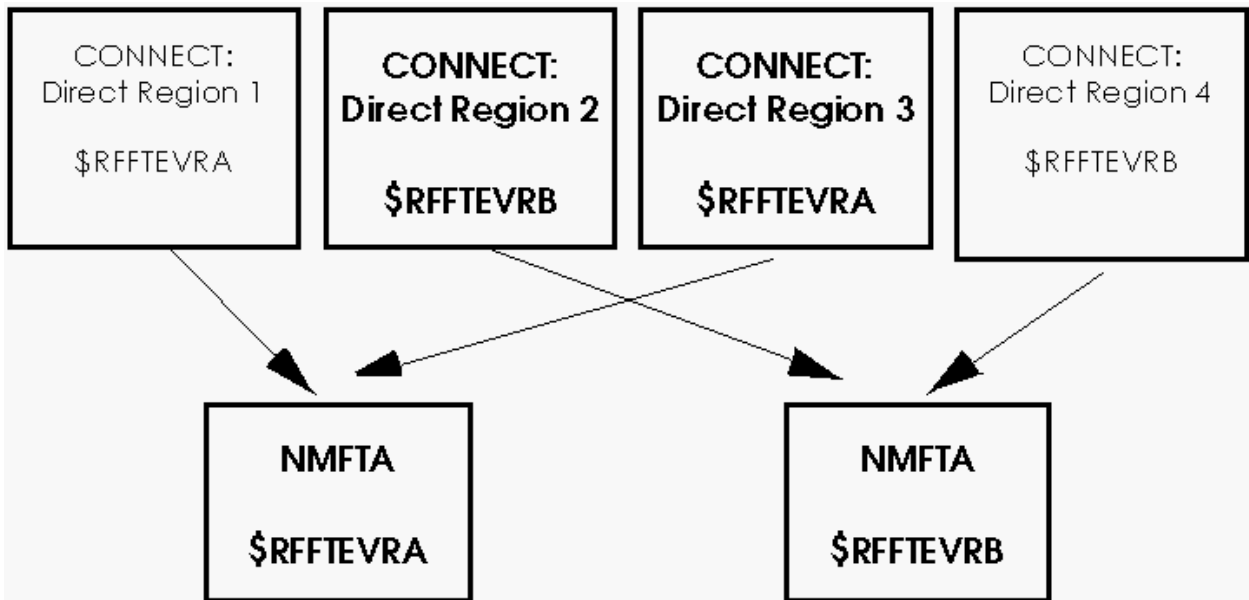
In this example, there is only one product region (NMFTA) within one LPAR. The event receiver ID in the CDAPI parameter group of NMFTA is configured with a value (\$RFFTEVR). Usually, all the CONNECT:Direct regions in the LPAR are configured with the same event receiver ID in their statistics exits so that region NMFTA can monitor them.



### Example: Multiple Regions

In this example, there are two product regions (NMFTA and NMFTB) within one LPAR. The event receiver ID in the CDAPI parameter group of NMFTA is configured with \$RFFTEVRA and NMFTB is configured with \$RFFTEVRB.

The scope of monitoring for each FT region will be configured according to the definitions of the event receiver ID in the statistics exits of individual CONNECT:Direct regions. In this example, NMFTA will monitor CONNECT:Direct Region 1 and CONNECT:Direct Region 3 while NMFTB will monitor CONNECT:Direct Region 2 and CONNECT:Direct Region 4.



## Customize CONNECT:Direct Initialization Parameters

Your product region uses the CONNECT:Direct interface program DMCHLAPI to interface with a CONNECT:Direct region and must sign on to that region. Because CONNECT:Direct places limits on the number of batch users that can be signed on concurrently, you should increase this limit to let the extra users sign on.

### To customize each managed CONNECT:Direct region

1. Increase the value of the MAXBATCH or the MAXUSERS initialization parameter as follows:
  - If the current value of MAXBATCH is zero, add 1 to the value of MAXUSERS.
  - If the current value of MAXBATCH is *not* zero, add 1 to the value of MAXBATCH.
2. Ensure that MCS.SIGNON is specified in the initialization parameters.
3. Ensure that the CONNECT:Direct startup JCL procedure and the STATISTICS.EXIT initialization parameter are updated.
4. Restart the CONNECT:Direct region.

## Define the Region as CONNECT:Direct User

You can use this procedure to enable the product region to execute commands in the managed CONNECT:Direct regions.

### To define the region as a CONNECT:Direct user

1. Define this product as a user in each of the CONNECT:Direct regions.
2. Ensure that the defined user is authorized for the following functions:
  - Change, delete, flush, select, and suspend processes
  - Selecting the network map
  - Other functions that you want to be able to perform from the region

For example, with CONNECT:Direct for MVS or CONNECT:Direct for OS/390, you can use the following suggestion when specifying the authority of a user:

```
CHANGE=Y  
DELPR=Y  
FLUSH=Y  
SELNET=Y  
SELPR=Y  
SELSTAT=Y  
SUBMITTER.CMDS=(Y Y Y Y Y)
```

**Note:** For more information about how to specify the authority of a CONNECT:Direct user, see the *CONNECT:Direct for MVS Installation and Administration Guide* or the *CONNECT:Direct for OS/390 Installation and Administration Guide*.

## Customize Managed CONNECT:Mailbox Regions

You can use this procedure to implement the flow of CONNECT:Mailbox events.

### To customize a managed CONNECT:Mailbox region

1. Include the supplied APF-authorized CC2DLOAD library in the STEPLIB DD statements of the CONNECT:Mailbox startup JCL procedure. (The library is set up as *dsnpref.NMC0.CC2DLOAD*.)
2. Update the following statements in the *dsnpref.NMC0.CC17SAMP(NMCMLGEX)* log exit:
  - `USREXIT=userexit`—if you are using an existing log exit.
  - `EPSRCVR=newid`—if the default EPS receiver ID is not suitable. Ensure that the value of the EPSRCVR parameter matches the CONNECT:Mailbox event receiver ID specified in the CMAPI parameter group of CA NetMaster FTM.

**Important!** If modifications are required, we recommend that you create an SMP/E ++USERMOD to record and control the changes, and then copy the member to TESTEXEC. Alternatively, you can copy the distributed member to the region's TESTEXEC data set for modification.

3. If you updated the copy of NMCMLGEX in TESTEXEC, do the following steps:
  - a. Copy the ASMCMLGX job from the *dsnpref.NMC0.CC17SAMP* library to the *dsnpref.NMC0.rname.JCL* library.
  - b. Customize the ASMCMLGX job in the *dsnpref.NMC0.rname.JCL* library, following the instructions provided by the comments in the file.
  - c. Submit the customized job to assemble and link edit the exit.
4. Specify the following OPTIONS definitions in the CONNECT:Mailbox ODF file:

```
MODIFY=RESP  
XLOG=NMCLGEX
```

NMCMLGEX is the default log exit. If you assemble and link edit the exit manually, the log exit name you specify in the ODF file must match the exit name specified in the ASMCMLGX job.



## How to Set Up SAF Access for TCPAccess Policy Rule Sets

**Note:** This section applies only if you use CA TCPAccess FTP Server.

To maintain policy rule sets, the user ID attempting to update the rule set must be associated with a new SAF facility, `$SOLVE.FTP.CONTROL`, that must be defined to your security system.

The user's access to this facility determines the user's access to policy rule sets as follows:

- Read access allows the user to view policy rule sets.
- Update access allows the user to both view and maintain policy rule sets.

The following sequence of events illustrates how the facility and a user ID are associated:

1. You define user `FTPUSER` to your security system.
2. You define a SAF facility to your security system.
3. You associate user `FTPUSER` to the SAF facility and give the user update access.
4. When `FTPUSER` user accesses the FTP policy rule set list panel a SAF call is made to ensure that `FTPUSER` has access to the `$SOLVE.FTP.CONTROL` facility and then to determine the authority of the user. In this example, the user has update authority.

## How to Define `$SOLVE.FTP.CONTROL` to Your Security System

The steps to define `$SOLVE.FTP.CONTROL` depend on your security system. They are described in the sections that follow.

## Define \$SOLVE.FTP.CONTROL to CA ACF2

To define \$SOLVE.FTP.CONTROL to CA ACF2 for z/OS, compile the following rule to authorize users to maintain policy rules:

```
ACF
COMP *
$KEY($SOLVE.FTP.CONTROL) TYPE(FAC)
  UID(uid_string) SERVICE(UPDATE) ALLOW

STORE
END
```

**Note:** Rule lines after the \$KEY line must be in column 2. If you compile this rule in TSO, you must enter a blank line after the last rule line entry and before the STORE command.

## Define \$SOLVE.FTP.CONTROL to CA Top Secret

Use this procedure to define \$SOLVE.FTP.CONTROL to CA Top Secret for z/OS.

### To define \$SOLVE.FTP.CONTROL to CA Top Secret for z/OS

1. To define ownership of the SAF facility, enter the following command:

```
TSS ADD(department-id) IBMFAC($SOLVE.FTP.CONTROL)
```

2. To allow access to policy maintenance functions, enter the following command:

```
TSS PER(userid) IBMFAC($SOLVE.FTP.CONTROL)
ACC(WRITE)
```

## Define \$SOLVE.FTP.CONTROL to RACF

Define \$SOLVE.FTP.CONTROL to RACF by issuing the following command:

```
RDEFINE FACILITY $SOLVE.FTP.CONTROL UACC(NONE)
PE $SOLVE.FTP.CONTROL CLASS(FACILITY) ID(userid or group)
ACCESS(UPDATE)
SETROPTS GENERIC(FACILITY) REFRESH
```

# Chapter 11: Preparing to Start Your Product

---

This chapter describes the tasks needed before CA NetMaster FTM can be started and used.

**Note:** The Install Utility places SYSIN members and parameter members in a default data set. If you move these members to a more secure data set, you must update the started task JCL to point to the new data set.

This section contains the following topics:

[Started Task JCL Setup](#) (see page 235)  
[Subsystem Identifier Setup](#) (see page 240)  
[Load Libraries](#) (see page 240)  
[Assign Consoles](#) (see page 241)  
[Activate VTAM Applications](#) (see page 242)  
[Enable Auditing by CA Auditor](#) (see page 242)

The Install Utility places RUNSYSIN (for the product region) in a default data set. If you move this member to a more secure data set, you must update the started task JCL to point to the new data set.

## Started Task JCL Setup

The Install Utility places the following SYSIN and parameter members into default data sets:

- SSIPARMS and SSISYSIN—for SOLVE SSI
- RUNSYSIN—for the product region
- FTPPARMS and FTPSYSIN—for NMFTP Monitor

If you move these members into a more secure data set, update the started task JCL and SYSIN members to point to the new data set.

## TESTEXEC Data Set

The install utility populates the TESTEXEC data set based on the values entered during the installation and setup process.

Review the members in TESTEXEC to:

- Ensure that they meet your site-specific requirements
- Reapply any previous customization that is still required

Review the following members in *dsnpref.rname*.TESTEXEC:

### **NMREADY**

Is the NCL procedure that is executed as part of system initialization after the VTAM ACBs have been opened successfully.

### **NMINIT**

Is the NCL procedure that is executed as part of system initialization before the VTAM ACBs are opened.

Do not:

- Code any SYSPARMS commands in the NMINIT or NMREADY procedures.
- Activate or modify links, or use commands such as DEFLINK, DEFTRANS, and ISR in NMINIT or NMREADY. In a multisystem network, the region uses link definitions during initialization. Defining DEFLINK, DEFTRANS, and ISR in these procedures can interfere with region linkage.

## Started Task Product Region Parameter Member

The Install Utility generates the RUNSYSIN member based on the values entered during the installation and setup process.

RUNSYSIN specifies the product region parameters.

Review RUNSYSIN to:

- Ensure that it meets your site-specific requirements
- Reapply any previous customization that is still required

If you have set SUBS=YES in the member, you can update the RUNSYSIN started task members to use z/OS static system symbols. This assists in planning future deployment.

Review the following parameters in *dsnpref.rname*.TESTEXEC(RUNSYSIN):

### **PPREF='XOPT=SDUMP'**

Specifies that ABEND dumps are written to the SYS1.DUMP data set.

If you do not want SYS1.DUMP data sets for dumps, remove the parameter and add the SYSDUMP DD statement to the generated task in *dsnpref.NMCO.rname*.JCL(*rname*).

### **PPREF='INIFILE=??????'**

Specifies the INI file used for parameter customizations.

To use a migrated INI file, uncomment the parameter and replace the question marks with the name of the INI file.

## SOLVE SSI Started Task Parameter Member

The Install Utility generates the SSIPARM member based on the values entered during the installation and setup process.

SSIPARM specifies the SOLVE SSI started task parameters.

Review the SSIPARM member:

- Ensure that the member meets your site-specific requirements
- Reapply any previous customization that is still required

Review the following members in *dsnpref.NMC0.SSIPARM*:

### **SSISYSIN**

(Optional) (If you are using an existing shared SOLVE SSI region, you do not have to review this member.)

If SUBS=YES is set, you can update the SSISYSIN started task member to use z/OS static system symbols. System symbols assist in planning future deployment.

### **SSIPARMS**

(Optional) (If you are using an existing shared SOLVE SSI region, you do not have to review this member.)

This member is present only if you created it when you specified the SOLVE SSI region.

Parameters can be shared with any other products using this SOLVE SSI. Review these parameters, and ensure that they are set correctly for the products (these parameters can be in SSISYSIN or SSIPARMS).

**Note:** For more information about sharing a SOLVE SSI, see the *SOLVE Subsystem Interface Guide*.

## Review and Copy the Product Region Started Task

The Install Utility generates a product region started task that you must review to ensure that it meets your site-specific requirements; if necessary, reapply any previous customization that is still required.

Use this procedure to review, update, and copy the started task to a procedure library.

**Note:** To assist you in planning future deployment, you can update the product region started task to use z/OS static system symbols.

### To review and copy the product region started task

1. In the product region started task member *dsnpref.NMC0.rname.JCL(rname)*, review and update the DD statements for your site-specific requirements.
2. In `CONNECT:Direct` for OS/390, ensure that the started task can access the `CONNECT:Direct` load library (for example, by having the library in the link list or by a `STEPLIB` DD statement in the started task member).
3. Copy the reviewed member to `SYSx.PROCLIB`.

## Review and Copy the SOLVE SSI Started Task

The Install Utility generates a SOLVE SSI started task that you must review to ensure that it meets your site-specific requirements; if necessary, reapply any previous customization that is still required.

**Note:** If you are using an existing shared SOLVE SSI region, skip this procedure.

Use this procedure to review, update, and copy the SOLVE SSI started task to a procedure library.

**Note:** To assist you in planning future deployment, you can update the SOLVE SSI started task to use z/OS static system symbols.

### To review and copy the SOLVE SSI started task

1. In the SOLVE SSI started task member *dsnpref.NMC0.ssiname.JCL(ssiname)*, review and update the DD statements for your site-specific requirements.
2. Copy the reviewed member to `SYSx.PROCLIB`.

## Review and Copy the NMFTP Monitor Started Task

**Note:** You do not need to perform this task if you did not [specify the NMFTP Monitor](#) (see page 207).

To assist you in planning future deployment, you can update the NMFTP Monitor started task to use MVS static system symbols.

### To review and copy the NMFTP Monitor started task

1. In the NMFTP Monitor started task member *dsnpref.NMCO.nmftname.JCL(nmftname)*, review and update the DD statements for your site-specific requirements.
2. Copy the reviewed member to SYSx.PROCLIB.

## Subsystem Identifier Setup

The setup of your product environment usually requires the following subsystem identifier (SSID) values that were defined during the [setup process](#) (see page 201):

- An SSID value for the subsystem identifier for the SOLVE SSI. The SOLVE SSI started task automatically identifies this SSID value to the system.
- An SSID value to enable the use of z/OS commands and messages. This SSID is called the AOM subsystem interface ID (AOM SSID). The product region started task automatically identifies this SSID value to the system.
- An SSID value for the subsystem identifier for the NMFTP Monitor. The NMFTP Monitor started task automatically identifies this SSID value to the system.

If you want the SSID values to be set permanently and available at system IPL time, you can set them in the SYS1.PARMLIB(IEFSSNxx) member. If you do this, ensure that you add the AOM SSID for the region first (after JES) in the list of subsystem names, because the first region listed in the SYS1.PARMLIB(IEFSSNxx) member controls the processing of messages by the subsystem interface.

## Load Libraries

Most products have their own load library but also require the load libraries of supporting services. The following load libraries must be APF-authorized:

- CC2DLOAD
- CC22DPLD (If SSL is installed)



## Authorization of the Load Libraries

To APF-authorize your load libraries, add the run-time load libraries to the SYS1.PARMLIB(IEAAPFxx) APF list.

To dynamically APF-authorize the load libraries, issue the following z/OS command:

```
SETPROG APF,ADD,DSNAME=?loadlib,VOLUME=?volser
```

### **?loadlib**

Specifies the name of the load library.

### **?volser**

Specifies its volume serial number.

## Assign Consoles

Your product needs a pool of consoles (either JES or extended MCS consoles) to issue system commands. As delivered, this product uses extended MCS consoles that are dynamically defined.

To use JES consoles instead of the default MCS consoles, define at least six consoles that are *not* used by other products.

### **To assign consoles**

1. Open the SYS1.PARMLIB(CONSOLxx) member.
2. Add the following statement for each console you want to define:

```
CONSOLE DEVNUM(SUBSYSTEM)...
```

An IPL is required to activate the updated CONSOLxx member. To start using JES consoles, you must also update the \$RM CONSOLES [Customizer parameter group](#) (see page 253).

## Activate VTAM Applications

You must activate VTAM applications for your regions. The Create VTAM Definitions and Tables facility builds a VTAM major node that contains APPL definitions for all product regions. The member V01LDVTM copies *vtamname* to SYS1.VTAMLST, which is the VTAM library that contains all the major node and application definitions used by your product.

### To activate the VTAM applications

1. Add *vtamname* to the startup list in SYS1.VTAMLST(ATCCONxx).
2. Activate the VTAM major node by entering the following VTAM command:  
  
`V NET,ACT,ID=vtamname`
3. Check that all of the applications are defined to VTAM after the activation. To do this, display the major node by entering the following VTAM command:

`D NET,ID=vtamname,E`

## Enable Auditing by CA Auditor

If your auditors require CA Auditor or CA Common Inventory Service to have knowledge of this product running on your system, you must put a load module in your system link list.

To define the load module to the system link list, include the library *dsnpref.NMC0.CAILINK* in the system link list SYS1.PARMLIB(PROGxx), for example:

```
LNKLST ADD NAME(LNKLST00) DSNAME(dsnpref.NMC0.CAILINK)
```

**Note:** Common load modules are used for all CA Mainframe Network Management products. You only need to include one copy of this *dsnpref.NMC0.CAILINK* library in the system link list.

# Chapter 12: Performing Initial Migration

---

This chapter describes migration tasks to perform before you start your product region.

## **More information:**

[Migration Preparation](#) (see page 39)

This section contains the following topics:

[NPF and SAF Security Members](#) (see page 243)

[SYSPARMS Usage](#) (see page 243)

[\\$CACALL Changes](#) (see page 245)

**Note:** If you are migrating from a version earlier than r11, [contact Technical Support](#) (see page iv).

## NPF and SAF Security Members

The Install Utility generates Network Partitioning Facility (NPF) and System Authorization Facility (SAF) security members. If you have previously customized any of these security members, update the regenerated members with your changes.

**Note:** For information about security members, see the *Security Guide*.

## SYSPARMS Usage

**Note:** This section does not apply if you are migrating from r11.5, r11.6, or r11.7.

Consider the changes to the SYSPARMS command when you migrate your product.

## New Commands that Replace SYSPARMS Operands

The following SYSPARMS operands were replaced. You need to search for usage in your NCL procedures, including NMINIT and NMREADY, and replace as described in the following table.

Old Command	New Command
SYSPARMS APPLSTAT=xxxx	APPLSTAT APPL=xxxx
SHOW SYSPARMS APPLSTAT=xxxx	SHOW APPLSTAT APPL=xxxx
SYSPARMS MAIFPREF=xxxx	MAIFPREF POOL=xxxx
SHOW SYSPARMS=MAIFPREF	SHOW MAIFPREF=xxxx
	<b>Note:</b> MAI-FS pool names are set using the EXTAPPLPOOLS Customizer parameter group.
SYSPARMS MAPLOAD=xxxx	LOAD MAP=xxxx
SYSPARMS MAPDEL=xxxx	UNLOAD MAP=xxxx
SYSPARMS MAPRESET=xxxx	This command is obsolete. Use LOAD MAP=xxxx.
SYSPARMS MODLOAD=xxxx	LOAD MOD=xxxx
SYSPARMS MODDEL=xxxx	UNLOAD MOD=xxxx
SYSPARMS PRELOAD=xxxx	LOAD PROC=xxxx
SYSPARMS UNLOAD=xxxx	UNLOAD PROC=xxxx

**Note:** You must make these changes in NCL procedures that use these commands either natively, or by way of &INTCMD.

## Revised SHOW SYSPARMS Output

SHOW SYSPARMS output includes additional columns. Review any user NCL procedures that execute SHOW SYSPARMS using &INTCMD to take the additional columns into account.

## Amended SYSPARMS Operand Processing

By default, when a SYSPARMS operand is set by a Customizer parameter group, it can only be updated subsequently using Customizer and cannot be set using OCS, Command Entry, or an NCL procedure.

If your site uses NCL procedures that execute SYSPARMS commands (either natively or using &INTCMD), note them, and after you initialize a region, you can use the SHOW SYSPARMS command to display all SYSPARMS operand origins. Locate the SYSPARMS you previously noted and, if they are set by Customizer, remove these SYSPARMS operands from the NCL procedures.

**Note:** For more information, see the online help for message N12810.

## \$CACALL Changes

**Note:** This section does not apply if you are migrating from r11.5, r11.6, or r11.7.

The following functions were removed:

- ACTION=BUILD,CLASS=CFPATH
- MODE=BROWSE is not supported for ACTION=DISPLAY,CLASS=HELP

If you have any NCL procedures issuing \$CACALL, ensure that these functions are not used.



# Chapter 13: Starting Up

---

This chapter describes how to start up your regions and log on to your product for the first time.

This section contains the following topics:

- [Start the SOLVE SSI Region](#) (see page 247)
- [Restart the SOLVE SSI Region](#) (see page 248)
- [Start the Product Region](#) (see page 248)
- [Start the NMFTP Monitor Region](#) (see page 248)
- [Perform the Initial Logon](#) (see page 249)
- [Add the Initial Administrator User ID](#) (see page 249)
- [Perform Subsequent Logon](#) (see page 250)

**Note:** If you want to run other CA Mainframe Network Management products in this region, before proceeding, complete the tasks described in the *Installation Guide* for the other products.

## Start the SOLVE SSI Region

You only need to perform this procedure if you use a new SOLVE SSI region.

### Notes:

- If you are using an existing shared SOLVE SSI region and did not make any changes when [specifying the SOLVE SSI region](#) (see page 203), skip this procedure.
- If you are using an existing shared SOLVE SSI region and have made changes, skip this procedure and proceed to [restarting the SOLVE SSI region](#) (see page 248).

To start the SOLVE SSI region, issue the following command from the MVS console:

```
S ssiname
```

*ssiname* is the name you specified for the SOLVE SSI during the setup process.

To stop the SOLVE SSI started task, issue the following command from the MVS console:

```
F ssiname,FSTOP
```

**Note:** If you are using cross-memory services and the SOLVE SSI is terminated, the address space ID is not available until after the next IPL.

## Restart the SOLVE SSI Region

You only need to perform this procedure if you are using an existing shared SOLVE SSI region and made changes when [specifying the SOLVE SSI region](#) (see page 203).

### To restart the SOLVE SSI region

1. Stop the SOLVE SSI started task, issue the following command from the MVS console:

```
F ssiname,FSTOP
```

2. Start the SOLVE SSI region, issue the following command from the MVS console:

```
S ssiname
```

## Start the Product Region

To start the product region, issue the following command:

```
S rname
```

*rname* is the name you specified for the region during the setup process.

**Note:** To stop the started task, issue the following command from the MVS console:

```
F rname,FSTOP
```

## Start the NMFTP Monitor Region

To start the NMFTP Monitor, issue the following command from the MVS console:

```
S nmftname
```

*nmftname* is the name you specified for the NMFTP Monitor during the setup process.

**Note:** To stop the NMFTP Monitor started task, issue the following command from the MVS console:

```
F nmftname,FSTOP
```



## Perform the Initial Logon

**Note:** If your region is using an existing UAMS data set, you will already have an administrator user ID available for the region. You can use that ID to log on to the region.

### To perform the initial logon

1. Log on to the product region. You can use the VTAM logon command:

```
LOGON APPLID(priacbnm) or LOGON APPLID=priacbnm
```

*priacbnm* is the name of the primary VTAM ACB application nominated in the *PPREF='PRI=priacbnm'* command in *dsnpref.rname.TESTEXEC(RUNSYSIN)*.

The region logon panel appears.

2. Enter the user ID **INSTALL** and password **99999999**, and press Enter.

The UAMS : Primary Menu appears.

The INSTALL 99999999 is a special user ID and password combination that can be used once only, and is accepted if the USERID data set is empty. The only functions that the INSTALL user ID can perform are those associated with user ID maintenance.

## Add the Initial Administrator User ID

The only functions that the INSTALL user ID can perform are those associated with user ID maintenance. Therefore, you must add an initial administrator user ID.

**Note:** If you are using a full security exit, user authorities are not specified through UAMS. You must specify these authorities as structured fields in your security exit. For more information, see the *Security Guide*.

**To define an initial user with full authority to UAMS**

1. At the UAMS : Primary Menu, type the initial administrator user ID in the User field, **USER** in the Definition Type field, and select the **A – Add User Definition** option.

The UAMS : User Details panel appears.

2. Type the initial password and user details for this initial user ID.

**Important!** The user must change the password again at first logon.

3. Go to the UAMS definition panels and ensure that you give full authority to this initial user to perform future administration tasks. Set the following minimum values:

**User Authorities panel, page 2**

Authority Level: 255

APPC Access Key: ALL

APPC Access Lock: ALL

**Access Authorities panel, page 3**

Set all fields to Y.

**Network Management Details panel, page 7**

Set fields that correspond to the features your site has configured to Y or the maximum authority.

**AOM MVS Details panel, page 11**

Console Authority: M

**Print Services Manager Details panel, page 12**

For all fields, set the maximum authority (1 through 4).

**Report Writer Details panel, page 13**

For all fields, set the maximum authority (1 through 4).

4. Press F3.

The user definition is saved.

## Perform Subsequent Logon

You are now ready to log on to your product and begin using it as an authorized user.

### To log on to your product

1. Press F3 to log off the product region.
2. Log on using your new initial administrator user ID and password.
3. If necessary, change your password by typing **U.P**, confirm your change, and press F3 (File) to save the change.

#### Notes:

- If you set SEC=PARTSAF or SEC=NMSAF in the RUNSYSIN member, you are not required to change your password.
- (Optional) To enable users to logon to the product from TSO, add the:
  - *dsrefix*.NMC0.CC2DLMD0 data set to LINKLIST or STEPLIB concatenation for the appropriate TSO procedure
  - *dsrefix*.NMC0.CC2DSAMP data set to the SYSHELP concatenation for the appropriate TSO procedure



# Chapter 14: Customizing Your Product

---

This chapter describes how to customize your product.

**Note:** After completing the steps in this chapter, you can use product system variables and z/OS static system symbols to assist you in planning future deployment when configuring multiple regions, but you must generate an initialization (INI) file. For information about setting up the INI file, see the *Administration Guide*.

This section contains the following topics:

[Initial Customization Requirements](#) (see page 253)

[Web Browser Settings](#) (see page 258)

[Additional Parameter Groups](#) (see page 259)

[Define File Transfer Resources to Your Region](#) (see page 261)

[Define the Region as a CA SOLVE:FTS User](#) (see page 261)

[Initialization Failures](#) (see page 261)

[Perform Additional Customization](#) (see page 263)

## Initial Customization Requirements

You must set various parameters for your site-specific requirements. Use Customizer to review and update the parameter groups in your product region.

**Note:** Customizer is used to set the majority of your region parameters. If you need to permanently change any SYSPARMS values that are not handled by Customizer, [contact Technical Support](#) (see page iv).

**Important!** Setting certain SYSPARMS to values other than the defaults can render certain product features inoperable.

Customization can only be performed by a user with [UAMS maintenance authority](#) (see page 249). That user's UAMS definition should have an APPC Access Key and Lock value of ALL.

## Customizer Setup Types

From the Customizer : System Parameters panel, you can select the following options:

### **Fast Setup**

Customizes the required parameter groups and quickly implements your region. It provides default values wherever possible, but lets you review all the required parameter groups to ensure that they match your installation standards. You can customize other parameters at a later time.

**Note:** You must review all the parameter groups in this option for the region to become operational.

### **Custom Setup**

Customizes the required parameter groups and additional file and data set names, to bring the system operation closer to your installation standards. This option quickly implements your region and still lets you perform some extra customization. It provides some default values, lets you specify names for certain files and data sets, and lets you review the required parameter groups (which are highlighted).

### **Complete Setup**

Customizes all initialization and customization parameters.

## Customize Parameter Values

You can use the provided default values or customize the parameter values to suit your site's needs.

**Note:** All parameters have default values.

### To customize parameter values

1. Enter **U** beside the parameter group that you want to review, and make the necessary changes for your site.
2. Press F6 (Action) to apply the change immediately. You can view the results by pressing F5 (ILog).

**Note:** The F6 option is not available for some parameters.

3. Press F3 (File) to save your changes and indicate that you have reviewed the group.

The value you assign to a parameter is associated with one or more actions, such as setting SYSPARMS or allocating data sets. You can action some parameter groups as soon as you enter appropriate values on the parameter panel. However, when you change the value of some parameters, for example, MODS file names, these parameter values can only be actioned by restarting the product region.

**Note:** If you change a parameter, perform an action, and then cancel that action, the new value will be in effect for that action; but when you restart, the value will return to the last saved value. In addition, you can change a value and save it without actioning it to have it take effect on the next startup.

## Interrupted Customization

If you exit the customization process before reviewing all required parameter groups, you are presented with a confirmation panel. You can choose to log off and continue with the customization later. Alternatively, another authorized user can log on and complete the customization process. Users cannot access the region until all the required parameter groups have been reviewed.

## Update and Review the Fast Setup Customization Parameters

To begin the process of updating and reviewing the Fast Setup Customization parameters, select the Fast Setup Customization Parameters option. The Customizer : Fast Setup panel appears.

## Implement Operating System Identifiers Parameters

Use this procedure to implement the operating system identifiers.

### To implement the operating system identifiers parameters

1. Enter **U** beside the Operating System Identifiers parameter group.

The OPSYSIDS - Operating System Identifiers panel appears.

Complete the fields on this panel. If the system uses the JES3 job entry subsystem, ensure that information about the job entry subsystem is updated.

**Note:** Press F1 (Help) for more information.

2. Press F6 (Action) to action the entries.
3. Press F3 (File) to save your settings.

The Customizer : Fast Setup panel appears with the Reviewed column marked Yes for the operating system identifiers parameters.

## Implement File Transfer Mechanism Parameters

If you are licensed for CONNECT:Direct or CONNECT:Mailbox, the fast setup displays the following interface parameters:

- CDAPI—CONNECT:Direct
- CMAPI—CONNECT:Mailbox

### To implement the file transfer mechanism parameters

1. Enter **U** beside the required parameter group (either CDAPI or CMAPI). The selected panel appears.
2. Complete the fields on this panel. Press F1 (Help) for more information.
3. Press F6 (Action) to action the entries.
4. Press F3 (File) to save your settings.

The Customizer : Fast Setup panel appears with the Reviewed column marked Yes for each updated field.

5. Repeat these steps for the other parameter group.

## Implement the TCP/IP Sockets Interface Parameters

Use this procedure to enable TCP/IP support.

Access to sockets interfaces requires [UNIX System Services authorization](#) (see page 279) provided by an OMVS segment security definition.



**To implement the TCP/IP sockets interface parameters**

1. Enter **U** beside the TCP/IP Sockets Interface parameter group.  
The first SOCKETS - TCP/IP Sockets Interface panel appears.
2. Tab to the TCP/IP Software Type input field, and enter the required value.  
Only one type of TCP/IP software can be configured as the sockets interface in each region.
3. Complete the remaining fields on the first panel. For information about the fields, press F1 (Help).

The Inbound Connections Port field contains a default port number. If another region on this system is already using that number, tab to the field and change it.

**Important!** The port number must be unique on a system.

4. Press F8.  
The second panel for this parameter group appears.
5. Complete the fields on the panel. For information about the fields, press F1 (Help).

Specify the details of the TCP/IP software as follows:

- If you are using the IBM Communications Server, enter your TCPIP.DATA data set name in the TCPIP.DATA DSN field, and review the Domain Name Resolution fields.
- If you are using CA TCPaccess CS, tab to the CA TCPaccess CS SSID field and enter the required SSID. If you are unsure of the CA TCPaccess CS subsystem ID, access the CA TCPaccess CS startup procedure and check the value of the SSN parameter.

6. Press F6 (Action) to set the specified values and start the interface.
7. Press F3 (File) to save your settings.

The Customizer : Complete Setup panel appears with the TCP/IP Sockets Interface Reviewed field marked as YES.

8. Press F3 (Exit).

The Customizer : System Parameters panel appears.

## Implement the WebCenter Parameters

Use this procedure to implement access to the WebCenter interface.

### To implement the WebCenter parameters

1. Enter **U** beside the WebCenter Web Interface parameter group.  
The WEBCENTER - WebCenter Web Interface panel appears.
2. Tab to the Web Interface Port input field, and enter a unique value.
3. Complete the fields on the panel. For more information about the fields, press F1 (Help).
4. To use SSL to encrypt WebCenter traffic, press F11.  
The panel that sets SSL parameters appears.
5. When you have completed all the fields, press F6 (Action) to set the specified values.  
  
If you specified a WebCenter port number, note the generated WebCenter Access URL because you will need this to access your product region using WebCenter.
6. Press F3 (File) to save your settings.  
  
The Customizer : Fast Setup panel appears with the Reviewed column marked Yes for the WebCenter web interface parameters.
7. Press F3 (Exit).  
  
You are returned to the Customizer : System Parameters panel, and the WebCenter parameters are implemented.

## Web Browser Settings

If you are using WebCenter, ensure that all users do the following:

- Clear the cache of their web browser to prevent them from getting a mix of old and new web files.
- Disable pop-up blocker, or define WebCenter as an allowed website.

## Additional Parameter Groups

Depending on which product features you want to implement, you may want to review other parameter groups and add any values that you saved from your old product region.

You can review these parameter groups now or later, as follows:

- **Now**—Select the Complete Setup Customization Parameters option to list all parameter groups and review the relevant groups. When you complete the review, exit the list and the Customizer : System Parameters panel.
- **Later**—Exit the Customizer : System Parameters panel. (When you are ready to review these parameter groups, enter **/PARMS** to list the groups.)

**Note:** If you are using other file transfer products, you can review these parameter groups now using the Complete Setup Customization Parameters option, or review them later.

## Implement Additional File Transfer Mechanism Parameters

If you are using CA XCOM Data Transport or a file transfer application that interfaces with CA NetMaster FTM through the generic event API, you will need to review and update the appropriate parameter group:

- CA XCOM Data Transport interface parameters—XCAPI
- Generic API interface parameters—GEAPI

**Note:** You must reassemble your NMFT Generic Support API code if you use an IPv6 address as the source or target node address.

### To implement additional file transfer mechanism parameters

1. Enter **U** beside the required parameter group.  
The selected panel appears.
2. Complete the fields on this panel. Press F1 (Help) for more information.
3. Press F6 (Action) to action the entries.
4. Press F3 (File) to save your settings.  
The Customizer : Fast Setup panel appears with each updated field marked as YES.
5. Repeat these steps for the other parameter group.

**Note:** To set up a generic file transfer product to work with this product, see the *Administration Guide*.

## Customize Region for FTP Events

Use this procedure to enable the flow of FTP events to and the receipt of the events in your region.

### To customize your region for FTP events

1. Access the FTPCNTL parameter group.
2. To monitor the IBM FTP Server and CA TCPaccess FTP Server, do the following:
  - a. Ensure that you have prepared your TCP/IP interface for the IBM Communications Server or the [CA TCPaccess CS](#) (see page 219).  
The FTP event flow to the region is enabled.
  - b. In the For Non TCPaccess FTP Server section of the FTPCNTL parameter group, set the following:
    - Enable FTP Event Receiver = YES.
    - FTP Transfer ID = FTPXFER.
3. To monitor the CA TCPaccess FTP Server, in the For TCPaccess FTP Server section of the parameter group, set the following:
  - Enable FTP Event Receiver = YES.
  - Event Receiver ID = \$RFFTEVR.
  - Enable SSI Policy Monitoring = YES.
  - If you intend to use ReportCenter, set FTP Transfer ID to match the name of the FTP managed source.
4. Press F6 (Action).  
Your changes are implemented.

## Define File Transfer Resources to Your Region

This task partially builds your file transfer management environment.

If you are using this product for the first time, you should use the File Transfer Assisted Resource Definition Facility. The facility also provides default parameter values that determine how and when automation will operate.

### To define file transfer resources

1. At the AutoAssist Setup panel, enter **S** beside the File Transfer Assisted Resource Definition option.

The Assisted Resource Definition panel appears. (If you are using a model 2 terminal, press F8 to scroll forward to select the option.)

2. Define the file transfer resources.

**Note:** For more information about how to define resources, see the *Administration Guide*.

## Define the Region as a CA SOLVE:FTS User

You can enable the product region to execute commands in the managed CA SOLVE:FTS regions.

### To define a region as a CA SOLVE:FTS user

1. Define its BSYS background user in each of the CA SOLVE:FTS regions by copying its user ID definition, xxxxBSYS.
2. In the product region, enter CMD at a command prompt to access the Command Entry panel.
3. Enter SHOW USERS to list the users who are currently logged on to the region and find the ID of the BSYS background user.

## Initialization Failures

Fatal errors occur (for example, you are unable to log on) if either or both of the following are unavailable:

- Panel libraries
- MODS control files

## Resolve Initialization Failures

If you log on to a region where the initialization of a parameter group has failed, Customizer displays the System Initialization In Progress dialog. This dialog indicates progress and assists you with identifying and rectifying any problems by displaying the current initialization status and whether actions associated with parameter groups have failed.

### To resolve initialization failures

1. Enter **S** next to List Only Failed Parameters.
2. Enter **L** next to a failed parameter group to view its log and look for error messages.
3. Use the message help and the full activity log to determine the cause of the failure.
4. Make the necessary changes to the parameter group and press F6.  
The parameter group changes are applied.
5. Press F3 to save the changes.

## Parameter Group Actions

You can apply the following actions to listed parameter groups:

- **S** or **B** (Browse) to browse parameter group details.
- **H** (Help) to view the help for a parameter group.
- **U** (Update) to update parameter group details.
- **AC** (Action) to action a parameter group.
- **L** (Log) to view the associated initialization and customization log.
- **I** (Ignore) to indicate to the system that it should ignore a failed parameter group, and proceed to run dependent parameter groups. This action is not available when initializing for the first time.

**Important!** Ignoring parameter groups is not recommended. Consider carefully before applying this action.

- **SD** (Set Default) to reset the parameter group values to the default values.

**Note:** Press F1 (Help) for more information.

An action can only be performed against an already completed parameter group or a failed parameter group.

When you correct an error by updating an incorrect parameter group record, you must action that parameter group before processing can continue (unless you apply the Ignore action). To action the parameter group, do *one* of the following:

- Press F6 (Action) when you finish updating the parameter group.
- Apply **AC** (Action) to the listed parameter group.

## Perform Additional Customization

You have now completed the initial customization tasks for your product.

There are many other ways that you can customize your product, and they are described in the *Administration Guide*.





# Chapter 15: Completing Migration

---

This chapter describes how to complete the migration process. It includes tasks that you perform after you start your r12 product region.

This section contains the following topics:

[NetMaster : Primary Menu](#) (see page 265)

[Knowledge Base Migration](#) (see page 266)

[MODS Migration](#) (see page 270)

[Panel Migration](#) (see page 271)

[OSCNTL File Migration](#) (see page 274)

[PSM Default Values Migration](#) (see page 274)

[Region Links to a Multisystem Network](#) (see page 274)

[Scenario: Run Your Old Region in Parallel with the New Region](#) (see page 278)

**Note:** If you are migrating from a version earlier than r11, [contact Technical Support](#) (see page iv).

## NetMaster : Primary Menu

The NetMaster : Primary Menu provides the expanded or collapsed menu options.

Each user can specify their own menu format and will be prompted until they have done so. To change the menu format, enter PROFILE in the Command field, as indicated by the prompt.

## Knowledge Base Migration

The knowledge base is where you store your resource definitions. System images, in which you define resources that are to be managed by a region, are part of the knowledge base.

**Note:** For more information about the knowledge base, see the *Reference Guide*.

As part of region setup, an r12 knowledge base is created, comprising the following data sets:

- RAMDB
- ICOPANL

Migrate any existing data that you want to keep to this knowledge base.

**Important!** The IDCAMS REPRO command must never be used to manage the definitions in the knowledge base.

**Note:** In r11.5, Graphical Monitor support was added to this product. If you are migrating from a prior release, and have created your own resource groups, ensure that they do not use the following names:

- ASMON
- CIP
- CIPRT
- CSM
- EE
- FT
- IPNDE
- NCPMN
- OSA
- ROUTR
- STACK
- TCPIP
- VIPA

## Migrate Your Existing Knowledge Base

If you are migrating multiple synchronized regions, you only need to perform this task for the first focal region. You do not have to perform this task when migrating subsequent regions because when you link the regions, the knowledge base is synchronized.

**Important!** Keep the old knowledge base until your r12 product regions are performing correctly.

### To migrate your existing knowledge base

1. Shut down the region using your existing knowledge base.
2. From the new product region, enter **/RAMUTIL.M**.  
The RAMDB Migration Utility panel appears.
3. Perform the following steps:
  - a. Specify the data set name for your existing RAMDB in the Old RAMDB Data Set Name field.  
The data set name is *dsnpref.rname*.RAMDB.
  - b. Specify **NO** in the Selective Migration field to migrate all definitions.  
The utility migrates only customized definitions from the old knowledge base to the knowledge base in the r12 product region. Definitions that are not migrated are listed for further action.
  - c. Press F6 (Action) to display the Migration Statistics panel.
4. After migration has completed, perform the following steps:
  - a. Look for the components that have a non-zero value in the Not Copied column. (The utility does not copy a component if the component already exists in the new knowledge base.)  
You might have customized some of these components and want to copy them.
  - b. Enter **R** beside the components that you want to copy, and copy the records.  
The copying options depend on whether a component contains [multiple objects](#) (see page 268), such as a system image, or is the [object itself](#) (see page 268), such as a user profile definition.
5. After you have copied the components, exit the migration utility.

**Note:** If you do not want to move directly from your established regions to r12 product regions, you can run the two releases in parallel.

## How to Copy Multi-Object Components

**Important!** The products use template images \$TEMPLAT 0001 through 0009 for the distribution of new and updated template definitions. Do not overwrite or replace them in the r12 knowledge base.

If a component contains multiple objects, you operate on the component as a whole. You can perform the following actions:

- Merge the component in the old knowledge base into the component in this knowledge base. Only objects that do not exist in this knowledge base are migrated. Existing objects are unchanged.
- Overwrite the existing objects in this knowledge base with the objects in the old knowledge base. This does not affect any objects that are not in the old knowledge base.
- Replace the component in this knowledge base with the component in the old knowledge base.

**Note:** To migrate specific objects, see the activity log and use the RMMUAD05 messages to determine which objects have not been copied. You can then delete the appropriate objects and redo the migration by merging (to list only the RMMUAD05 messages in the log, enter **TEXT RMMUAD05**).

## How to Copy Single-Object Components

For a component that is the object, do *one* of the following:

- Rename the component to create a copy of the component in this knowledge base using a different name.
- Overwrite the existing component in this knowledge base with the component in the old knowledge base.

## Apply Updated Templates

After you have migrated your knowledge base, review the r12 distributed templates.

**Note:** All templates were changed in r11, and some were changed in later releases. For more information about changes to the distributed knowledge base since r11.5, see *Reference Guide*.

**To apply updated templates**

1. Review the new templates to determine whether they are suitable for your requirements.
2. Enter **/RADMIN.T**.  
The Template Definition menu appears.
3. Select the appropriate option to list the definitions you want to review.
4. If you use any template image except the default (as specified in the OPSYSIDS parameter group), copy the required definitions to your working template images.

**Important!** When you copy definitions from the distributed template images to your working template images, you can replace your working definition with a distributed definition of the same name. If you want to retain your working definition, ensure that you make a copy of the definition beforehand.

If you want to copy all the new definitions, perform the following steps:

- a. Copy the template image (enter **/RADMIN.T.I**).
- b. Enter **C** beside the distributed image to merge the distributed template image with the target image.
- c. Specify **YES** in the Enter 'YES' to OVERLAY Like-named Components field.

If you want to copy changed definitions, you need to copy them one by one.

5. If you want to apply a new template to all the resource definitions (in one or more system images) that use it, use the **AP** (Apply Template) action code. Specify **RESET** and **REPLACE** to ensure that the template is applied in full. If you want to retain an old definition, ensure that you make a copy of the definition before you apply the template.

## Managed CONNECT:Direct Region

**Note:** This section does not apply if you are migrating from r11.5, r11.6, or r11.7.

To enable monitoring of the CONNECT:Direct statistic exit, reapply the CDMGR template to each of your managed CONNECT:Direct region CDMGR resources.

If you have a customized copy of the \$RFXPRMS NCL procedure (that is, if you do not use a CONNECT:Direct MCS user ID), you must also reapply your customized definitions.

**Important!** If modifications are required, we recommend that you create an SMP/E ++USERMOD to record and control the changes, and then copy the member to TESTEXEC. Alternatively, you can copy the distributed member to the region's TESTEXEC data set for modification.

**Note:** For more information, see the *Administration Guide*.

## Managed FTP Resources

**Note:** This section does not apply if you are migrating from r11.6 or r11.7.

The following templates has been updated to handle IPv6 support. Reapply the templates to each of your managed FTP resources.

- All FTPMGR templates
- REMOTENODE FTPMON template

# MODS Migration

**Note:** If you have not created your own MODS file, or individual MODS entities, do not perform this step.

## MODS File

The format of the MODS file is unchanged. If you have a MODS file containing only user-defined MODS entities that you want to keep, copy the entire file to the r12 file using the IDCAMS REPRO command.

**Note:** The allocation of MODS data sets is controlled by the MODSFILES parameter group in Customizer. For more information, enter **/PARMS** on any panel, select \$NM MODSFILES, and press F1 (Help).

## Copy MODS Definitions

The following entities are stored in the MODS file:

- Application definitions
- Command definitions
- Criteria definitions
- Help definitions
- List definitions
- Menu definitions
- Message definitions
- Print Services definitions
- Report definitions
- Table definitions

**Note:** Help alias entities are no longer supported. If you have installation-defined help aliases, convert them to a help page, and code the .cp macro to copy the original member. For more information about help macros, see the *Managed Object Development Services Programmer and Administrator Guide*.

**To copy MODS entities from your previous MODS file to your current one**

**Important!** Copy only installation-defined entities. Do not copy distributed entities.

1. Enter **/MODSADE** from any panel.  
The MODS : Entity Administration Menu appears.
2. Type **C** at the prompt, specify the information to copy your entities from the MODSUSR data set used by the old region to the MODSUSR data set used by this region, and press Enter.  
The MODS : Entity List panel appears.
3. Select the entities that you want to copy, and press Enter.

## Panel Migration

**Note:** If you have not created your own panel file, or individual panel entities, do not perform this step.

## Installation-Defined Panel Library

The format of the panel library is unchanged. If you have a panel library that contains only user-defined panel definitions that you want to keep, copy the entire file to the r12 file using the IDCAMS REPRO command.

**Note:** The allocation of panel data sets is controlled by the PANELLIBS parameter group in Customizer. For more information, enter **/PARMS** on any panel, select \$NM PANELLIBS, and press F1 (Help).

**Notes:**

- You do not need to migrate installation-defined icon panels in the ICOPANL file. These are recreated during the knowledge base migration.
- The allocation of panels data sets is controlled by the PANELLIBS parameter group in Customizer. For more information, enter **/PARMS** from any panel, select \$NM PANELLIBS, and press F1 (Help).

## Individual Panels

If you have installation-defined panel definitions in the same panel library as distributed panel definitions, you can copy the individual panel definitions to an r12 panel library.

**Important!** You should only copy installation-defined panel definitions. Do not copy distributed panel definitions.



## Copy Panel Definitions

You must copy the required panel definitions to the panel library in your r12 product region.

### To copy panel definitions

1. Define a temporary panel library for your old panels using the following steps:
  - a. Enter **/MODSAD.P.**  
The MODS : Panel Library Maintenance Menu appears.
  - b. Select **L - Library Definitions.**  
The MODS : Library Definition Menu appears.
  - c. Select **A - Allocate, Open, and Define Library** and specify a library name (for example, OLDPANLS) and the data set name where your old panels are located. Optionally, specify a description.  
A temporary panels library is defined.
  - d. Press F3 (Exit) to return to the MODS : Panel Library Maintenance Menu.
2. Copy the panels using the following steps:
  - a. Select **C - Copy Panel(s)** and specify the From library as the library name you just defined (for example OLDPANLS), and the To library as the target panels library name.  
If you leave the Panel Name field empty, the MODS : Panel Copy List appears, showing the panels in the From library.
  - b. Use the **C** (Copy) or **R** (Replace) action against the panels you want to copy. Press F1 (Help) for additional information.
  - c. When all requested panels have been copied, press F3 (Exit) to return to the MODS : Panel Library Maintenance Menu.
3. Delete the temporary panel library definition using the following steps:
  - a. Select **L - Library Definitions.**  
The MODS : Library Definition Menu appears.
  - b. Select **U - Remove Library Definition, Close and Unallocate** and specify the library name (for example OLDPANLS).  
The temporary panels library definition is removed.

**Note:** For more information about the MODS Panel Library Maintenance facility, see the *Managed Object Development Services Programming and Administrator Guide*.

## OSCNTL File Migration

The format of the OSCNTL file is unchanged. If your installation's existing OSCNTL file contains installation-defined ASN.1 maps, you must recompile them in the r12 product region.

Ensure the data set containing the map source is added to the COMMANDS concatenation in your new region. To compile a map, use the Compile Map option of Mapping Services. To access the Mapping Services Primary Menu, enter **/MAPMENU** from any panel.

**Note:** For more information about Mapping Services, see the *Managed Object Development Services Programming and Administration Guide*.

## PSM Default Values Migration

**Note:** This section does not apply if you are migrating from r11.5, r11.6, or r11.7.

When PSM Printer or Form definitions are added, some fields are primed from defaults stored in a Defaults record. PSM Defaults are customized using the PSMDEFAULTS Customizer parameter group.

If you did not amend the default values, there is no migration action. However, if you changed these values, review them in the PSMDEFAULTS parameter group and update as required.

Defaults that were previously set using /PSMADMN.UD are now set in Customizer. If you have changed your defaults using /PSMADMN.UD in previous releases, update your changes in the PSMDEFAULTS parameter group.

## Region Links to a Multisystem Network

If the region you are migrating is to be [synchronized with other regions](#) (see page 41), review the sections that follow.

**Important!** You must ensure that you unlink your existing region from the multisystem network before upgrading it to r12 and relinking it to the multisystem network.

## Important Considerations Prior to Linking

Consider the following before linking:

- The first region linked in migration mode must be used to perform all monitoring, command, and control functions across the entire multisystem environment.
- Migration mode does not support database synchronization between the old and new product regions. We recommend that you do not perform database maintenance while operating in migration mode.
- If database maintenance is unavoidable, changes should be made in an old region, and again in a new region so that all linked regions have the changes propagated to them.

## Link in Migration Mode

If this is the first product region to be migrated, you can link your new product regions to your existing product regions in migration mode.

Migration mode lets you migrate your existing product regions in an orderly fashion while maintaining visibility and control of your entire multisystem environment.

### Notes:

- Ensure the relevant maintenance has been applied to your product region, including checking [software requirements](#) (see page 17) and [multisystem network migration](#) (see page 42).
- If you have specified the NMSUP parameter in your existing product region's RUNSYSIN member, ensure that you specify this parameter in your new product region's RUNSYSIN member. The NMSUP parameter can be used to decrease the number of unique background user IDs that must be defined if you are using an external security package.

**Note:** For more information, see the *Security Guide*.

### To link in migration mode

1. Enter **=/MADMIN.MM** in the new product region.
2. Specify the name of an existing focal region in your multisystem network.
3. Press F6 (Action).

## Migrate Subsequent Regions

When a subsequent product region is migrated to r12, you can use this procedure to link it to the first r12 product region.

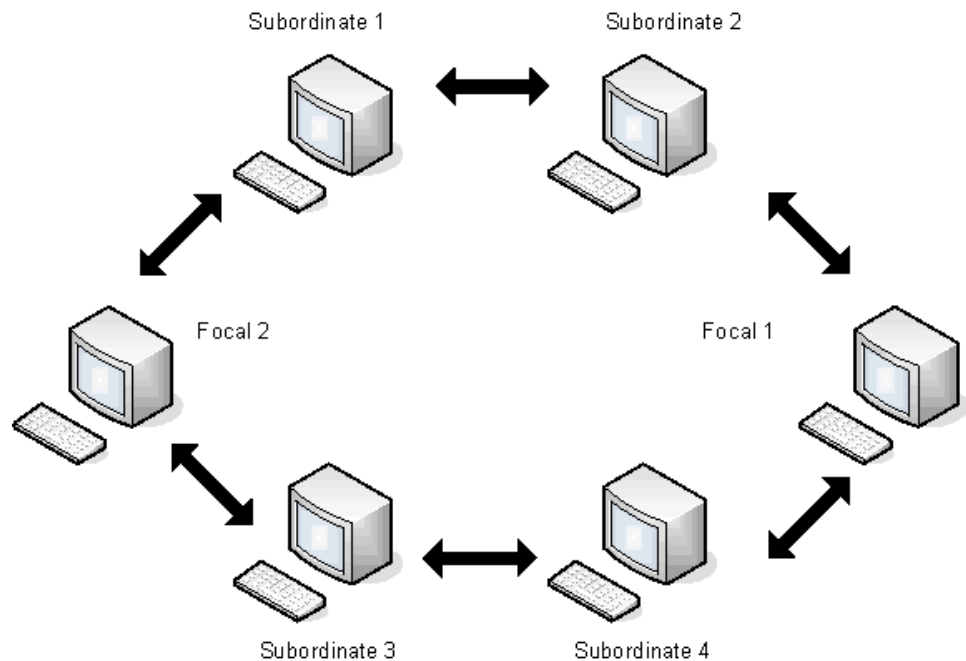
### To migrate subsequent regions

1. Enter **=/MADMIN.SD**.
2. Specify the first r12 product region as the remote region.
3. Specify the role for this region (focal or subordinate).
4. Press F6 (Action).
5. Repeat these steps for all of the remaining subordinate and focal regions.
6. Ensure that the final region you migrate is the focal region that you first linked using migration mode.

This ensures that the visibility to the multisystem network is retained throughout the migration process.

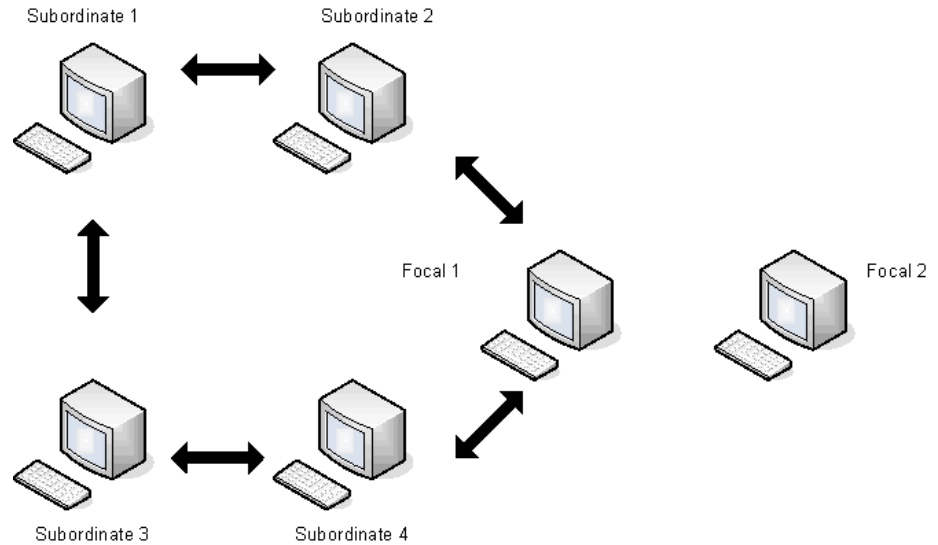
## Migrate a Multisystem Network

The following diagram shows a multisystem network with two focal regions and four subordinate regions:

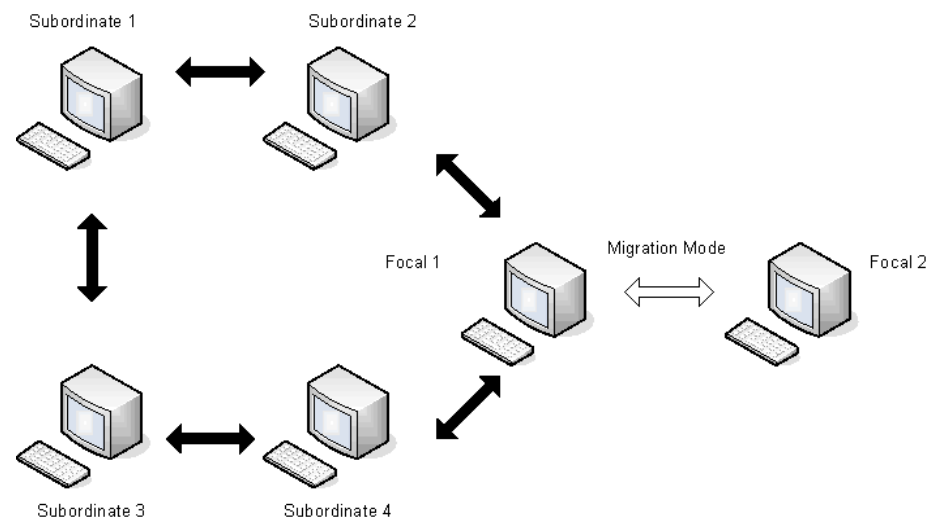


**To migrate a multisystem network**

1. Unlink Focal 2 from the existing multisystem network, as shown in the following diagram:

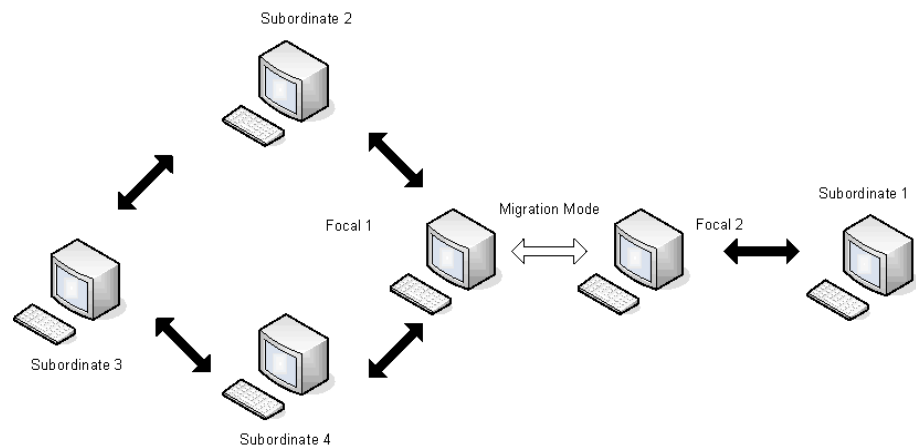


2. Upgrade Focal 2 to r12.
3. Link Focal 2 to Focal 1 in migration mode, as shown in the following diagram:



4. Unlink Subordinate 1 from the multisystem network and upgrade it to r12.

5. Link and synchronize Subordinate 1 to Focal 2, as shown in the following diagram:



6. Repeat Steps 4 and 5 for Subordinates 2-4 and Focal 1.

## Scenario: Run Your Old Region in Parallel with the New Region

If your existing region uses global mode AUTOMATED to perform desired state management, you can ease your r12 product regions into production as described in this section.

If you do not want to move directly from your existing regions to r12 regions, you can do the following:

1. Create an equivalent r12 region for each of your existing regions, so that you have a mirrored pair on each system.
2. Initially, have the existing region performing automation, and the r12 region running in the global mode of MANUAL (that is, merely monitoring) but using the same data.
3. Gradually, reverse the global mode of operation between the mirrored pairs, until r12 is performing automation in all regions.

This suggested scenario provides you with a hot backup, letting you instantly swap from an r12 region to the established region if you experience any problems. You can then correct the problem before swapping back to try r12 again.

# Appendix A: Defining UNIX System Services Authorization

---

This appendix describes how to authorize a user ID for UNIX System Services (USS).

This section contains the following topics:

[USS Authorization Requirements](#) (see page 279)

[Set Up OMVS Segment](#) (see page 279)

## USS Authorization Requirements

To complete this task you must have the following:

- Administrative access to your security package
- OMVS shell write privileges

To authorize a user, you can use one of the following:

- Default OMVS segment
- Specific OMVS segment

### More information:

[Define UNIX Authorization for Your Started Task User IDs](#) (see page 211)

## Set Up OMVS Segment

Use this procedure to set up an OMVS segment.

### To set up an OMVS segment

1. Choose an OMVS UID number to associate with each user ID. Your security administrator may have a policy for assigning OMVS UID numbers. If not, use a unique number.

**Note:** For more information about OMVS UID numbers, see IBM's *UNIX System Services Planning* guide.

2. Define the OMVS segment for the user. For a user ID *uuuuuuu* and UID number *nnn*, enter the following commands:

- For CA ACF2 for z/OS systems, enter the following commands:

```
SET PROFILE(USER) DIV(OMVS)
INSERT uuuuuuu UID(nnn) HOME(/) PROGRAM(/bin/sh)
```

- For CA Top Secret for z/OS systems, enter the following commands:

```
TSS ADD(uuuuuuu) HOME(/) OMVSPGM(/bin/sh) UID(nnn)
GROUP(OMVSGRP)
```

- For RACF systems, enter the following command:

```
ALU uuuuuuu OMVS(UID(nnn) HOME(/) PROGRAM(/bin/sh))
```

**Note:** The OMVS segment must contain the following:

- A home directory (HOME)
- A login shell (PROGRAM or OMVSPGM)

3. Ensure that you have completed this process for each user ID that you want to authorize. To confirm the contents of the OMVS segment enter the following commands:

- For CA ACF2 for z/OS systems, enter the following commands:

```
SET PROFILE(USER) DIV(OMVS)
LIST uuuuuu
```

- For CA Top Secret for z/OS systems, enter the following command:

```
TSS LIS(uuuuuu) DATA(ALL)
```

- For RACF systems, enter the following command:

```
LISTUSER uuuuuu OMVS NORACF
```

4. Choose a home directory to associate with each user ID, and ensure that it exists and that the UID has at least read access to it.

You can use the UNIX root directory (/) as shown in step 2, or you can use a customized home directory name.

For example, to set up a directory called /u/name for UID*nnn*, issue the following commands in the OMVS UNIX shell:

```
mkdir /u/name
chown nnn /u/name
chmod 777 /u/name
```

5. Confirm the owner and access to the directory by using the following command:

```
ls -ld /u/name
```

The following result appears:

```
drwxrwxrwx  2 user  group  8192 Sep  31 14:58 /u/name
```



6. If you have previously installed this product and have authorized the UNIX shell, remove the previous authorization by using the following command:

```
extattr -a/bin/sh
```



# Appendix B: Tape Format

---

This appendix provides information about the function modification identifiers (FMIDs) and details about the format of the tapes that you receive to install your product.

**Note:** The tapes contain all files for all products in the CA Mainframe Network Management family of products. Only some of the files apply to your product, and therefore, only the files necessary to install your product are unloaded.

This section contains the following topics:

[FMID Descriptions](#) (see page 283)

[Format of Cartridge VOLSER C2D66A](#) (see page 284)

[Format of Cartridge VOLSER C2D66B](#) (see page 285)

## FMID Descriptions

The sections in the remainder of this appendix reference the following FMIDs, which are codes that identify the release levels of a product:

### **CBT2C00**

Is the FMID for NetSpy SNA Services.

### **CC11C00**

Is the FMID for TCP/IP Services.

### **CC17C00**

Is the FMID for File Transfer Services.

### **CC18C00**

Is the FMID for SNA Automation Services.

### **CC2AC00**

Is the FMID for SNA Services.

### **CC2D66E**

Is the FMID for PDSE Services.

### **CC2D66H**

This is the FMID for Health Checker.

### **CC2D66R**

Is the FMID for ReportCenter.

**CC2D66S**

Is the FMID for WebCenter SDK.

**CC2D660**

Is the FMID for Management Services.

**CDEMC00**

Is the FMID for FTS Services.

## Format of Cartridge VOLSER C2D66A

This table lists the file sequence numbers, data set names, and data set contents for the first tape.

Files	DSN	Contents
1	CAI.SAMPJCL	Installation and maintenance JCL members
2	CAI.RESERVED.S002	Reserved for future use
3	CAI.HOLDDATA	SMP HOLDDATA
4–31	CAI.RESERVED.S004-S031	Reserved for future use
32	CAI.SMPMCS	Modification control statements (MCSs) containing functions and all published SYSMODs for those functions
33	CAI.CC2D66H.F1	JCLIN for CC2D66H
34	CAI.CC2D66H.F2	NCAL-linked MODS for CC2D66H
35	CAI.CC2D66H.F3	Installation and maintenance JCL members
36	CAI.CBT2C00.F1	JCLIN for CBT2C00
37	CAI.CBT2C00.F2	NCAL-linked MODS for CBT2C00
38	CAI.CBT2C00.F3	++MAC for CBT2C00 (RECFM=FB)
39	CAI.CBT2C00.F4	XML for CA MSM
40	CAI.CC11C00.F1	++MAC for CC11C00 (RECFM=FB)
41	CAI.CC11C00.F2	++DATA for CC11C00 (RECFM=VB)
42	CAI.CC11C00.F3	XML for CA MSM
43	CAI.CC17C00.F1	++MAC for CC17C00 (RECFM=FB)
44	CAI.CC17C00.F2	++DATA for CC17C00 (RECFM=VB)

45	CAI.CC17C00.F3	XML for CA MSM
46	CAI.CC2AC00.F1	++MAC for CC2AC00 (RECFM=FB)
47	CAI.CC2AC00.F2	++DATA for CC2AC00 (RECFM=VB)
48	CAI.CC2AC00.F3	XML for CA MSM
49	CAI.CC18C00.F1	++MAC for CC18C00 (RECFM=FB)
50	CAI.CC18C00.F2	++DATA for CC18C00 (RECFM=VB)
51	CAI.CC18C00.F3	XML for CA MSM
52	CAI.CDEMC00.F1	++MAC for CDEMC00 (RECFM=FB)
53	CAI.CDEMC00.F2	++DATA for CDEMC00 (RECFM=VB)
54	CAI.CDEMC00.F3	XML for CA MSM
55	CAI.CC2D66R.F1	++HFS for CC2D66R
56	CAI.CC2D66S.F1	++HFS for CC2D66S
57	CAI.CC2D66E.F1	JCLIN for CC2D66E
58	CAI.CC2D66E.F2	NCAL-linked MODS for CC2D66E

## Format of Cartridge VOLSER C2D66B

This table lists the file sequence numbers, data set names, and data set contents for the second tape.

Files	DSN	Contents
1-2	CAI.RESERVED.S001-S002	Reserved for future use
3	CAI.HOLDDATA	SMP HOLDDATA
4-31	CAI.RESERVED.S004-S031	Reserved for future use
32	CAI.SMPMCS	Modification control statements (MCSs) containing functions and all published SYSMODs for those functions
38	CAI.CC2D660.F1	JCLIN for CC2D660
39	CAI.CC2D660.F2	NCAL-linked MODS for CC2D660
40	CAI.CC2D660.F3	++MAC for CC2D660 (RECFM=FB)
41	CAI.CC2D660.F4	++DATA for CC2D660 (RECFM=VB)



# Index

---

## A

- access
  - login • 52
- acquiring the product • 14, 53
- acquisition
  - download • 44, 54
- add
  - custom data set • 123
  - data destination • 95
  - FTP Locations • 100
  - product • 122
  - system • 147
- aggregated package, viewing • 69
- allocate and mount • 157
- APF authorization • 241
- application names, VTAM • 242
- authorization • 84

## C

- CA Auditor, setting up • 242
- CA TCPaccess
  - subsystem ID • 256
- catalog, update • 53
- Communications Server, IBM
  - prefix.PW.SRC data set • 213
- completed deployment
  - remove • 120
- confirm deployment • 120
- connection awareness, enabling • 214
- consoles, assigning • 241
- contacting technical support • iv
- copy files to USS directory • 158, 159, 162
- create
  - data destination • 93
  - deployment • 106
  - methodology • 132
  - monoplex • 80
  - shared DASD cluster • 83
  - staging • 82
  - sysplex • 80
- CSIs (consolidated software inventories)
  - creation • 63
  - migration • 44
- custom data sets • 132
- Custom Data Sets

- add • 123
- edit • 128
- remove • 132
- customer support, contacting • iv
- Customizer parameter groups
  - OPSYSIDS • 256
  - SOCKETS • 256

## D

- data destinations
  - add • 95
  - create • 93
  - maintain • 96
- data set name mask • 135
- data sets
  - allocate region-specific (local) • 204
- default
  - data destination • 99
  - FTP Location • 102
- delete • 100
  - completed deployment • 120
  - data destination • 100
  - development • 119
  - product • 59
  - product gen level • 59
  - product release • 59
  - system registry • 92
- delivery, product acquisition • 14
- deployment
  - about • 105
  - confirm • 120
  - create • 106
  - delete • 119
  - How to Trace a Failed Deployment • 87
  - preview • 110
  - summary • 148
  - view • 113
- disk space requirements • 21
  - download • 54
  - download multiple • 56
  - maintenance packages, viewing status • 72
  - migration • 55
- distribution tape • 14
- download • 44, 54
  - files using ESD • 153
  - installation packages • 44, 54

---

- LMP keys • 64
- maintenance packages • 44, 66
- multiple installation packages • 56
- options • 158
- overview • 151
- to mainframe through a PC • 162
- using batch JCL • 159

## E

- edit
  - custom data set • 128
  - methodology • 144
- ESD (Electronic Software Delivery) • 14
  - space requirement • 21
- external HOLDDATA • 173
- external packages
  - installation • 57, 59
  - migration • 55, 68

## F

- file transfer mechanism parameters • 256
- FMIDs • 283
- free space • 156
- FTP Locations
  - edit • 101
  - FTP locations • 100
  - remove • 102
  - set default • 102
- FTP resource definitions • 270

## G

- gathering information in preparation for
  - installation and setup • 24
- GIMUNZIP utility • 164
- GROUPEXTEND mode • 73

## H

- hardware
  - security • 20
  - software • 17
  - storage • 21
- hash setting • 164
- high-level qualifier • 164
- HOLDDATA • 173
  - external • 173
  - internal • 173
- How to Trace a Failed Deployment • 87

## I

- IBM Communications Server, TCPIP.DATA data set name • 256
- implementation
  - file transfer mechanism parameters • 256
  - operating system identifiers parameters • 256
  - TCP/IP sockets interface • 256
  - WebCenter parameters • 258
- initialization
  - failures • 262
  - INI file • 40
  - setup types • 254
- installation • 44, 59
  - generating install jobs • 167
  - JCL • 166, 167
  - required information • 24
  - setup process • 24
  - unloading installation software • 165, 183
- installation packages
  - download • 54
  - download multiple • 56
  - migration • 55
- installing
  - from Pax-Enhanced ESD • 151
  - from tape • 183
- Integrated Cryptographic Services Facility (ICSF) • 164
- internal HOLDDATA • 173

## J

- Java version support • 164
- JCL, installation • 166, 167

## K

- knowledge base
  - migrating • 266

## L

- LMP keys • 64
- load library authorization • 241

## M

- maintain
  - data destinations • 96
  - system registry • 84
- maintenance • 171
  - application • 44, 69



---

- applying directly to RAMDB • 177
- backing up RAMDB • 176
- backout • 76
- GROUPEXTEND mode • 73
- RAMDB • 176
- restoring RAMDB • 178
- SMP fixes • 171
- USERMODs • 72
- maintenance packages
  - backout • 76
  - download • 44, 66
  - installation • 44, 69, 72
  - maintenance packages, viewing status • 72
  - migration • 68
  - USERMODs • 72
- menu format • 265
- methodology
  - create • 132
  - remove • 146
  - symbolics qualifiers • 135
- migrations
  - INI file • 40
  - installation packages • 55
  - knowledge base • 266
  - maintenance packages • 68
  - MODS • 270
  - OSCNTL file • 274
  - panels • 271
- MODS, migrating • 270
- monoplex
  - create • 80
- multi-object components • 268
- multiple product installation packages,
  - download • 56

## N

- nested packages • 69
- NPF member, reviewing • 243

## O

- operating system identifiers parameters • 256
- OPSYSIDS parameter group • 256
- OSCNTL file, migrating • 274

## P

- panels, migrating • 271
- parallel, running regions in parallel • 278
- parameters
  - file transfer mechanism • 256

- operating system identifiers • 256
  - WebCenter • 258
- partitioned data sets, loading • 204
- pax ESD procedure
  - copy product files • 158
  - create product directory • 163
  - create product-specific directory • 164
  - download files • 153
  - set up USS directory • 156
- pax file
  - copy files to USS directory • 158, 159, 162
- port number • 256
- primary menu • 265
- process overview • 151
- product
  - acquisition • 14
- product download window • 153
- product regions
  - setup • 204
  - starting • 248
  - stopping • 248
- product-level directory • 163
- products
  - acquired externally • 57, 68
  - add • 122
  - download • 44, 54
  - download multiple • 56
  - installation • 44, 59
  - maintenance • 44, 69, 76
  - removal of • 59
  - remove • 123

## R

- RAMDB
  - maintenance • 177
- read me • 151, 164
- regions
  - product • 204
  - setup, product selection • 204
- Remote Credentials
  - add • 103
  - delete • 105
  - edit • 104
- remove
  - FTP Locations • 102
  - methodologies • 146
  - product • 123
  - system • 147
- restart SOLVE SSI region • 248

---

reviewing  
    NPF member • 243  
    SAF member • 243  
running regions in parallel • 278

## S

SAF member, reviewing • 243  
sample jobs • 159, 163  
    CAtoMainframe.txt • 159  
    Unpackage.txt • 163  
scenarios, usage • 44  
security  
    access, checking • 20  
    requirements • 20  
set default • 99  
setting up CA Auditor • 242  
setup  
    product regions • 204  
    subsystem identifiers • 240  
    subsystem interfaces • 203  
    types • 254  
sharing a SOLVE SSI region • 202  
single-object components • 268  
SMP fixes • 171  
SMP/E  
    GIMUNZIP utility • 164  
SNMP  
    agent • 213  
    collecting data from CA TCPaccess • 221  
    query engine • 213  
SOCKETS parameter group • 256  
software  
    inventory • 53  
software delivery • 14  
SOLVE SSI  
    as common component • 202  
    methods of specifying region • 202  
    sharing a region • 202  
    specifying • 203  
SOLVE SSI region  
    restarting • 248  
    starting • 247  
    stopping • 247  
start product region • 248  
start SOLVE SSI region • 247  
started task JCL • 235  
startup • 248  
stop product region • 248  
stop SOLVE SSI region • 247

storage requirements • 21  
subsystem identifiers, set up • 240  
subsystem interfaces, specify • 203  
support, contacting • iv  
symbolic qualifiers • 135  
system  
    add • 147  
    remove • 147  
system registry  
    about • 77  
    authorization • 84  
    create non-sysplex • 78  
    create, data destination • 93  
    create, shared DASD cluster • 83  
    create, staging • 82  
    create, sysplex • 80  
    delete • 92  
system symbols • 239, 253

## T

tape, installing from • 183  
TCP/IP interface, z/OS • 256  
technical support, contacting • iv

## U

UAMS  
    administrator, initial • 249  
UNIX System Services (USS)  
    access requirements • 151, 156  
    directory cleanup • 169  
    directory structure • 156  
    product directory cleanup • 169  
UNZIPJCL • 164  
updated templates, applying • 268  
usage • 44  
user IDs, adding • 249  
USERMODs • 72

## V

viewing  
    aggregated package • 69  
    deployment • 113  
viewing maintenance package status • 72  
VTAM  
    applications, defining • 242

## W

WebCenter  
    clearing the browser cache • 258

---

- parameters • 258
- port number, defining • 258
- third-party products recommended • 18
- worksheets • 24
  - installation information • 24
  - region setup information • 28

## Z

- z/OS environment, TCP/IP interface • 256