

# CA TPX™ Session Management

## Installation Guide

Release 5.3



Second Edition

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

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

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

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

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

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

The manufacturer of this Documentation is CA.

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

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

## CA Technologies Product References

This document references the following CA Technologies products:

- CA TPX™ Session Management (CA TPX)
- CA STX™ (CA STX)
- CA ACF2™ Security (CA ACF2)
- CA Top Secret® Security (CA Top Secret)
- CA IDMS™ Database (CA IDMS Database)
- CA IDMS™/DC Database (CA IDMS/DC Database)
- CA 7® Job Management (CA 7)
- CA Remote Console™ (CA Remote)
- CA TCPaccess™ Telnet Server (CA TCPaccess Telnet Server)
- CA Vman™ (CA Vman)
- CA Common Services™ Resource Initialization Manager (CAIRIM)
- CA MII Data Sharing (CA MII)
- CA Mainframe Software Manager (CA MSM)

# Contact CA Technologies

## Contact CA Support

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

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

## Providing Feedback About Product Documentation

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

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

# Contents

---

## Chapter 1: Overview 11

Audience .....	11
How the Installation Process Works.....	12

## Chapter 2: Preparing for Installation 13

CA Common Services Requirements .....	13
CA LMP .....	13
LMP Key Certificate .....	14
Specify the LMP Code .....	14
Other Requirements.....	15
Coupling Facility .....	16
Naming Conventions .....	16
How You Acquire the Product .....	16
Use CA MSM Method.....	16
Use ESD PAX Process.....	17
Concurrent Releases .....	17

## Chapter 3: Installing Your Product Using CA MSM 19

CA MSM Documentation.....	19
Getting Started Using CA MSM .....	20
How to Use CA MSM: Scenarios.....	20
Access CA MSM Using the Web-Based Interface .....	29
Acquiring Products .....	30
Update Software Catalog .....	30
Download Product Installation Package .....	31
Migrate Installation Packages Downloaded External to CA MSM .....	32
Add a Product.....	33
Installing Products .....	35
Install a Product .....	35
Create a CSI .....	38
Download LMP Keys.....	41
Maintaining Products .....	42
How to Apply Maintenance Packages .....	42
Download Product Maintenance Packages.....	43
Download Maintenance Packages for Old Product Releases and Service Packs .....	44
Manage Maintenance Downloaded External to CA MSM .....	45

---

Manage Maintenance .....	47
GROUPEXTEND Mode .....	51
Back Out Maintenance.....	55
Setting System Registry .....	56
View a System Registry .....	56
Create a Non-sysplex System .....	57
Create a Sysplex or Monoplex.....	58
Create a Shared DASD Cluster.....	59
Create a Staging System.....	60
Authorization .....	61
Change a System Registry .....	62
Maintain a System Registry using the List Option.....	68
Delete a System Registry.....	69
FTP Locations .....	69
Data Destinations.....	73
Remote Credentials.....	79
Deploying Products .....	81
Deployment Status.....	82
Creating Deployments.....	83
View a Deployment.....	88
Change Deployments .....	89
Delete a Deployment .....	95
Confirm a Deployment.....	96
Products .....	98
Custom Data Sets .....	100
Methodologies .....	107
Systems .....	124
Deployment Summary .....	126

## **Chapter 4: Installing Your Product from Pax-Enhanced ESD 129**

How to Install a Product Using Pax-Enhanced ESD .....	129
How the Pax-Enhanced ESD Download Works .....	131
ESD Product Download Window .....	131
USS Environment Setup .....	134
Allocate and Mount a File System.....	135
Copy the Product Pax Files into Your USS Directory .....	138
Download Using Batch JCL .....	139
Download Files to Mainframe through a PC.....	142
Create a Product Directory from the Pax File .....	143
Sample Job to Execute the Pax Command (Unpackage.txt) .....	144
Copy Installation Files to z/OS Data Sets.....	144

---

Customize the Installation JCL.....	146
Clean Up the USS Directory.....	146

## **Chapter 5: Installing Your Product From Tape** **149**

Gather Information .....	150
Copy the INSTALL Data Set.....	151
Access the Online Documentation .....	152
Customize the Installation JCL.....	152

## **Chapter 6: Configuring Your Product** **153**

Calculate VSAM Storage.....	153
Define APPL Statements.....	154
Copy the Logmode Tables .....	155
Copy the Startup Procedure.....	156
Authorize the Load Library.....	156
Authorize the Load Library Using IEAAPFxx Method .....	157
Authorize the Load Library Using PROGxx Method .....	157
Install Other Language Panels .....	157

## **Chapter 7: Starting Your Product** **159**

Issue Console Commands.....	159
Log On a Terminal to CA TPX.....	159
The Default Logo Panel .....	160
Sign On to CA TPX.....	161
Stop CA TPX .....	161

## **Chapter 8: Post-Installation Tasks** **163**

Use Authorized Path Facility .....	163
Define the Coupling Facility Structure.....	163
Enable the TCPaccess Telnet Server Interface .....	164
Customize the JCL .....	164
Activate the Feature.....	165
Define Administrators .....	165
Define System Options and Applications .....	165
Define Operator Capabilities.....	166
Define Users .....	166
Static Users.....	166
Dynamic Users.....	166
Allow Dynamic Users.....	167

---

Convert Dynamic Users to Static Users.....	167
Convert Users to a Different Type.....	167
Saved Dynamic Users .....	168
Write ACL/E Program .....	168
Set Up VSAM Sharing .....	168
Implement a Signon and Signoff Exit .....	169
MAIL and VIEW Files.....	169

## **Chapter 9: Migration Information** **171**

Migration from Releases Prior to r4.....	171
Coupling Facility System Managed Rebuild .....	171
Migration Checklist .....	171

## **Chapter 10: Frequently Asked Questions** **173**

FAQs .....	173
------------	-----

## **Appendix A: VSAM File Sharing Without CA-L-Serv** **175**

How It Works.....	175
Allow VSAM Sharing Without CA-L-Serv .....	176

## **Appendix B: VSAM File Sharing With CA-L-Serv** **177**

CA-L-Serv Benefits .....	177
File Sharing With CA-L-Serv .....	177
CA-L-Serv Cross-system Sharing.....	178
If CA-L-Serv Becomes Unavailable.....	178
How to Customize CA TPX.....	179
Omit DD Statements .....	179
Identify CA-L-Serv to CA TPX .....	179
Specify the DDname Prefix.....	179
Specify the ICSN .....	179
How to Customize CA-L-Serv for CA TPX.....	180
Specify the Files CA-L-Serv Manages.....	180
Specify the Disposition and Share Options .....	180
Propagate ENQs .....	181
Use Private Buffer Pools.....	181
Sample Members .....	182
Installation Checklist .....	182

---

<b>Appendix C: APPL Statements</b>	<b>185</b>
Primary APPL Statement .....	185
Rebind APPL Statement .....	185
APPL Statements for Shared Virtual Terminals .....	185
APPL Statements for Group Virtual Terminals .....	186
APPL Statements for Unique Virtual Terminals .....	186
APPL Statements for Application Passthrough Printing .....	187
APPL Statements for User Passthrough Printing .....	187
<b>Appendix D: Tape Contents</b>	<b>189</b>
Data Sets on the Product Tape .....	189
<b>Appendix E: Data Set Name Changes</b>	<b>191</b>
New Data Set Names .....	191
<b>Index</b>	<b>193</b>



# Chapter 1: Overview

---

CA TPX (Terminal Productivity Executive) is a VTAM session management tool that provides a consistent, secure point of entry to multiple, simultaneous mainframe applications. This chapter describes the audience for this guide and provides an overview of CA TPX functions.

CA TPX allows you to run multiple application sessions on a 3270-type terminal (real or emulated) in a VTAM environment. The product manages these sessions. As a user, you have simultaneous access to a number of applications and can toggle between application sessions without having to log off one application and log on to another. You can access all the applications you need from one physical terminal.

For users who access the mainframe through a PC-based 3270-type terminal emulator, the TCPAccess Telnet Server provides a fast, direct Telnet connection to CA TPX.

This section contains the following topics:

[Audience](#) (see page 11)

[How the Installation Process Works](#) (see page 12)

## Audience

The system programming group is usually responsible for software product installation and maintenance because of their SMP/E (System Modification Program Extended) knowledge. This guide assumes a working knowledge of the SMP/E facility and its processes.

This guide provides basic standalone SMP/E install and maintenance instructions. For the knowledgeable SMP/E user, there is enough information provided in this guide, and the generated JCL and control statements, to allow integration with any site-specific SMP/E standards. For the SMP/E novice, this guide should provide enough of the basic information and concepts you need to complete the basic SMP/E installation process.

## How the Installation Process Works

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

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

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

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

To install your product, do the following tasks:

1. Prepare for the installation by [confirming that your site meets all installation requirements](#) (see page 13).
2. Acquire the product using one of the following methods:
  - CA MSM
  - Pax-Enhanced Electronic Software Delivery (ESD)
  - Order a DVD.
3. Install the product based on your acquisition method.
4. Install the CA Common Services using the pax files that contain the CA Common Services you need at your site.

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

# Chapter 2: Preparing for Installation

---

This section describes what you need to know and do before you install the product.

This section contains the following topics:

[CA Common Services Requirements](#) (see page 13)

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

[How You Acquire the Product](#) (see page 16)

[Concurrent Releases](#) (see page 17)

## CA Common Services Requirements

CA TPX uses the CCS component CAIRIM, the Resource Initialization Manager, for product license authorization.

CAIRIM is a common component whose features and functions are shared by many CA z/OS products. This component prepares your operating system environment for your CA products and components and executes them.

CAIRIM routines are grouped under CA z/OS Dynamic Service Code S910. For further details about the features and associated utilities of CAIRIM, review the CCS for z/OS documentation.

## CA LMP

This product requires CA LMP (License Management Program) to initialize correctly. CA LMP also provides a standardized and automated approach to the tracking of licensed software.

CA LMP is provided as an integral part of CAIRIM. When a currently supported version of CAIRIM has been installed, assistance is available to you for all CA LMP-supported products.

## LMP Key Certificate

Examine the CA LMP Key Certificate you received with your installation or maintenance tape. Your certificate contains the following information:

Term	Definition
Product Name	The trademarked or registered name of CA TPX as licensed for the designated site and CPUs.
Product code	The two-character code that corresponds to the CA TPX product.
Supplement	The reference number of your license for the particular product facility in the format: <i>nnnnnn - nnn</i> This format differs slightly inside and outside North America, and in some cases can not be provided.
CPU ID	The code that identifies the specific CPU for which installation of this product is valid.
Execution Key	An encrypted code required by CA LMP for product installation. During installation, it is referred to as the "LMP Code."
Technical Contact	The name of the designated technical contact at your site responsible for installation and maintenance of this product. CA addresses all CA LMP correspondence to this person.
MIS Director	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, you should supply the actual name when correcting and verifying the certificate.
CPU Location	The address of the building in which the CPU is installed.

## Specify the LMP Code

You must add the CA LMP Execution Key provided on the Key Certificate to the CAIRIM parameters to ensure proper initialization of this product.

To define a CA LMP Execution Key to the CAIRIM parameters, modify member KEYS in CAI.PPOPTION.

The statement structure for member KEYS is:

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

## CAIRIM Parameters

The CAIRIM parameter definitions are:

Parameter	Definition
<i>pp</i>	The two-character product code. This code agrees with the product code already in use by the CAIRIM initialization parameters for any earlier versions of this product (if applicable). This is required.
<i>ddmmmyy</i>	The CA LMP licensing agreement expiration date.
<i>ttt-mmmm</i>	The CPU type and model on which CA LMP is to run (for example, 3090-600). If the CPU type, model, or both require less than four characters, blank spaces are inserted for the unused characters. This is required.
<i>ssssss</i>	The serial number of the CPU on which CA LMP is to run. This is required.
<i>kkkkkkkkkkkkkkkk</i>	The execution key needed to run CA LMP. This CA LMP execution key is provided on the Key Certificate shipped with each CA LMP software solution.

Following is an example of a control statement for the CA LMP execution software parameter. The product code and execution key value will be different when you install this product at your site.

```
PROD(1B) DATE (27JUN03) CPU(3090-600 /370623)
LMPCODE(52H2K06130Z7RZD6)
```

For more information regarding the CA Common Services CAIRIM and its CA-LMP facility, see the *CA Common Services for z/OS Administration Guide*.

## Other Requirements

The installation procedure involves loading the CA TPX installation data sets from the distribution media and customizing statements in these data sets for your site.

The administration facility, required for performing online administration, is installed automatically when you install this product.

## Coupling Facility

Optionally define the Coupling Facility structure for use by CA TPX in the z/OS policy data set. This is required if multiple instances of CA TPX are to operate as a single VTAM generic resource.

## Naming Conventions

The INSTALL data set that you use to install this product uses PREFIX execution parameters to set the values of the prefixes used in data set names. If you choose to change this value, make sure you change it consistently throughout the installation procedure, and check that all parameters in the INSTALL data sets conform to the conventions at your site.

The examples in this guide use the original values for the application name, TPX. If you assign a different name, make appropriate changes consistently throughout the installation procedure.

## How You Acquire the Product

You can acquire the product using one of the following methods:

- Using CA Mainframe Software Manager (CA MSM), which is an application with a web-based user interface (UI) that helps you download, install, and maintain z/OS products, and provides a unified view of the products

**Note:** If you do not have the application, you can download it using Electronic Software Delivery (ESD). For more information about CA MSM, see the *CA Mainframe Software Manager Guide*.

- Using ESD, which lets you download the product from the Technical Support Download Center at CA Support Online

## Use CA MSM Method

CA MSM is an application with a web-based user interface (UI) that helps you download, SMP/E-install, and maintain CA products that run on z/OS. It also provides a unified view of CA products.

If you do not have the application, you can download it using Electronic Software Delivery (ESD).

**Note:** For more information about CA MSM, see the *CA Mainframe Software Manager Guide*. The CA MSM Web Online Interface tells you how to SMP/E-install CA Mainframe products.

After you use CA MSM to acquire and SMP/E-install CA TPX, proceed to [Calculate VSAM Storage](#) (see page 153) to continue with configuring CA TPX.

## Use ESD PAX Process

You can obtain CA TPX in a compressed format (pax.Z file) that enables you to install directly from DASD. This is known as the ESD PAX process.

### To install CA TPX using the ESD PAX process

1. Follow the procedures in the Electronic Software Delivery Downloading and Unpackaging CA Products. This guide tells you how to download the product pax.Z file and uncompress it into a number of CA TPX product distribution data sets on DASD.

The CA TPX product distribution data sets are available on your local DASD.

2. Continue with the product installation.

## Concurrent Releases

You can install this release of CA TPX and continue to use an older release in another SMP/E CSI environment. If you plan to continue to run a previous release, consider the following points:

- When installing into an existing SMP/E environment, this installation deletes previous releases in that environment.
- If you acquired your product from tape or with Pax-Enhanced ESD, select different target and distribution zones for your new release from where your current release is installed. The new zones use different libraries than your current release.

**Note:** CA MSM installs into a new CSI by default.

- Define DDDEF entries in your new zones to point SMP/E to the proper libraries for installation. Ensure that they point to the new release libraries.



# Chapter 3: Installing Your Product Using CA MSM

---

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

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

When you have completed the procedures in this section, go to [Configuring Your Product](#) (see page 153).

This section contains the following topics:

- [CA MSM Documentation](#) (see page 19)
- [Getting Started Using CA MSM](#) (see page 20)
- [Acquiring Products](#) (see page 30)
- [Installing Products](#) (see page 35)
- [Maintaining Products](#) (see page 42)
- [Setting System Registry](#) (see page 56)
- [Deploying Products](#) (see page 81)

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

## CA MSM Documentation

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

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

## Getting Started Using CA MSM

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

### How to Use CA MSM: Scenarios

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

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

### How to Acquire a Product

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

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

**Follow these steps:**

1. Set up a CA Support Online account.

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

2. Determine the CA MSM URL for your site.

To [access CA MSM](#) (see page 29), you require its URL. You can get the URL from your site's CA MSM administrator and log in using your z/OS credentials. When you log in for the first time, you are prompted to create a CA MSM account with your credentials for [the CA Support Online website](#). This account enables you to download product packages.

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

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

If you cannot find the product you want to acquire, [update the catalog](#) (see page 30). CA MSM refreshes the catalog through [the CA Support Online website](#) using the site IDs associated with your credentials for [the CA Support Online website](#).

4. [Download the product installation packages](#) (see page 31).

After you find your product in the catalog, you can [download the product installation packages](#) (see page 31).

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

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

## How to Deploy a Product

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

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

### Follow these steps:

1. Set up the system registry:
  - a. Determine the systems you have at your enterprise.
  - b. Set up [remote credentials](#) (see page 79) for those systems.
  - c. Set up the target systems ([Non-Sysplex](#) (see page 57), [Sysplex or Monoplex](#) (see page 58), [Shared DASD Cluster](#) (see page 59), and [Staging](#) (see page 60)), and validate them.
  - d. [Add FTP](#) (see page 69) information, including data destination information, to each system registry entry.
2. Set up [methodologies](#) (see page 107).

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

After creating the deployment, you can save it and change it later by adding and editing [systems](#) (see page 124), [products](#) (see page 98), [custom data sets](#) (see page 100), and [methodologies](#) (see page 107), or you can deploy directly from the wizard.

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

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

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

## System Registration

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

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

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

1. Set up your remote credentials.

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

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

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

## 2. Set up your system registry.

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

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

### Non-Sysplex Systems

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

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

### Sysplex or Monoplex Systems

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

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

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

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

### Shared DASD Clusters

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

### Staging Systems

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

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

3. Define the FTP location information for every system.

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

To define the FTP location, provide the following:

#### URI

Specifies the host system name.

#### Port Number

Specifies the port number.

**Default:** 21.

#### Directory Path

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

4. Define a data destination for every system.

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

**FTP**

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

**Shared DASD**

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

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

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

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

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

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

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

5. Register each system by validating that it exists.

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

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

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

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

You are now ready to deploy your products.

## Deploying Products

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

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

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

### Deployment Name and Description

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

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

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

### CSI Selection

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

### Product Selection

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

### Custom Data Set

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

- For a z/OS data set, you need to provide a data set name that is the actual existing z/OS data set and a mask that names the data set on the target system. This mask may be set up using [symbolic qualifiers](#) (see page 111) 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 111) 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 101).

### Methodology

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

To [create a methodology](#) (see page 108), specify the following:

#### Data set name mask

Lets you choose symbolic variables that get resolved during deployment.

#### Disposition of the target data sets

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

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

#### Partitioned data set

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

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

#### Directory in a UNIX file system

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

### **Sequential data set or a file in the UNIX file system**

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

### **For a VSAM data set (cluster)**

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

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

### **System Selection**

Select the system for this deployment.

### **Preview**

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

Use this option to review your deployment before deploying.

### **Deploy**

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

### **Summary**

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

### **Confirm**

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

## How to Maintain Existing Products

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

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

### Follow these steps:

1. Migrate the CSI to CA MSM to maintain an existing CSI in CA MSM.  
During the migration, CA MSM stores information about the CSI in the database.
2. [Download the latest maintenance](#) (see page 43) 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 44).
3. [Apply the maintenance](#) (see page 47).

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

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

## Access CA MSM Using the Web-Based Interface

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

### Follow these steps:

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

3. Click New.

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

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

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

You are prompted to review your user settings.

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

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

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

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

## Acquiring Products

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

## Update Software Catalog

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

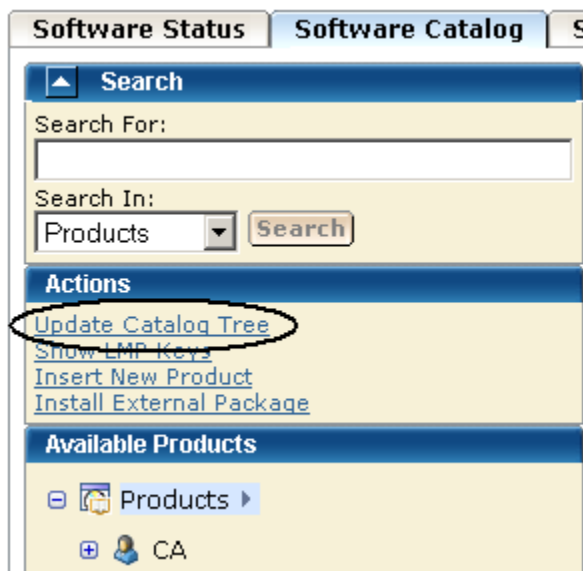
If you update the catalog tree and some changes are missing, check your user settings on [the CA Support Online website](#).

### Follow these steps:

1. Click the Software Catalog tab.

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

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



You are prompted to confirm the update.

- Click OK.

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

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

## Download Product Installation Package

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

### Follow these steps:

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

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

The product releases are listed.

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

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

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

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

The product packages are downloaded.

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

## Migrate Installation Packages Downloaded External to CA MSM

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

Migrating these packages to CA MSM provides a complete view of all your product releases. After a package is migrated, you can use CA MSM to [install the product](#) (see page 35).

### Follow these steps:

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

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

An entry is added for the product.

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

The packages for the gen level are listed.

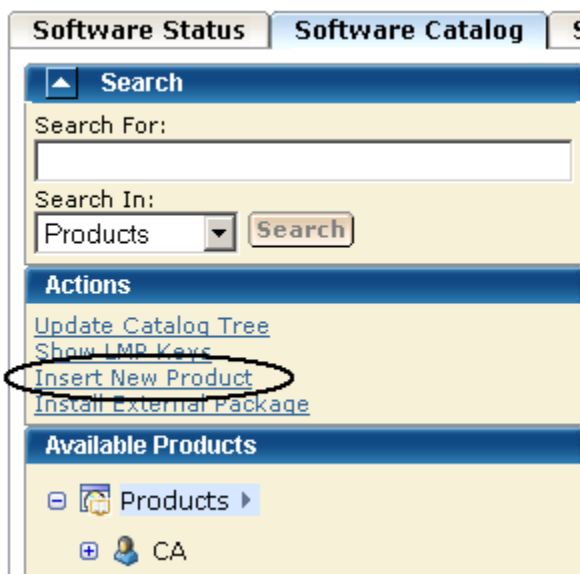
3. Click the Add External Package button.  
You are prompted to enter a path for the package.
  4. Specify the USS path to the package you want to migrate, and click OK.  
Information about the package is saved in the CA MSM database.
- Note:** To see the added package, refresh the page.

## Add a Product

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

### Follow these steps:

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



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

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

**Note:** To add several packages from the same location, use [masking](#) (see page 34).

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

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

## Masking for External Packages

Masking lets you add more than one [package](#) (see page 33) (or set of [maintenance files](#) (see page 45)) from the same location using a pattern (mask). You can use masking for components, maintenance in USS, and maintenance in data sets. You can use masking for files only, not for directories.

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

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

- For sequential data sets, use the following characters:

?

Match on a single character.

\*

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

\*\*

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

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

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

### Example 1

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

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

### Example 2

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

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

### Example 3

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

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

### Example 4

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

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

## Installing Products

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

### Install a Product

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

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

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

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

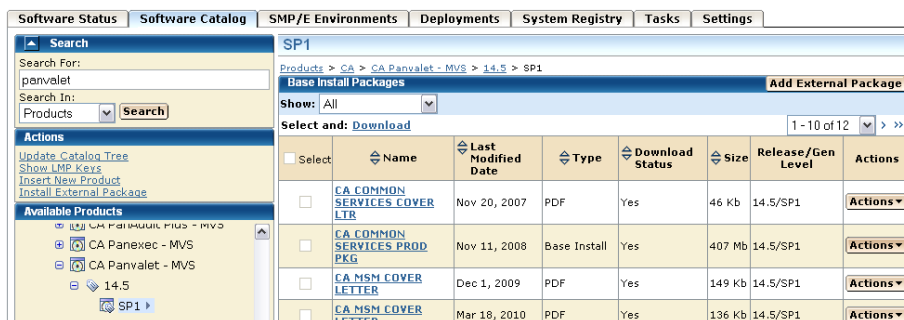
During installation, you select the CSI where the product is to be installed, and specify its zones. You can either specify target and distribution zones to be in the existing CSI data sets, or create new data sets for each zone.

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

**Follow these steps:**

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

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



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

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

The Introduction tab of the wizard appears.

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

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

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

You are prompted to select the type of installation.

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

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

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

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

- If no prerequisites exist, click Next.

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

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

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

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

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

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

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

If you select Create a New SMP/E CSI, you are prompted to [specify the CSI parameters](#) (see page 38).

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

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

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

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

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

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

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

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

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

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

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

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

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

9. Review the summary, and click Install.

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

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

## Create a CSI

You can create a CSI while you are [installing a product](#) (see page 35). During the process, you are asked to specify the following:

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

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

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

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

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

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

**Follow these steps:**

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

You are prompted to define a CSI.

2. Specify the following, and click Next:

**Name**

Defines the name for the environment represented by the CSI.

**Data Set Name Prefix**

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

**Catalog**

Defines the name of the SMP/E CSI catalog.

**Cross-Region**

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

**Cross-System**

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

### High-Level Qualifier

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

### DSN Type

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

### SMS Parameters / Data Set Parameters

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

#### Storage Class (SMS Parameters only)

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

#### Management Class (SMS Parameters only)

Defines the management class for SMP/E data sets.

#### Data Class (SMS Parameters only)

Defines the data class for SMP/E data sets.

#### VOLSER (Data Set Parameters only)

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

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

#### Unit (Data Set Parameters only)

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

#### Catalog (Data Set Parameters only)

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

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

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

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

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

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

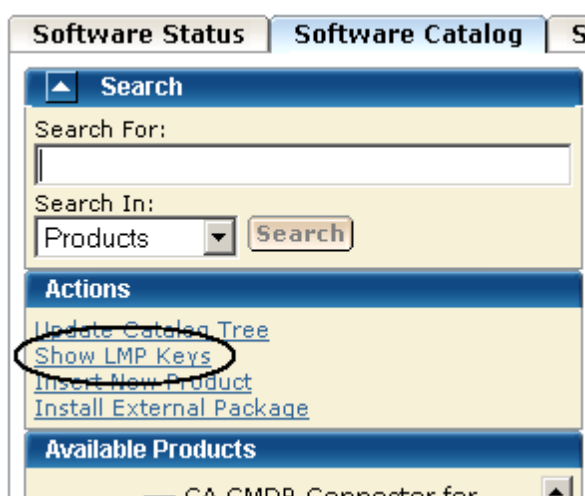
You are prompted to specify any additional parameters. A new CSI is specified.

## Download LMP Keys

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

### Follow these steps:

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



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

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

The list is refreshed for the selected site ID.

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

3. Click Update Keys.

You are prompted to confirm the update.

4. Click OK.

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

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

## Maintaining Products

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

### How to Apply Maintenance Packages

Use this process to download and apply product maintenance packages.

1. Identify your download method. This section details the steps to use the following download methods:
  - [Download Product Maintenance Packages](#) (see page 43)
  - [Download Product Maintenance Packages for Old Product Releases and Service Packs](#) (see page 44)
  - [Manage Maintenance Downloaded External to CA MSM](#) (see page 45)

Contact your system administrator, if necessary.

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

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

## Download Product Maintenance Packages

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

### Follow these steps:

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

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

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

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

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

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

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

The maintenance packages are downloaded.

### More information:

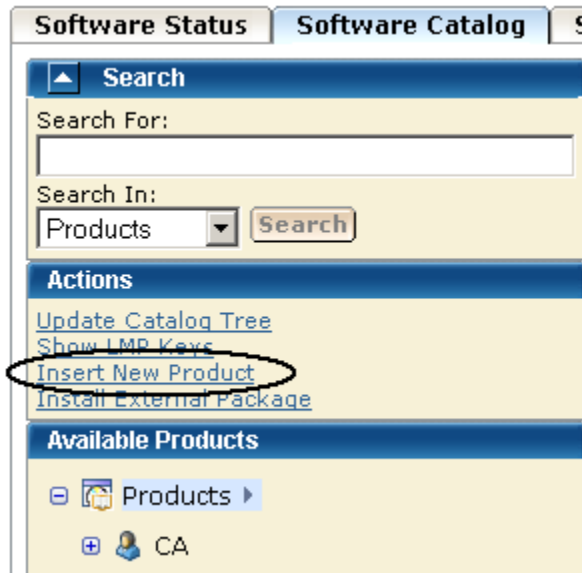
[Download Maintenance Packages for Old Product Releases and Service Packs](#) (see page 44)

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

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

**Follow these steps:**

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



You are prompted to supply information about the product release.

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

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

The product release is added to the software catalog.

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

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

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

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

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

## Manage Maintenance Downloaded External to CA MSM

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

Adding these maintenance packages to CA MSM provides you with a complete view of all the maintenance for a product release. After a package is migrated, you can use CA MSM to [apply the maintenance](#) (see page 47).

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

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

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

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

**Follow these steps:**

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

The maintenance packages for the release are listed.

2. Click the Add External Maintenance button.

You are prompted to specify the package type and location.

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

**Note:** To add several packages from the same location, use [masking](#) (see page 34).

4. Click OK.

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

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

**More information:**

[Manage Maintenance](#) (see page 47)

## View Aggregated Package Details

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

**Follow these steps:**

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

The maintenance packages for the release are listed.

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

The Maintenance Package Details dialog opens.

3. Click the Nested Packages tab.

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

## Manage Maintenance

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

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

The following installation modes are available:

### **Receive and Apply**

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

### **Receive and Apply Check**

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

### **Receive, Apply Check, and Apply**

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

### **Receive Only**

Receives the maintenance.

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

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

### **Follow these steps:**

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

The maintenance information is updated.

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

The maintenance packages are listed, for example:

Software Status		Software Catalog	SMP/E Environments	Deployments	System Registry	Tasks	Settings																																																																													
Search		14.5																																																																																		
Search For:		Products > CA > CA Panvalet - MVS > 14.5																																																																																		
Search In:		Maintenance Packages <span style="float:right">Add External Maintenance Refresh</span>																																																																																		
Products		Show: All <span style="float:right">All for current release</span> <span style="float:right">All source IDs</span>																																																																																		
Actions		Select and: Install <span style="float:right">1 - 10 of 70 &gt;&gt;</span>																																																																																		
Update Catalog Tree		<table border="1"> <thead> <tr> <th>Select</th> <th>Fix #</th> <th>Description</th> <th>Confirmed Date</th> <th>Type</th> <th>Installed</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td><a href="#">Q085668</a></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><a href="#">Q089243</a></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><a href="#">R012055</a></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><a href="#">Q088258</a></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><a href="#">Q088259</a></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><a href="#">Q086490</a></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><a href="#">Q090975</a></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><a href="#">Q081764</a></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><a href="#">Q081763</a></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><a href="#">Q086868</a></td> <td>14.5-SP00: ZTYPE7 NOT FORMATTED CORRECTLY ON TSO</td> <td>Mar 19, 2007</td> <td>PTF</td> <td>No (0/1)</td> <td>Actions</td> </tr> </tbody> </table>						Select	Fix #	Description	Confirmed Date	Type	Installed	Actions	<input type="checkbox"/>	<a href="#">Q085668</a>	* PRODUCT DOCUMENTATION CHANGE	Jan 29, 2007	PEA/PDC	Not installable	Actions	<input type="checkbox"/>	<a href="#">Q089243</a>	* PRODUCT ERROR ALERT *	Jun 20, 2007	PEA/PDC	Not installable	Actions	<input type="checkbox"/>	<a href="#">R012055</a>	0607: MSM INST. ADD SUPPORT FOR SAMPJCL UNDER SMP/E	Oct 7, 2009	PTF	No (0/1)	Actions	<input type="checkbox"/>	<a href="#">Q088258</a>	14.5-SP00 : PANO/PAN#1 INPUT STREAM INVALID COMMAND	May 11, 2007	PTF	No (0/1)	Actions	<input type="checkbox"/>	<a href="#">Q088259</a>	14.5-SP01 : PANO/PAN#1 INPUT STREAM INVALID COMMAND	May 11, 2007	PTF	No (0/1)	Actions	<input type="checkbox"/>	<a href="#">Q086490</a>	14.5-SP00 : DOING ++WRITE, LNG FMT CHANGED AFTER	Mar 6, 2007	PTF	No (0/1)	Actions	<input type="checkbox"/>	<a href="#">Q090975</a>	14.5-SP00/SP01: PAM DIRECTORY AVERAGE BYTES	Sep 4, 2007	PTF	No (0/1)	Actions	<input type="checkbox"/>	<a href="#">Q081764</a>	14.5-SP00: PAN#1 ++CONTROL WITH NO CODE GIVES ERROR	Aug 25, 2006	PTF	No (0/1)	Actions	<input type="checkbox"/>	<a href="#">Q081763</a>	14.5-SP00: PV071 DOING ++SCANS OF ZTYPE1-8 MEMBERS	Aug 25, 2006	PTF	No (0/1)	Actions	<input type="checkbox"/>	<a href="#">Q086868</a>	14.5-SP00: ZTYPE7 NOT FORMATTED CORRECTLY ON TSO	Mar 19, 2007	PTF	No (0/1)	Actions
Select	Fix #	Description	Confirmed Date	Type	Installed	Actions																																																																														
<input type="checkbox"/>	<a href="#">Q085668</a>	* PRODUCT DOCUMENTATION CHANGE	Jan 29, 2007	PEA/PDC	Not installable	Actions																																																																														
<input type="checkbox"/>	<a href="#">Q089243</a>	* PRODUCT ERROR ALERT *	Jun 20, 2007	PEA/PDC	Not installable	Actions																																																																														
<input type="checkbox"/>	<a href="#">R012055</a>	0607: MSM INST. ADD SUPPORT FOR SAMPJCL UNDER SMP/E	Oct 7, 2009	PTF	No (0/1)	Actions																																																																														
<input type="checkbox"/>	<a href="#">Q088258</a>	14.5-SP00 : PANO/PAN#1 INPUT STREAM INVALID COMMAND	May 11, 2007	PTF	No (0/1)	Actions																																																																														
<input type="checkbox"/>	<a href="#">Q088259</a>	14.5-SP01 : PANO/PAN#1 INPUT STREAM INVALID COMMAND	May 11, 2007	PTF	No (0/1)	Actions																																																																														
<input type="checkbox"/>	<a href="#">Q086490</a>	14.5-SP00 : DOING ++WRITE, LNG FMT CHANGED AFTER	Mar 6, 2007	PTF	No (0/1)	Actions																																																																														
<input type="checkbox"/>	<a href="#">Q090975</a>	14.5-SP00/SP01: PAM DIRECTORY AVERAGE BYTES	Sep 4, 2007	PTF	No (0/1)	Actions																																																																														
<input type="checkbox"/>	<a href="#">Q081764</a>	14.5-SP00: PAN#1 ++CONTROL WITH NO CODE GIVES ERROR	Aug 25, 2006	PTF	No (0/1)	Actions																																																																														
<input type="checkbox"/>	<a href="#">Q081763</a>	14.5-SP00: PV071 DOING ++SCANS OF ZTYPE1-8 MEMBERS	Aug 25, 2006	PTF	No (0/1)	Actions																																																																														
<input type="checkbox"/>	<a href="#">Q086868</a>	14.5-SP00: ZTYPE7 NOT FORMATTED CORRECTLY ON TSO	Mar 19, 2007	PTF	No (0/1)	Actions																																																																														

Red asterisks identify HIPER maintenance packages.

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

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

**Note:** The Installed column indicates whether a package is installed. The Introduction tab of the wizard appears.
- Review the information about the maintenance, and click Next.
 

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

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

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

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

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

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

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

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

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

A pop-up window opens.

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

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

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

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

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

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

14. Click Next.

A summary of the task appears.

15. Review the summary, and click Install.

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

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

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

## View Installation Status of Maintenance Package

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

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

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

### Follow these steps:

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

The maintenance packages for the release are listed.

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

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

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

## USERMODs

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

You can create a USERMOD manually, or we can provide an unpublished maintenance package as a USERMOD. In this case, the USERMOD file, which contains the ++USERMOD statement and the body of the USERMOD, must be [managed as an externally downloaded package](#) (see page 45).

## GROUPEXTEND Mode

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

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

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

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

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

### **Apply Check**

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

### **Apply**

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

### **Apply Check and Apply**

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

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

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

- Accept Check
- Accept
- Accept Check and Accept

### How Maintenance in GROUPEXTEND Mode Works

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

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

The followings options are available for bypassing HOLDDATA:

- HOLDSYSTEM
- HOLDCLASS
- HOLDERROR
- HOLDUSER

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

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

## Manage Maintenance in GROUPEXTEND Mode

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

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

### Follow these steps:

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

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

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

2. Click the Maintenance link.

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

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

The Introduction tab of the wizard appears.

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

The packages that you want to apply are listed.

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

5. Review the packages, and click Next.

The Prerequisites tab of the wizard appears.

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

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

Installation options appear.

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

**NOAPARS**

Excludes APARs that resolve error reason ID.

**NOUSERMODS**

Exclude USERMODs that resolve error user ID.

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

The Bypass HOLDDATA tab of the wizard appears.

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

A summary of the task appears.

10. Review the summary, and click Apply GROUPEXTEND.

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

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

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

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

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

## Back Out Maintenance

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

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

### Follow these steps:

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

Products installed in the environment are listed.

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

The features in the component are listed.

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

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

The maintenance packages for the feature are listed.

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

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

The maintenance wizard opens to the Introduction step.

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

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

The packages to back out are listed.

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

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

The Prerequisite tab of the wizard appears.

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

A summary of the task appears.

8. Review the summary, and click Restore.

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

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

## Setting System Registry

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

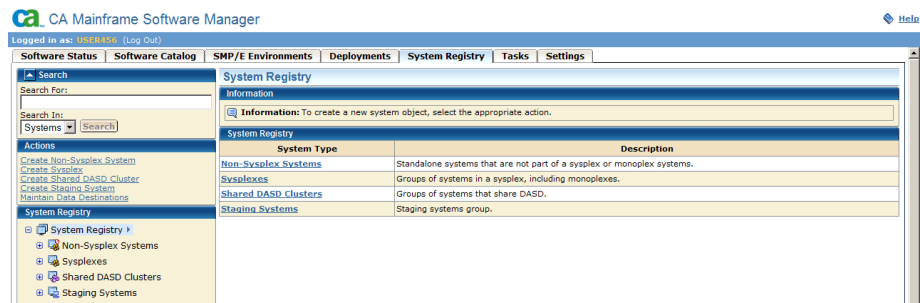
## View a System Registry

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

**Follow these steps:**

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

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

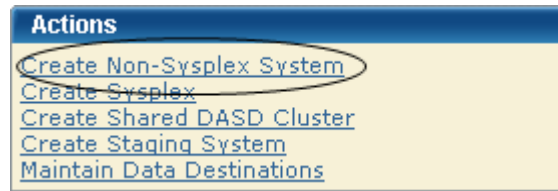


## Create a Non-sysplex System

You can create a non-sysplex system registry.

### Follow these steps:

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



The New Non-Sysplex System dialog appears.

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

2. Enter the following information, and click Save:

#### Name

Enter the non-sysplex system name.

**Limits:** Eight characters

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

#### Description

Enter the description.

**Limits:** 255 characters

#### CCI System ID

(Optional) Enter the CAICCI system ID.

**Limits:** Eight characters

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

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

**Note:** To withdraw this create request, click Cancel.

3. Detail the nonstaging system.

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

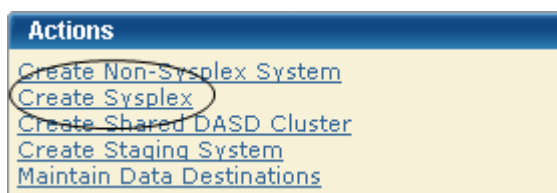
Property Name: z/OS LPAR Name, Value: \*\* Not Applicable \*\*.

## Create a Sysplex or Monoplex

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

### Follow these steps:

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



The New Sysplex dialog appears.

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

2. Enter the following and click Save.

#### Name

Enter the sysplex system name.

**Limits:** Eight characters

#### Description

Enter the description.

**Limits:** 255 characters

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

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

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

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

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

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

4. Enter the following data items for each system:

**Name**

Enter the sysplex system name.

**Limits:** Eight characters

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

**Description**

Enter the description.

**Limits:** 255 characters

**CCI System ID**

(Optional) Enter the CAICCI system ID.

**Limits:** Eight characters

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

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

**Note:** To withdraw this create request, click Cancel.

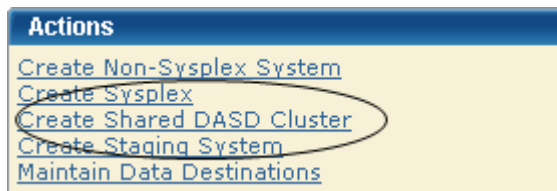
5. Detail the nonstaging system.

## Create a Shared DASD Cluster

You can create a shared DASD cluster.

**Follow these steps:**

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



The New Shared DASD Cluster dialog appears.

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

2. Enter the following information, and click Save:

**Name**

Enter the shared DASD cluster name.

**Limits:** Eight characters

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

**Description**

Enter the description.

**Limits:** 255 characters

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

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

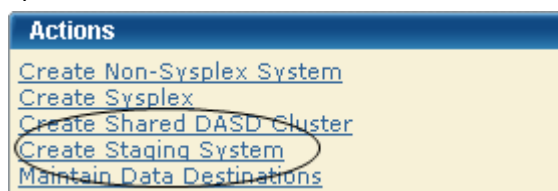
3. Right-click the newly added DASD cluster name and select Add System or Sysplex to this Shared DASD Cluster. Select the systems or sysplexes that you want to add to the DASD cluster.

## Create a Staging System

You can create a staging system.

**Follow these steps:**

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



The New Staging System dialog appears.

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

2. Enter the following information, and click Save:

**Name**

Enter the staging system name.

**Limits:** Eight characters

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

**Description**

Enter the description.

**Limits:** 255 characters

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

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

## Authorization

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

**Edit Mode**

Lets you update and change system registry information.

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

**View Mode**

Lets you view system registry information.

**Note:** You cannot edit information in this mode.

## Change a System Registry

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

### Follow these steps:

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

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

2. Select the system to change.

Detailed information about the system appears on the right side.

3. Update the following information as needed. The information that you update is dependent on whether you are changing a [Non-Sysplex System](#) (see page 57), [Sysplex](#) (see page 58), [Shared DASD Cluster](#) (see page 59), or [Staging System](#) (see page 60).

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

- For Shared DASD or sysplex system only, select the [contact system](#) (see page 67), which is the system where the Shared DASD or FTP is located. The FTP location should be set to the contact system URI. The contact system is used for remote credentials.

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

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

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

- For Staging systems, enter the GIMUNZIP volume and/or [zFS candidate volumes](#) (see page 68).

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

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

**Cancel**

Cancel this maintenance.

**Save**

Save the changes to this maintenance.

**Validate**

Validate authenticates this entry.

**Note:** The validation process is done in steps; each system in this request is validated with the last step summarizing, verifying, and confirming the validation. If the validation fails this step shows how the validation failed. You can [investigate the failed validation](#) (see page 65).

**Validation Rules**

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

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

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

The following are the system validation results:

**Validated**

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

**Validation in Progress**

Indicates that the system status is updated to in progress.

**Validation Error**

Indicates that the system status is updated to error, and you can [investigate the failed validation](#) (see page 65).

**Not Validated**

Indicates that this system has not been validated yet.

**Not Accessible**

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

**Validation Conflict**

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

**Error Details**

When there is a validation conflict, the Error details button appears. Click this button to find the reason for this conflict. You can [investigate the failed validation](#) (see page 65).

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

**Conflict Details**

When a validation is in conflict, the Error details button appears. Click this button to find the reason for this conflict. You can [investigate the failed validation](#) (see page 65).

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

## Failed Validations

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

- [Investigate a Failed Validation using the Tasks Page](#) (see page 65)
- [Investigate a Failed Validation Immediately After a Validation](#) (see page 66)
- [Download a Message Log](#) (see page 66)
- [Save a Message Log as a Data Set](#) (see page 67)
- [View Complete Message Log](#) (see page 67)

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

## Investigate a Failed Validation Using Task Output Browser

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

**Follow these steps:**

1. On the System Registry tab, in the column on the left, find the system with a validation status error and make a note of it.
2. Click the Tasks tab and then click Task History.
3. At the Show bar, select All task, or My task to list the tasks by Owner.
 

**Note:** You can refine the task list by entering USER ID, types, and status.
4. Find the failed validation and click the link in the Name column.

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

Owner	Name	Type	Status	Start Time	Stop Time	Task ID
USER456	<a href="#">Validating System: XX60</a>	System Registry	Failed	1/12/2010 02:26:01PM	1/12/2010 02:26:09PM	432

The Validate System Task Output Browser appears.

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

#	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

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

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

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

7. Correct the issue and validate again.

## Investigate a Failed Validation After Validation

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

### Follow these steps:

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

The validation results appear.

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

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

7. Correct the issue and validate again.

## Download a Message Log

You can save the message log in the following ways:

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

## Save a Message Log as a Data Set

You can save a message log as a data set.

### Follow these steps:

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

The Save Output as Data Set dialog appears.

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

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

2. Enter the following information and click OK:

#### Data Set Name

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

#### VOLSER

For non-SMS data, enter the Volser.

#### Example:

Volser: SYSP01 and SYSP02

#### Storage Class

For SMS Allocation data, enter the Storage Class.

The message log is saved as a data set.

## View Complete Message Log

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

**Note:** To close the message log, click Close.

## Contact System

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

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

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

## zFS Candidate Volumes

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

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

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

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

**Note:** Remote system requirement is customer defined.

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

### CA Allocate

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

### CA Disk Backup and Restore

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

You can also use the following standard IBM techniques:

- Allocation exits
- ACS routines

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

## Maintain a System Registry using the List Option

**Follow these steps:**

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

## Delete a System Registry

### Follow these steps:

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

The system list appears.

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

The system is deleted.

## FTP Locations

The [FTP](#) (see page 69) Locations lists the current FTP locations for this system. You can [add](#) (see page 69), [edit](#) (see page 71), [set default](#) (see page 72), or [remove](#) (see page 72) [FTP](#) (see page 69) locations.

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

## Deployment FTP Locations

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

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

## Add FTP Locations

You can add [FTP](#) (see page 69) locations.

### Follow these steps:

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

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

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

Detailed information about the system appears on the right side.

3. Click the FTP Locations tab.

The FTP Locations window appears.

4. Click Add.

The New FTP Location dialog appears.

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

5. Enter the following information, and click Save:

#### URI

Enter the URI.

**Limits:** Maximum length is 255.

#### Port

Enter the Port.

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

**Default:** 21

#### Directory Path

Enter the Directory Path.

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

The new FTP location appears on the list.

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

### More information:

[Edit FTP Locations](#) (see page 71)

[Delete FTP Locations](#) (see page 72)

[Set FTP Location Default](#) (see page 72)

## Edit FTP Locations

You can edit [FTP](#) (see page 69) locations.

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

**Follow these steps:**

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

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

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

Detailed information about the system appears on the right side.

3. Click the FTP Location tab.

The FTP Locations window appears.

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

The Edit FTP Location dialog appears.

5. Update the following and click Save:

**URI**

Enter the URI.

**Limits:** Maximum length is 255.

**Port**

Enter the Port.

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

**Default:** 21

**Directory Path**

Enter the Directory Path.

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

Your changes are saved.

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

## Set FTP Location Default

You can set an [FTP](#) (see page 69) location default.

### Follow these steps:

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

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

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

Detailed information about the system appears on the right side.

3. Click the FTP Locations tab.

The FTP Locations window appears.

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

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

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

## Delete FTP Locations

You can delete [FTP](#) (see page 69) locations.

### Follow these steps:

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

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

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

Detailed information about the system appears on the right side.

3. Click the FTP Locations tab.

The FTP Locations window appears.

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

The FTP location is deleted from this system.

## Data Destinations

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

### FTP

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

### Shared DASD

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

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

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

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

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

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

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

## Create Data Destinations

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

### Follow these steps:

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

The Maintains Data Destinations dialog appears.

2. Click Create.

The New Data Destination dialog appears.

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

3. Enter the following information, and click Save:

#### Name

Enter a meaningful name.

**Limits:** Maximum 64 characters.

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

#### Description

Enter the description.

**Limits:** Maximum 255 characters.

#### Transmission Method

Select the transmission method.

**Default:** Shared DASD.

#### Mount Point

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

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

**Limits:** Maximum 120 characters

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

**Storage Class**

(Shared DASD only) Enter the Storage Class.

**Limits:** Maximum 8 characters

**Example:** SYSPRG

**VOLSER**

(Shared DASD only) Enter the Volser.

**Limits:** Maximum 6 characters

**Example:** SYSP01 and SYSP02

**GIMUNZIP Volume**

Enter the GIMUNZIP volume.

**Limits:** Maximum 6 characters

**zFS Candidate Volumes**

Enter [zFS Candidate volumes](#) (see page 68).

**Limits:** Maximum 6 characters

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

The new data destination appears on the Data Destination list.

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

## Add a Data Destination

You can add current data destinations to an existing system.

**Follow these steps:**

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

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

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

Detailed information about the system appears on the right side.

3. Click the Data Destination tab.

The Data Destination window appears.

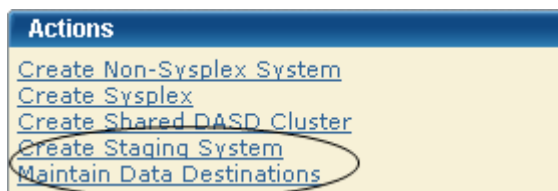
4. Click Add.  
The Pick Data Destination dialog appears.
5. Select the data destinations you want to add and click Select.  
The data destinations are added to the system.

## Maintain Data Destinations

You can maintain, [delete](#) (see page 78), or [create](#) (see page 74) data destinations.

### Follow these steps:

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



The Maintains Data Destinations dialog appears.

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

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

The Edit Data Destinations dialog appears.

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

3. Update the following and click Save:

#### Name

Enter a meaningful Name.

**Limits:** Maximum 64 characters.

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

#### Description

Enter the description.

**Limits:** Maximum 255 characters.

#### Transmission Method

Select the transmission method.

**Default:** Shared DASD.

**Mount Point**

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

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

**Limits:** Maximum 120 characters

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

**Storage Class**

(Shared DASD only) Enter the Storage Class.

**Limits:** Maximum 8 characters

**Example:** SYSPRG

**VOLSER**

(Shared DASD only) Enter the Volser.

**Limits:** Maximum 6 characters

**Example:** SYSP01 and SYSP02

**GIMUNZIP Volume**

Enter the GIMUNZIP volume.

**Limits:** Maximum 6 characters

**zFS Candidate Volumes**

Enter [zFS Candidate volumes](#) (see page 68).

**Limits:** Maximum 6 characters

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

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

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

## Set a Default Data Destination

You can set a default for a current data destination.

### Follow these steps:

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

## Delete Data Destinations

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

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

### Follow these steps:

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

## Remote Credentials

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

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

You can [add](#) (see page 79), [edit](#) (see page 80), or [delete](#) (see page 81) remote credentials.

### Add Remote Credentials

**Follow these steps:**

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

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

**Remote User ID**

Enter a correct remote user ID.

**Limits:** 64 characters

**Remote System Name**

Enter a remote system name.

**Limits:** Eight characters

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

**Password**

Enter a correct password.

**Limits:** 2 to 63 characters

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

### Confirm Password

Enter the correct confirm password.

**Limits:** 2 to 63 characters

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

The remote credential entry appears on the Remote Credentials list.

4. Click Apply.

Your changes are applied.

## Edit Remote Credentials

You can edit remote credentials.

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

### Follow these steps:

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

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

### Remote User ID

Enter a correct remote user ID.

**Limits:** Maximum 64 characters.

### Remote System Name

Enter a correct remote system name.

**Limits:** Maximum 8 characters.

**Example:** RMinPlex

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

**Password**

Enter a correct password.

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

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

**Confirm Password**

Enter the correct confirm password.

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

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

The remote credential entry appears on Remote Credentials list.

4. Click Apply

Your changes are applied.

## Delete Remote Credentials

You can delete remote credentials.

**Follow these steps:**

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

## Deploying Products

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

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

## Deployment Status

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

### **Under Construction**

The user is constructing the deployment.

**Available Actions:** All but Confirm

### **Snapshot in Progress**

Snapshot is in Progress

**Available Actions:** Reset Status

### **Snapshot in Error**

Snapshot failed

**Available Actions:** All but Confirm

### **Snapshot Completed**

Snapshot Succeeded

**Available Actions:** Delete, Preview, Transmit, Deploy

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

### **Transmitting**

The deployment archives are being transmitted using the FTP procedure.

**Available Actions:** Reset Status

### **Transmission Error**

Transmission Failed

**Available Actions:** Delete, Preview, Transmit, Deploy

### **Transmitted**

The deployment archives have been transmitted.

**Available Actions:** Delete, Preview, Deploy

### **Deploying**

The deployment archives are being deployed.

**Available Actions:** Reset Status

### **Deploying Error**

Deployment failed

**Available Actions:** Delete, Preview, Deploy

**Deployed**

The target libraries were deployed.

**Available Actions:** Delete, Summary, Confirm

**Complete**

The deployment is complete.

**Available Actions:** Delete, Summary

## Creating Deployments

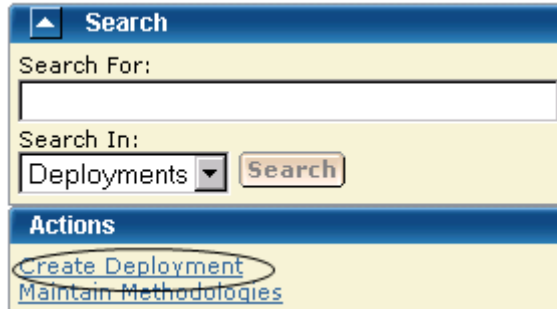
The deployment creation process consists of the following steps:

1. [Initiate deployment creation](#) (see page 84).
2. [Define a name and description](#) (see page 84).
3. [Select an SMP/E environment](#) (see page 85).
4. [Select a product](#) (see page 85).
5. [Select a custom data set](#) (see page 86).
6. [Select a methodology](#) (see page 86).
7. [Select a system](#) (see page 88).
8. [Preview and save](#) (see page 88).

## Initiate Deployment Creation

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

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



The New Deployment wizard opens to the Introduction step.

**Note:** When creating a deployment, you can save this deployment at any step in this wizard. This "under construction" deployment is added to the current deployments list. You can [maintain this deployment](#) (see page 89) until a successful snapshot has been created.

## Define Name and Description

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

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

### Follow these steps:

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

**Limits:** Maximum 64 characters.

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

2. Enter the description of this deployment.

**Limits:** Maximum 255 characters.

3. Click Next.

The CSI Selection step appears.

**Note:** When creating a deployment, you can save this deployment at any step in this wizard. This "under construction" deployment is added to the current deployments list. You can [maintain this deployment](#) (see page 89) until a successful snapshot has been created.

## Select a CSI

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

### Follow these steps:


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

**Note:** When creating a deployment, you can save this deployment at any step in this wizard. This "under construction" deployment is added to the current deployments list. You can [maintain this deployment](#) (see page 89) until a successful snapshot has been created.

## Select a Product

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

### Follow these steps:

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

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

The Custom Data Sets step appears.

**Note:** When creating a deployment, you can save this deployment at any step in this wizard. This "under construction" deployment is added to the current deployments list. You can [maintain this deployment](#) (see page 89) until a successful snapshot has been created.

## Select a Custom Data Set

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

### Follow these steps:

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

**Note:** To add a new custom data set, click Add Data Set and [enter the custom data set information](#) (see page 101).

2. Click Next.

The Methodology Selection step appears.

**Note:** When creating a deployment, you can save this deployment at any step in this wizard. This "under construction" deployment is added to the current deployments list. You can [maintain this deployment](#) (see page 89) until a successful snapshot has been created.

### More information:

[Add a Custom Data Set](#) (see page 101)

## Select a Methodology

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

### Follow these steps:

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

2. (Optional) Click the Create button and [enter the new methodology information](#) (see page 108).

**New Deployment**

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

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

**Methodologies** Create

1 - 5 of 44

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

Save Back Next Deploy Cancel Help

3. Click Next.

The System Selection step appears.

**Note:** When creating a deployment, you can save this deployment at any step in this wizard. This "under construction" deployment is added to the current deployments list. You can [maintain this deployment](#) (see page 89) until a successful snapshot has been created.

**More information:**

[Create a Methodology](#) (see page 108)

## Select a System

After you select a methodology, you select a system.

### Follow these steps:

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

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

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

2. Click Next.

The Preview step appears.

**Note:** When creating a deployment, you can save this deployment at any step in this wizard. This "under construction" deployment is added to the current deployments list. You can [maintain this deployment](#) (see page 89) until a successful snapshot has been created.

## Preview and Save the Deployment

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

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

**Note:** Click Cancel to exit the wizard without saving.

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

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

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

## View a Deployment

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

## Change Deployments

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

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

### Follow these steps:

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

The detailed deployment information appears.

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

This deployment's window appears.

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

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

[There are actions that you can perform based on Deployment State](#) (see page 82).

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

The [Edit Methodology window](#) (see page 121) appears. The Deployment ID is the value of the MSMID variable.

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

- You can [select](#) (see page 98), [add](#) (see page 99), or [remove](#) (see page 99) a product.
  - You can [select](#) (see page 125), [add](#) (see page 125), or [remove](#) (see page 126) a system.
  - You can [select](#) (see page 100), [add](#) (see page 101), or [remove](#) (see page 107) a custom data set.
5. Click Save on the Deployment Details window.

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

**Preview (Summary)**

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

Generates a list of the following current information:

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

**Snapshot**

Takes a snapshot of the current deployment.

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

**Transmit**

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

**Deploy**

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

**Confirm (see page 96)**

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

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

### Delete

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

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

### [Reset Status](#) (see page 94)

You can reset a deployment status when the deployment has a status of *snapshot in progress*, *transmitting*, or *deploying*. See [reset status](#) (see page 94) for a list of deleted files.

7. Click Save on the Deployment Details window.

Your changes are saved.

### More information:

- [Add a Product](#) (see page 99)
- [Add a System](#) (see page 125)
- [Remove a Product](#) (see page 99)
- [Remove a System](#) (see page 126)
- [View the Product List](#) (see page 98)
- [View a System List](#) (see page 125)
- [Edit a Methodology](#) (see page 121)
- [Confirm a Deployment](#) (see page 96)

## Deployment Maintenance

You can maintain a deployment in the following ways:

- Adding
  - [System](#) (see page 125)
  - [Product](#) (see page 99)
  - [Custom data sets](#) (see page 101)
- Delete
  - Deployment
- Removing
  - [System](#) (see page 126)
  - [Product](#) (see page 99)
  - [Custom data sets](#) (see page 107)

- Editing
  - [Maintain deployments](#) (see page 89)
  - [Edit a custom data set](#) (see page 104)
  - [Edit a methodology](#) (see page 121)
- Viewing
  - [System](#) (see page 125)
  - [Product](#) (see page 98)
  - [Custom data sets](#) (see page 100)

## Failed Deployments

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

- [Investigate a Failed Deployment Using the Tasks Page](#) (see page 92)
- [Download a Message Log](#) (see page 66)
- [Save a Message Log as a Data Set](#) (see page 67)
- [View Complete Message Log](#) (see page 67)

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

**More information:**

- [Download a Message Log](#) (see page 66)
- [Save a Message Log as a Data Set](#) (see page 67)
- [View Complete Message Log](#) (see page 67)

## Investigate a Failed Deployment

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

**Follow these steps:**

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

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

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

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

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

The Task Output Browser appears.

Deploy: Deployment Test <span style="float: right;">Close</span>			
General <span style="float: right;">Download Zipped Output</span>			
Name: Deploy: Deployment Test			
Task ID: 3172			
User ID: USER456			
Status: Failed			
Status Message: Failed			
Steps			
#	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 to view the results, and click on the messages logs to review the details for each error.

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

- Correct the issue and deploy again.

#### More information:

[Download a Message Log](#) (see page 66)

[Save a Message Log as a Data Set](#) (see page 67)

[View Complete Message Log](#) (see page 67)

## Download a Message Log

You can save the message log in the following ways:

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

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

## Save a Message Log as a Data Set

You can save a message log as a data set.

### Follow these steps:

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

The Save Output as Data Set dialog appears.

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

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

2. Enter the following information and click OK:

#### Data Set Name

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

#### VOLSER

For non-SMS data, enter the Volser.

#### Example:

Volser: SYSP01 and SYSP02

#### Storage Class

For SMS Allocation data, enter the Storage Class.

The message log is saved as a data set.

## View Complete Message Log

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

**Note:** To close the message log, click Close.

## Reset Deployment Status

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

You can also [investigate a failed deployment](#) (see page 65) to see additional details in the message log.

The following statuses may be reset.

### Snapshot in progress

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

**Transmitting**

Transmitting is reset to *transmit in error*.

**Deploying**

Deploying is reset to *deploy in error*.

The following artifacts are reset by status.

**Snapshot in Progress**

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

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

**Transmit in Progress**

Nothing is reset.

**Deploy in Progress**

Nothing is reset.

## Delete a Deployment

You can delete deployments.

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

A deployment deletion must be confirmed before a deletion starts.

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

The message log explains which containers, folders, and files were deleted during processing and which ones were not deleted. See how to [investigate a failed deployment](#) (see page 65) for details on finding the message log.

**Note:** Target libraries are never deleted.

The following artifacts are deleted by status:

**Under Construction**

All applicable database records

**Snapshot in Error**

All applicable database records

### **Snapshot Completed**

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

All applicable database records.

### **Transmit in Error**

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

### **Transmitted**

Same as Transmit in Error.

### **Deploy in Error**

Same as Transmitted.

### **Deployed**

Same as Snapshot Completed.

### **Complete**

Same as Snapshot Completed.

### **Follow these steps:**

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

## **Confirm a Deployment**

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

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

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

**Follow these steps:**

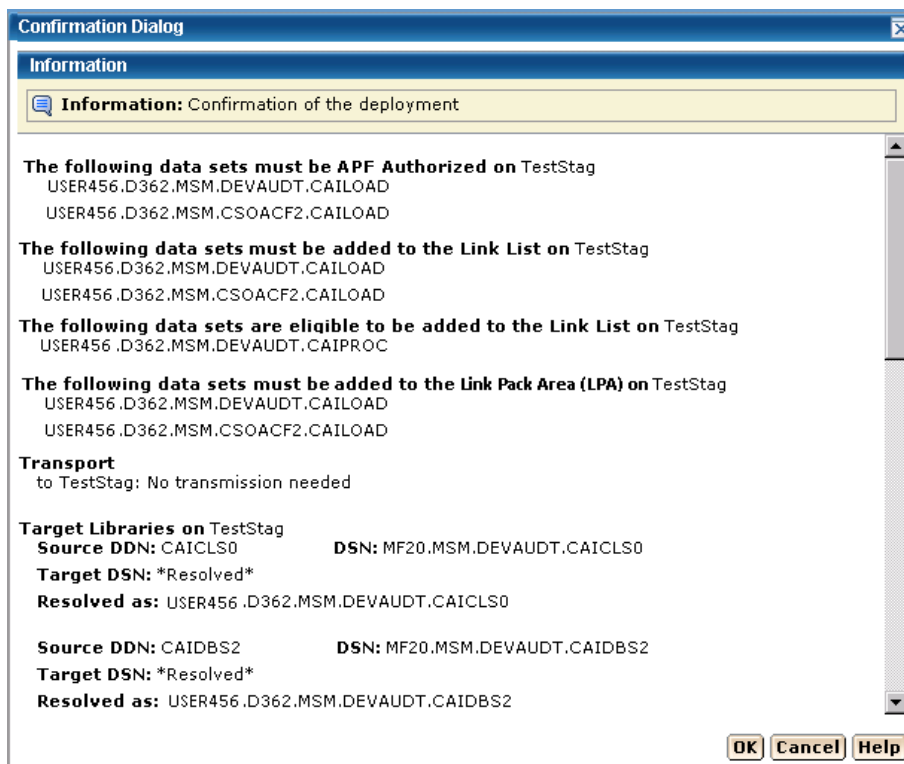
1. Click the Deployments tab.  
The Deployment page appears.
2. Click Confirm.  
The Confirmation dialog appears.
3. Review the confirmation.
4. Click OK when the deployment is correct.

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

The Deployment Summary window may contain the following:

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

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



## Products

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

### View the Product List

You can view a product.


**Follow these steps:**

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

## Add a Product

You can add a product to a deployment.

### Follow these steps:

1. Click the Deployments tab. The Deployments window appears.
2. On the right, in the Deployments panel click the Current Deployment link.  
A list of current deployments appears.
3. Click the deployment name link.
4. In the Product List panel click Add Products.  
The Add Products wizard appears.
5. Select a CSI and click Next.  
The Product Selection appears.
6. Select a product.
7. If there is a  text icon in Text column, click the text icon to read the instructions supplied by CA Support for product, data sets, and other necessary information.
8. Click the "I have read the associated text by selecting the text icon from the list about" box. This box appears only if there is a text icon.  
**Note:** You will not be able to click Next until you click this box.
9. Click Next.  
The Custom Data Set Selection appears
10. If needed, select or [add a custom data set](#) (see page 101).
11. Click Add Products.  
The Product is added.

## Remove a Product

You can remove a product from a deployment.

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

### Follow these steps:

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

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

## Custom Data Sets

You can view, [add](#) (see page 101), [edit](#) (see page 104), and [remove](#) (see page 107) custom data sets from a deployment.

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

- For a z/OS data set, you need to provide a data set name that is the actual existing z/OS data set and a mask that names the data set on the target system. This mask may be set up using [symbolic qualifiers](#) (see page 111) 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 111)), and a type of copy. The type of copy can be either a container copy or a file-by-file copy.

## View Custom Data Sets

You can view custom data sets.

### Follow these steps:

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

The detailed deployment information appears on the right side.

### Product Name Sort Arrows

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

## Add a Custom Data Set

You can add custom data sets to a deployment.

### Follow these steps:

1. Click the Deployments tab.  
The Deployments window appears.
2. On the right, in the Deployments panel, click the Current Deployment link.  
A list of current deployments appears.
3. Click the deployment name link.
4. In the Custom Data Sets List panel, click Add Data Sets.  
The Add Custom Data Sets dialog appears.  
**Note:** The asterisk indicates that the field is mandatory.
5. Select a Product from the drop-down list.  
**Note:** When there are instructions, they are required and supplied by CA Support.
6. Select the Data Set Type, either data set (step 7) or USS (step 10).  
**Default:** data set
7. For data set, enter the data set name.  
**Limits:** Maximum 44 characters.  
**Note:** This is the existing z/OS data set name that you want CA MSM to include in the deployment when it is deployed on the target systems.
8. Enter the data set name mask, click the file icon, and select a [symbolic name](#) (see page 111).

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

**Limits:** Maximum 64 characters.

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

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

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

- 

Two consecutive periods are required to separate the two masks.

9. Enter the Mask and click OK.
10. For USS data set type, enter the Local Path. The local path is the directory where files are to be copied from.  
**Limit:** Maximum 255 characters.  
**Note:** The asterisk indicates that the field is mandatory.
11. Enter the Remote Path and/or click the file icon and select a [symbolic name](#) (see page 111). The remote path is the path where the files are to be copied to.  
**Limit:** Maximum 255 characters.
12. Select the Type of Copy:
  - If you select Container Copy, proceed to step 14.
  - If you select File-by-file Copy, proceed to step 15, and ensure that the USS path exists on all of the remote systems of this deployment, and that there is sufficient space to hold these target libraries.  
**Default:** Container Copy
13. Click OK.
14. For Container Copy, enter the container name and/or click the file icon and select a [symbolic name](#) (see page 111).  
**Limit:** Maximum 64 characters.  
**Note:** It consists of one or more qualifiers separated by periods, and has a maximum input length of 64 characters, including the periods. When it is translated, it has a maximum length of 44 characters, including the periods.

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

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

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

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

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

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

16. Enter the Mount Point and/or click the file icon and select a [symbolic name](#) (see page 111).

**Limit:** Maximum 255 characters.

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

17. Enter the percentage of Free Space needed.

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

**Limit:** 0 to 1000.

18. Click OK.

The custom data set is added.

## Edit a Custom Data Set

You can edit a custom data set.

### Follow these steps:

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

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

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

**Default:** data set

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

**Limits:** Maximum 44 characters.

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

8. Enter the data set name mask, click the file icon, and select a [symbolic name](#) (see page 111).

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

**Limits:** Maximum 64 characters.

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

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

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

■

Two consecutive periods are required to separate the two masks.

9. Enter the Mask and click OK.
10. For USS data set type, enter the Local Path. The local path is the directory where files are to be copied from.  
**Limit:** Maximum 255 characters.  
**Note:** The asterisk indicates that the field is mandatory.
11. Enter the Remote Path and/or click the file icon and select a [symbolic name](#) (see page 111). The remote path is the path where the files are to be copied to.  
**Limit:** Maximum 255 characters.
12. Select the Type of Copy:
  - If you select Container Copy, proceed to step 14.
  - If you select File-by-file Copy, proceed to step 15, and ensure that the USS path exists on all of the remote systems of this deployment, and that there is sufficient space to hold these target libraries.  
**Default:** File-by-file Copy
13. Click OK.
14. For Container Copy, enter the container name and/or click the file icon and select a [symbolic name](#) (see page 111).  
**Limit:** Maximum 64 characters.

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

For container copy the following occurs during the deployment process:

- a. A file system of the requested type is created
- b. The size of the file system is computed as follows:
  - The size 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 is used to calculate the secondary allocation.
- c. All of the directories in the mount point will by dynamically created.
- d. The file system will be mounted at the requested mount point  
**Note:** The mount is not permanent. You will need to update your BPXPARMS to make this mount point permanent.
- e. The content from the local path will copied into the newly created and mounted file system.

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

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

16. Enter the Mount Point and/or click the file icon and select a [symbolic name](#) (see page 111).

**Limit:** Maximum 255 characters.

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

17. Enter the percentage of Free Space needed.

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

**Limit:** 0 to 1000.

18. Click OK.

The custom data set is changed.

---

## Remove a Custom Data Set

You can remove a custom data set from a deployment.

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

**Follow these steps:**

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

**Product Name Sort Arrows**

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

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

## Methodologies

You can [create](#) (see page 108), maintain, [edit](#) (see page 121), and [delete](#) (see page 123) methodologies from a deployment.

A methodology has the following attributes:

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

**z/OS data sets**

z/OS data sets use a data set name mask. The data set name mask is a valid data set name comprised of constants and [symbolic qualifiers](#) (see page 111).

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

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

#### **Create Only**

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

#### **Create or Replace**

Use *Create or Replace* to:

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

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

## **Create a Methodology**

You can create a methodology.

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

#### **Follow these steps:**

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

The Create a New Methodology dialog appears.

2. Enter the methodology name.

**Limits:** Maximum 64 characters.

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

3. Enter the description of this methodology.

**Limits:** Maximum 255 characters.

4. Enter the data mask name, click the file icon, and select a [symbolic name](#) (see page 111).

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

**Limits:** Maximum 64 characters.

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

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

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

■

5. Select a style of Deployment.

**Create only**

Creates new data sets.

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

**Create or Replace**

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

**Partitioned data set**

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

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

**Directory in a UNIX file system**

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

**Sequential data set or a file in the UNIX file system**

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

**For a VSAM data set (cluster)**

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

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

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

6. Click Save.

The methodology is saved.

**Note:** Click Cancel to close this dialog without saving.

## Symbolic Qualifiers

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

### Data Set Name Mask

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

### Directory Path

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

### Symbolic Substitution

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

### Symbolic Variables

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

**Example:** Assume MSMDID is 255.

SYSWORK.D&MSMDID..DATASET

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

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

### Numeric Values

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

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

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

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

An incorrect specification of the mask would be:

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

### Directory Paths

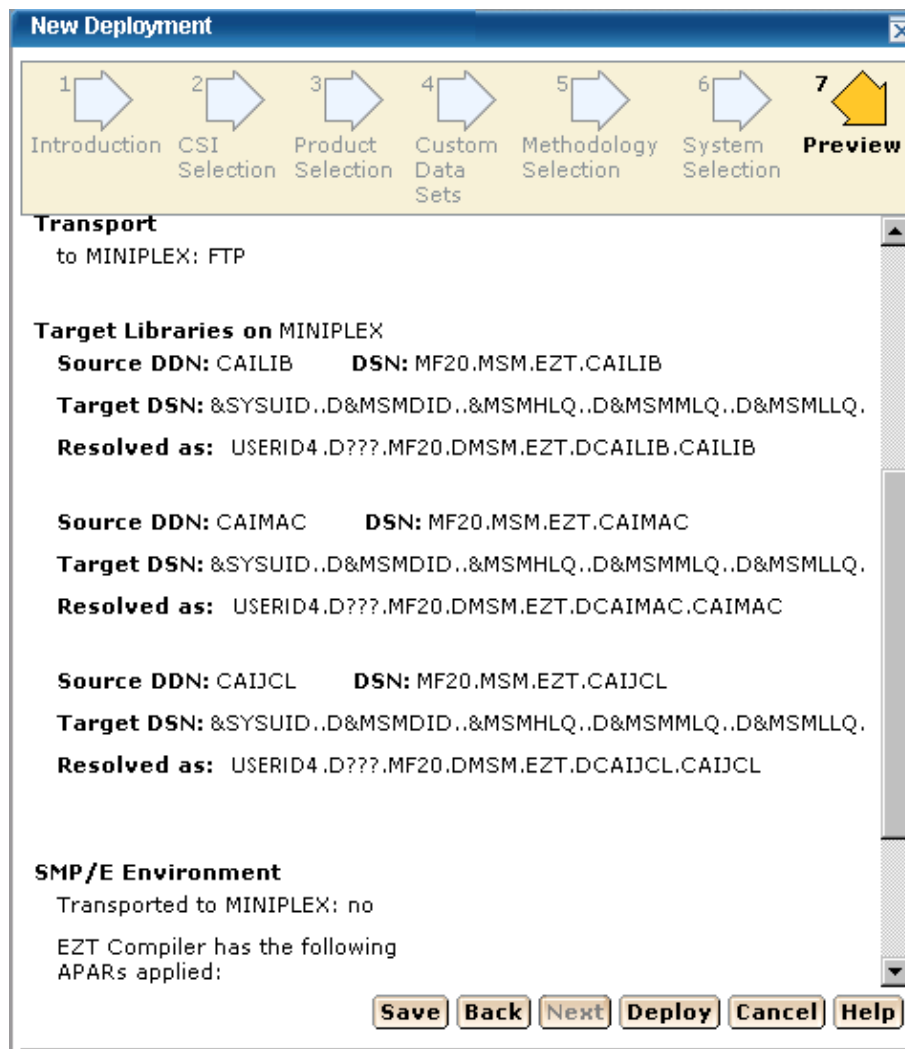
Symbolic substitution works in the same logical way for directory paths. However, directory paths do not typically have periods in them, so you will typically not see the double dots in directory paths.

**Example:** Assume the target system is SYSZ.

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

### Preview Example

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



### Symbolic Qualifiers

#### ID and System Information

##### MSMDID

This is the CA MSM deployment ID.

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

### MSMMPN

This is the CA MSM Mount Point Name. The value is entered into the mount point name field when [adding a custom data set](#) (see page 101) with both the USS radio button and the Container copy radio button set. It is of primary value in remote path.

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

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

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

Remote path: &MSMMPN.

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

### MSMSYSNM

This is the CA MSM system object name.

### SYSCLONE

This is the shorthand name of the system.

**Limits:** Maximum 2 characters.

### SYSNAME

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

### SYSPLEX

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

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

### SYSUID

The current user ID.

## Target Libraries

### MSMHLQ

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

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

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

**MSMMLQ**

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

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

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

**MSMLLQ**

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

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

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

**MSMSLQ**

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

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

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

**MSMPREF**

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

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

**MSMDLIBN**

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

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

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

Assume the methodology specified a mask of:

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

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

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

**Local Date and Time**

**LYMMDD**

This is the local two-digit year.

**YY** two-digit year

**MM** two-digit month (01=January)

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

**Example:** 100311

**LXR2**

This is the local two-digit year.

**LXR2** two-digit year

**Example:** 10

**LXR4**

This is the local four-digit year.

**LXR4** four-digit year

**Example:** 2010

**LXON**

This is the local month.

**LXON** two-digit month (01=January)

**Example:** 03

**LDAY**

This is the local day of the month.

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

**Example:** 11

**LJDAY**

This is the local Julian day.

**LJDAY** three-digit day (001 through 366)

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

**LWDAY**

This is the local day of the week.

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

**Example:** MON

**LHHMMSS**

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

**HH** two digits of hour (00 through 23) (am/pm NOT allowed)

**MM** two digits of minute (00 through 59)

**SS** two digits of second (00 through 59)

**Example:** 165148

**LHR**

This is the local time in hours.

**LHR** two-digits of hour (00 through 23) (am/pm NOT allowed)

**Example:** 16

**LMIN**

This is the local time in minutes.

**LMIN** two-digits of minute (00 through 59)

**Example:** 51

**LSEC**

This is the local time in seconds.

**LSEC** two-digits of second (00 through 59)

**Example:** 48

### UTC Date and Time

Coordinated Universal Time is abbreviated UTC.

#### YYMMDD

This is the UTC date.

**YY** two-digit year

**MM** two-digit month (01=January)

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

**Example:** 100311

#### YR2

This is the UTC two digit year.

**YR2** two-digit year

**Example:** 10

#### YR4

This is the UTC four digit year.

**YR4** four-digit year

**Example:** 2010

#### MON

This is the UTC month.

**MON** two-digit month (01=January)

**Example:** 03

#### DAY

This is the UTC day of the month.

**DAY** two-digit day of month (01 through 31)

**Example:** 11

#### JDAY

This is the UTC Julian day.

**JDAY** three-digit day (001 through 366)

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

#### WDAY

This is the UTC day of the week.

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

**Example:** MON

**HHMMSS**

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

**HH** two-digits of hour (00 through 23) (am/pm NOT allowed)

**MM** two-digits of minute (00 through 59)

**SS** two-digits of second (00 through 59)

**Example:** 044811

**HR**

This is the UTC time in hours.

**HR** two digits of hour (00 through 23) (am/pm NOT allowed)

**Example:** 04

**MIN**

This is the UTC time in minutes.

**MIN** two-digits of minute (00 through 59)

**Example:** 48

**SEC**

This is the UTC time in seconds.

**SEC** two-digits of second (00 through 59)

**Example:** 11

## Maintain Methodologies

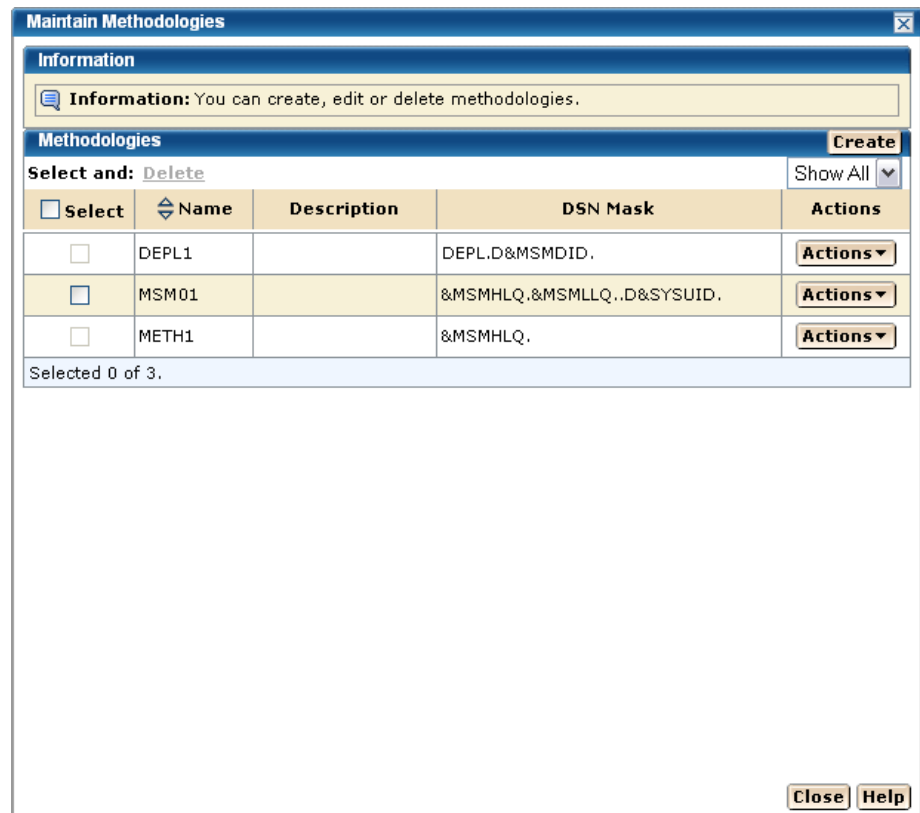
You can edit, replace, or [remove](#) (see page 123) methodologies.

### Follow these steps:

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



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



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

[The Methodology window appears for editing](#) (see page 121).

**More information:**

[Delete Methodologies](#) (see page 123)

[Edit a Methodology](#) (see page 121)

## Edit a Methodology

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

**Follow these steps:**

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

The Edit Methodologies dialog appears.

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

As with Add a Methodology, all fields are available to be edited and the details for each field are listed.

3. Enter the Methodology Name.

**Limits:** Maximum 64 characters.

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

4. Enter the Description of this Methodology.

**Limits:** Maximum 255 characters.

5. Enter the data set name mask, click the file icon, and select a [symbolic name](#) (see page 111).

**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 111).

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

**Limits:** Maximum 64 characters.

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

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

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

■

6. Select a Style of Deployment.

**Create only**

Creates new data sets.

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

**Create or Replace**

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

**Partitioned data set**

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

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

**Directory in a UNIX file system**

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

**Sequential data set or a file in the UNIX file system**

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

**For a VSAM data set (cluster)**

*Create or Replace* indicates that an existing VSAM cluster should be populated with the data from the source file.

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

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

7. Click Save.

Your changes are saved.

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

**More information:**

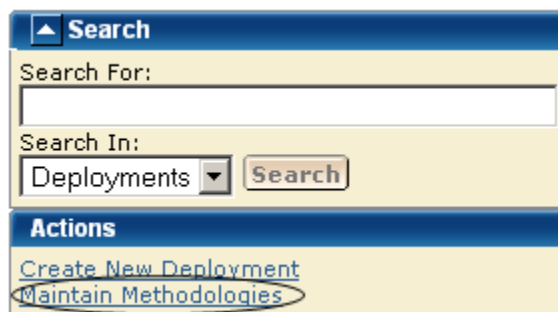
[Symbolic Qualifiers](#) (see page 111)

## Delete Methodologies

**Follow these steps:**

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

The Maintain Methodologies select window appears.



2. Select the methodology that you want to delete.

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

3. Click Delete and then OK to the Delete Methodologies confirmation window.  
The methodology is deleted.

## Systems

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

### Target System Types

There are two types of *target systems*.

#### Test Environment

Test Environment target systems isolate untested deployment changes and outright experimentation from the production environment or repository. This environment is used a temporary work area where deployments can be tested, modified, overwritten, or deleted.

#### Production

Production target systems contain current working product deployments. When activating products in a production target system care must be taken, CA MSM recommends using the following procedure.

1. Copy the product to that target system with the data set names set to private. This allows only those assigned to this area to test these deployed products. The purpose of this first stage is to test or verify that the product is working.
2. Use intermediate test phases for products as they move through various levels of testing. For example you may want to let the application development group as a whole use the product in its test mode prior to moving to production.
3. Move the deployed products to production.

## View a System List

You can view a system list.

### Follow these steps:

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

The detailed deployment information appears on the right side.

### System Name Sort Arrows

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

### Type Sort Arrows

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

### Description Sort Arrows

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

## Add a System

You can add a system to a deployment.

### Follow these steps:

1. Click the Deployments tab.  
The Deployment page appears.
2. On the right, in the Deployments panel click the Current Deployment link.  
A list of current deployments appears.
3. Click the deployment name link.
4. In the System List panel, click Add Systems.  
The Add Systems window appears.
5. Select a system to add and click OK.

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

The Preview window appears, and the system is added.

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

## Remove a System

You can remove a system from a deployment.

### Follow these steps:

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

#### System Name Sort Arrows

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

#### Type Sort Arrows

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

#### Description Sort Arrows

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

4. In the System List panel, select a system you want to remove.
5. Click Remove and then OK to the Remove Products confirmation window.  
The system is removed.

## Deployment Summary

The Action button is available after a successful deployment.

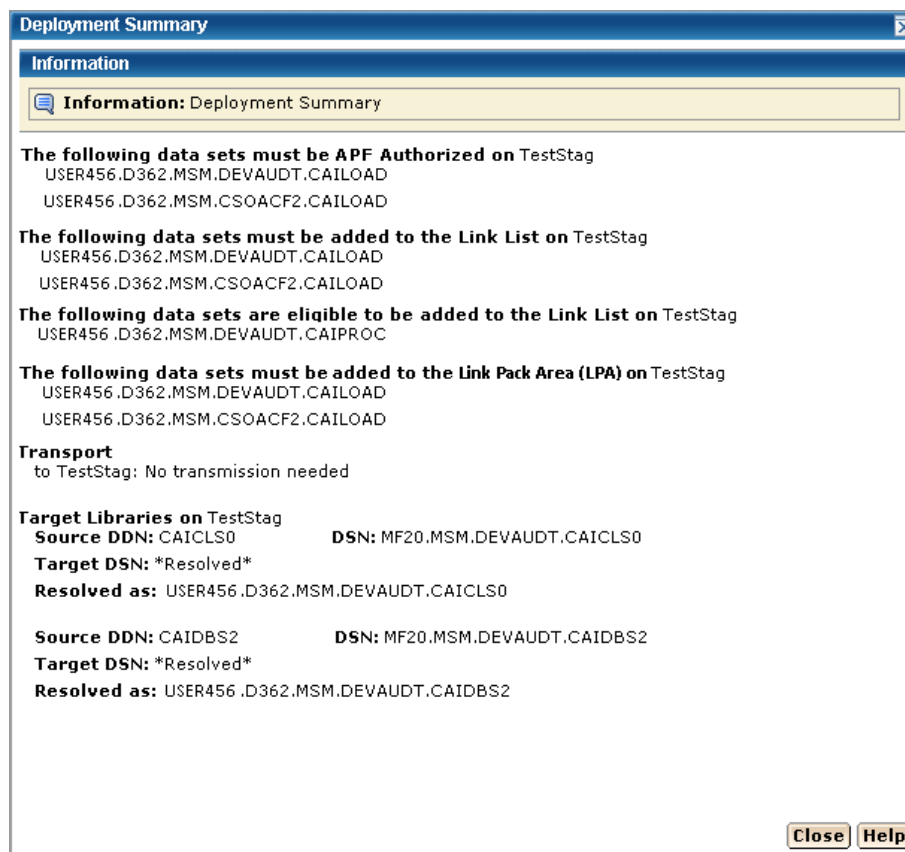
**Important!** Data sets may need to be APF-authorized and added to the Link List and Link Pack Area. These data sets are identified in this dialog.

The Deployment Summary window may contain the following:

- Deployment ID
- Name
- Products
- Systems
- Data Sets actions
- Transport information

- Target libraries including: source, target, and resolved data set names.
- SMP/E environment
- Snapshot path and container

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



**Note:** When you have completed the procedures in this section, go to [Configuring Your Product](#) (see page 153).



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

---

This section contains the following topics:

[How to Install a Product Using Pax-Enhanced ESD](#) (see page 129)

[Allocate and Mount a File System](#) (see page 135)

[Copy the Product Pax Files into Your USS Directory](#) (see page 138)

[Create a Product Directory from the Pax File](#) (see page 143)

[Copy Installation Files to z/OS Data Sets](#) (see page 144)

[Customize the Installation JCL](#) (see page 146)

[Clean Up the USS Directory](#) (see page 146)

## How to Install a Product Using Pax-Enhanced ESD

This section describes the Pax-Enhanced ESD process. We recommend that you read this overview and follow the entire procedure the first time you complete a Pax-Enhanced ESD installation. For experienced UNIX users, the *Pax-Enhanced ESD Quick Reference Guide* has sufficient information for subsequent installations.

**Important!** Downloading pax files for the SMP/E installation as part of the Pax-Enhanced ESD process requires write authority to the UNIX System Services (USS) directories that are used for the ESD process.

If you prefer not to involve all CA Technologies product installers with z/OS UNIX System Services, assign a group familiar with USS to perform Steps 1 through 4 and provide the list of the unpacked MVS data sets to the product installer. USS is not required for the actual SMP/E RECEIVE of the product or for any of the remaining installation steps.

To install files using Pax-Enhanced ESD, use the following process:

1. Allocate and mount the file system. This process requires a USS directory to receive the pax file and to perform the unpack steps. We recommend that you allocate and mount a file system that is dedicated to Pax-Enhanced ESD and create the directory in this file system. Ensure that all users who will be working with pax files have write authority to the directory.

2. Copy the product pax files into your USS directory. To download files, choose one of the following options:

- Download a zip file from CA Support Online to your PC, unzip the file, and then upload the product pax files to your USS file system.
- FTP the pax files from CA Support Online directly to your USS directory.

**Note:** Perform Steps 3 through 6 for each pax file that you upload to your USS directory.

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

```
pax -rvf pax-filename
```

4. Use the SMP/E GIMUNZIP utility to create z/OS installation data sets. The file UNZIPJCL in the directory that the pax command created in Step 3 contains a sample JCL to GIMUNZIP the installation package. Edit and submit the UNZIPJCL JCL.
5. Receive the SMP/E package. Use the data sets that GIMUNZIP created in Step 4. Perform a standard SMP/E RECEIVE using the SMPPTFIN and SMPHOLD (if applicable) DASD data sets. Also, specify the high-level qualifier for the RELFILES on the RFPREFIX parameter of the RECEIVE command.
6. Proceed with product installation. Consult product-specific documentation, including AREADME files and installation notes to complete the product installation.
7. (Optional) Clean up the USS directory. Delete the pax file, the directory that the pax command created, all of the files in it, and the SMP/E RELFILES, SMPMCS, and HOLDDATA data sets.

**More Information:**

[USS Environment Setup](#) (see page 134)

[Allocate and Mount a File System](#) (see page 135)

[Copy the Product Pax Files into Your USS Directory](#) (see page 138)

[Create a Product Directory from the Pax File](#) (see page 143)

[Copy Installation Files to z/OS Data Sets](#) (see page 144)

## How the Pax-Enhanced ESD Download Works

**Important!** To download pax files for the SMP/E installation as part of the Pax-Enhanced ESD process, you must have write authority to the UNIX System Services (USS) directories used for the ESD process and available USS file space before you start the procedures in this guide.

Use the following process to download files using Pax-Enhanced ESD:

1. Log in to <https://support.ca.com/>, and click Download Center.

The CA Support Online web page appears.

2. Under Download Center, select Products from the first drop-down list, and specify the product, release, and genlevel (if applicable), and click Go.

The CA Product Download window appears.

3. Download an entire CA Technologies product software package or individual pax files to your PC or mainframe. If you download a zip file, you must unzip it before continuing.

For both options, [The ESD Product Download Window](#) (see page 131) topic explains how the download interface works.

**Note:** For traditional installation downloads, see the *Traditional ESD User Guide*. Go to <https://support.ca.com/>, log in, and click Download Center. A link to the guide appears under the Download Help heading.

4. Perform the steps to install the product based on the product-specific steps.

The product is installed on the mainframe.

## ESD Product Download Window

You can download CA Technologies product ESD packages multiple ways. Your choices depend on the size of the individual files and the number of files that you want to download. You can download the complete product with all components, or you can select individual pax and documentation files for your product or component.

The following illustration shows sample product files. The illustration lists all components of the product. You can use the Download Cart by selecting one or more components that you need, or selecting the check box for Add All to cart. If you prefer to immediately download a component, click the Download link.

CA Earl - MVS

- [Pax Enhanced Electronic Software Delivery \(ESD\) Guide](#)
- [Pax Enhanced Electronic Software Delivery \(ESD\) Quick Reference Guide](#)
- [Traditional Electronic Software Delivery \(ESD\) Guide](#)
- [Learn more about Using pkzip with your Downloaded Mainframe Products](#)
- [Learn more about downloading components of CA product](#)
- [Mounting ISO Images with OpenVMS](#)

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

**Note:** Related Published Solutions are available on the other results tab on this page. You must add these solutions to your Download Cart to include them with your product files for download.

[View Download Cart](#)

				<input type="checkbox"/> Add All to cart		
Product Components				Add to cart	Download	
CCS - LEGACY - ESD ONLY 140000AW030.pax.Z	14.0 /0000	07/06/2011	4.89MB	<input type="checkbox"/>	<a href="#">Download</a>	
CCS - MFNSM - ESD ONLY 140000AW040.pax.Z	14.0 /0000	07/06/2011	202.01MB	<input type="checkbox"/>	<a href="#">Download</a>	
CCS - BASE - ESD ONLY 140001AW010.pax.Z	14.1 /0000	06/05/2012	27.44MB	<input type="checkbox"/>	<a href="#">Download</a>	
CCS - OPTIONAL - ESD ONLY 140001AW020.pax.Z	14.1 /0000	06/05/2012	14.49MB	<input type="checkbox"/>	<a href="#">Download</a>	
CA EARL PRODUCT PACKAGE 610106AEO00.pax.Z	6.1 /0106	10/30/2008	1.85MB	<input type="checkbox"/>	<a href="#">Download</a>	
EARL PIPPACK AEO61010600.pdf	6.1 /0106	01/29/2010	93.92KB	<input type="checkbox"/>	<a href="#">Download</a>	
CA EASYTRIEVE PRODUCT PACKAGE B60000ESA00.pax.Z	11.6 /0000	07/05/2011	6.12MB	<input type="checkbox"/>	<a href="#">Download</a>	
DATACOM/AD PROD INFO PACKET CAIE00000P0.pdf	14.0 /0000	06/01/2012	220.53KB	<input type="checkbox"/>	<a href="#">Download</a>	
DATACOM/AD XPRESS INSTALL				<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 ordered product files, the Download Method screen could also have these options:

**Note:** For mainframe downloads using this HTTP method, click the Learn More link.

### Download Method

---

Please choose a download method to complete your download request. [Learn More](#)

---

#### HTTP via Download Manager

This is the CA recommended method for download. The Download Manager allows you to download your files faster and more efficiently.

[Download](#)

---

#### Create a Zip File

This method allows you to bundle your download files into one or more zip files of up to 3.5 GB each. These zip files can then be downloaded via HTTP or FTP.

**Note:** Processing is required and an email notification will be sent when your request is ready for downloading.

[Create Zip](#)

The HTTP method lets you start downloading immediately. The FTP method takes you to the Review Orders page that displays your order, first in a Pending status changing to Ready when your order has been processed.

Preferred FTP uses the new content delivery network (CDN). Alternate FTP uses the CA Technologies New York-based FTP servers.

The Create a Zip File option first creates the zip, and when ready, offers the options that the Zip Download Request examples show in the next illustration.

### Review Download Requests

Below is a list of the FTP and large HTTP downloads that have been requested by your site. When status is set to **'Ready'** a link will appear.

- For FTP requests, click on the FTP link to view the path information for your download. For more information view our [FTP Help document](#)
- For HTTP requests, click on the HTTP link to initiate your download.
- To view the details of your request, click on the desired order number.

#### Today's Downloads

Order #	Status	Description	Date Placed	Download Options
<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 that is dedicated to Pax-Enhanced ESD. The amount of space that you need for the file system depends on the following variables:

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

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

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

## Allocate and Mount a File System

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

This procedure describes how to perform the following tasks:

- Allocate a zFS or an HFS.
- Create a mount point in an existing maintenance USS directory of your choice.
- Mount the file system on the newly created mount point.

**Note:** You must have either SUPERUSER authority, or the required SAF profile setting to allow you to issue the USS mount command for the file system.

- Optionally, permit write access to anyone in the same group as the person who created the directory.

**Important!** USS commands are case-sensitive.

**Follow these steps:**

1. Allocate the file system by customizing one of the following samples to your site requirements:

- On a zFS, use the following sample:

```
//DEFINE EXEC PGM=IDCAMS
//SYSPRINT DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//AMSDUMP DD SYSOUT=*
//SYSIN DD *
  DEFINE CLUSTER ( +
    NAME(your_zFS_data_set_name) +
    STORAGECLASS(class) +
    LINEAR +
    CYL(primary secondary) +
    SHAREOPTIONS(3,3) +
  )
/*
//FORMAT EXEC PGM=IOEAGFMT,REGION=0M,
// PARM=(' -aggregate your_zFS_data_set_name -compat')
//SYSPRINT DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//STDOUT DD SYSOUT=*
//STDERR DD SYSOUT=*
//CEEDUMP DD SYSOUT=*
/*
```

- On an HFS, use the following sample:

```
//ALCHFS EXEC PGM=IEFBR14
//CAESD DD DSN=yourHFS_data_set_name,
// DISP=(NEW,CATLG,DELETE),UNIT=3390,
// DSNTYPE=HFS,SPACE=(CYL,(primary,secondary),1)
```

The file system is allocated.

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

2. Create a mount point for the file system. This example shows how to create a /CA/CAESD directory in an existing directory, /u/maint. From the TSO OMVS shell, enter the following commands:

```
cd /u/maint/  
mkdir CA  
cd CA  
mkdir CAESD
```

**Note:** This document refers to this structure as *yourUSSESDdirectory*.

The mount point is created.

3. Mount the file system by customizing one of the following samples to your site requirements:

- On a zFS, use the following sample:

```
MOUNT FILESYSTEM('your_zFS_data_set_name')  
MOUNTPOINT('yourUSSESDdirectory')  
TYPE(ZFS) MODE(RDWR)  
PARM(AGGRGROW)
```

- On an HFS, use the following sample:

```
MOUNT FILESYSTEM('your_HFS_data_set_name')  
MOUNTPOINT('yourUSSESDdirectory')  
TYPE(HFS) MODE(RDWR)
```

The file system is mounted.

4. (Optional) Set security permissions for the directory. You can use the chmod command to let other users access the ESD directory and its files. For example, to allow write access to the ESD directory for other users in your USS group, from the TSO OMVS shell, enter the following command:

```
chmod -R 775 /yourUSSESDdirectory/
```

Write access is granted.

**Note:** For more information about the chmod command, see the IBM *z/OS UNIX System Services User Guide (SA22-7802)*.

## Copy the Product Pax Files into Your USS Directory

To begin the CA Technologies product installation procedure, copy the product pax file into the USS directory that you set up. Use one of the following methods:

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

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

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

Ensure that sufficient free space is available in the USS file system that you are using for Pax-Enhanced ESD to hold the product pax file. If you do not have sufficient free space, error messages similar to the following appear:

```
EZA1490I Error writing to data set  
EZA2606W File I/O error 133
```

When the download finishes, the pax file size in your USS directory matches the value in the Size column for the corresponding pax file on the CA Technologies Products Download window.

**More Information:**

[How the Pax-Enhanced ESD Download Works](#) (see page 131)  
[ESD Product Download Window](#) (see page 131)

## Download Using Batch JCL

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

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

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

### Follow these steps:

1. Supply a valid JOB statement.
2. Replace *yourTCPIP.PROFILE.dataset* with the name of the TCP/IP profile data set for your system. Consult your local network administrators, if necessary.

The job points to your profile.

3. Replace *YourEmailAddress* with your email address.

The job points to your email address.

4. Replace *yourUSSESDdirectory* with the name of the USS directory that you use for ESD downloads.

The job points to your USS directory.

5. Locate the product component to download on the CA Support Product Download window.

You have identified the product component to download.

6. Click Download for the applicable file.

**Note:** For multiple downloads, add files to a cart.

The Download Method window opens.

7. Click FTP Request.

The Review Download Requests window displays any files that you have requested to download.

**Note:** We send you an email when the file is ready to download or a link appears in this window when the file is available.

8. Select one of the following methods:

**Preferred FTP**

Uses CA Technologies worldwide content delivery network (CDN). If you cannot download using this method, review the security restrictions for servers that company employees can download from that are outside your corporate network.

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

**Alternate FTP**

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

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

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

**Note:** The following links provide details regarding FTP: the FTP Help document link in the Review Download Requests window and the Learn More link available in the Download Methods window.

9. Submit the job.

**Important!** If your FTP commands are incorrect, it is possible for this job to fail and still return a zero condition code. Read the messages in the job DDNAME SYSPRINT to verify the FTP succeeded.

After you run the JCL job, the pax file resides in the mainframe USS directory that you supplied.

**Example: CAtoMainframe.txt, JCL**

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

```
//GETPAX JOB (ACCOUNTNO),'FTP GET ESD PACKAGE',
//          MSGCLASS=X,CLASS=A,NOTIFY=&SYSUID
//*****
/* This sample job can be used to download a pax file directly from *
/* CA Support Online to a USS directory on your z/OS system.      *
/*                                                                *
/* When editing the JCL ensure that you do not have sequence numbers *
/* turned on.                                                    *
/*                                                                *
/* This job must be customized as follows:                        *
/* 1. Supply a valid JOB statement.                               *
/* 2. The SYSTCPD and SYSFTPD JCL DD statements in this JCL may be *
/* optional at your site. Remove the statements that are not    *
/* required. For the required statements, update the data set   *
/* names with the correct site-specific data set names.         *
/* 3. Replace "Host" based on the type of download method.      *
/* 4. Replace "YourEmailAddress" with your email address.       *
/* 5. Replace "yourUSSESDdirectory" with the name of the USS    *
/* directory used on your system for ESD downloads.             *
/* 6. Replace "FTP Location" with the complete path              *
/* and name of the pax file obtained from the FTP location     *
/* of the product download page.                                *
//*****
//GETPAX EXEC PGM=FTP,PARM='(EXIT',REGION=0M
//SYSTCPD DD DSN=yourTCPIP.PROFILE.dataset,DISP=SHR
//SYSFTPD DD DSN=yourFTP.DATA.dataset,DISP=SHR
//SYSPRINT DD SYSOUT=*
//OUTPUT DD SYSOUT=*
//INPUT DD *
Host
anonymous YourEmailAddress
lcd yourUSSESDdirectory
binary
get FTP_location
quit
```

## Download Files to Mainframe through a PC

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

### Follow these steps:

1. Follow the procedures in [How the Pax-Enhanced ESD Download Works](#) (see page 12) to download the product pax or zip file to your PC. If you download a zip file, first unzip the file to use the product pax files.

The pax or zip file resides on your PC.

2. Open a Windows command prompt.

The command prompt appears.

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

The pax file is transferred to the mainframe.

### Example: FTP Commands

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

```
ftp mainframe
userid
password
bin
lcd C:\PC\folder\for\thePAXfile
cd /yourUSSESDdirectory/
put paxfile.pax.Z
quit
exit
```

## Create a Product Directory from the Pax File

Use the sample job attached to the PDF file as Unpackage.txt to extract the product pax file into a product installation directory.

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

### Follow these steps:

1. Supply a valid JOB statement.
2. Replace *yourUSSESDdirectory* with the name of the USS directory that you use for ESD downloads.

The job points to your specific directory.

3. Replace *paxfile.pax.Z* with the name of the pax file.

The job points to your specific pax file.

4. Submit the job.

The job runs and creates the product directory.

**Note:** If the PARM= statement exceeds 71 characters, uncomment and use the second form of UNPAXDIR instead. This sample job uses an X in column 72 to continue the PARM= parameters to a second line.

## Sample Job to Execute the Pax Command (Unpackage.txt)

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

```
//ESDUNPAX JOB (ACCOUNTNO),'UNPAX ESD PACKAGE ',
// MSGCLASS=X,CLASS=A,NOTIFY=&SYSUID
//*****
//* This sample job can be used to invoke the pax command to create  *
//* the product-specific installation directory.                      *
//*                                                                    *
//* This job must be customized as follows:                          *
//* 1. Supply a valid JOB statement.                                  *
//* 2. Replace "yourUSSESDdirectory" with the name of the USS        *
//*    directory used on your system for ESD downloads.              *
//* 3. Replace "paxfile.pax.Z" with the name of the pax file.       *
//* NOTE: If you continue the PARM= statement on a second line, make *
//*    sure the 'X' continuation character is in column 72.         *
//*****
//UNPAXDIR EXEC PGM=BPXBATCH,
// PARM='sh cd /yourUSSESDdirectory/; pax -rvf paxfile.pax.Z'
//*UNPAXDIR EXEC PGM=BPXBATCH,
//* PARM='sh cd /yourUSSESDdirectory/; pax                            X
//          -rvf paxfile.pax.Z'
//STDOUT DD SYSOUT=*
//STDERR DD SYSOUT=*
```

## Copy Installation Files to z/OS Data Sets

Use this procedure to invoke the SMP/E GIMUNZIP utility to create MVS data sets from the files in the product-specific directory.

### Follow these steps:

1. Locate and read the product readme file or installation notes, if applicable, which resides in the product-specific directory that the pax command created. This file contains the product-specific details that you require to complete the installation procedure.

You have identified the product-specific installation details.

2. Use ISPF EDIT or TSO ISHELL to edit the UNZIPJCL sample job. You can perform this step in one of the following ways:
  - Use ISPF EDIT. Specify the full path name of the UNZIPJCL file.
  - Use TSO ISHELL. Navigate to the UNZIPJCL file and use the E line command to edit the file.

The job is edited.

3. Change the SMPDIR DD PATH to the product-specific directory created by the pax command.

Your view is of the product-specific directory.

4. If ICSF is not active, perform the following steps:
  - a. Change the SMPJHOME DD PATH to your Java runtime directory. This directory varies from system to system.

**Note:** The default Java location is the following:

```
/usr/lpp/java/Java_version
```

- b. Perform one of the following steps:
    - Change the SMPCPATH DD PATH to your SMP/E Java application classes directory, typically /usr/lpp/smp/classes/.
    - Change HASH=YES to HASH=NO on the GIMUNZIP parameter.

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

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

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

6. Submit the UNZIPJCL job.

The UNZIPJCL job completes with a zero return code. Messages GIM69158I and GIM48101I in the output and IKJ56228I in the JES log are acceptable.

GIMUNZIP creates z/OS data sets with the high-level qualifier that you specified in the UNZIPJCL job. You use these data sets to perform the product installation. The pax file and product-specific directory are no longer needed.

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

## Customize the Installation JCL

Customize the installation JCL in the SAMPJCL data set to allocate and load the required data sets.

### To customize the installation JCL

1. Edit and submit the DEFSMPE member of the SAMPJCL data set.  
This job defines and initializes the SMP/E control data sets.
2. Edit and submit the JCL in the INSTPXD member of the SAMPJCL data set.  
Comments in the JCL specify what information you must supply or modify. The job executes successfully with a condition code of 0.

## Clean Up the USS Directory

**Important!** This procedure is optional. Do not use this procedure until you complete the entire installation process.

To free file system disk space for subsequent downloads after downloading and processing the pax files for your CA Technologies product, we recommend removing the files from your USS directory and deleting unnecessary MVS data sets. You can delete the following items:

- Pax file
- Product-specific directory that the pax command created and all of the files in it
- SMP/E RELFILES, SMPMCS, and HOLDDATA MVS data sets

These data sets have the HLQ that you assigned in the UNZIPJCL job.

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

### Follow these steps:

1. Navigate to your Pax-Enhanced ESD USS directory.  
Your view is of the applicable USS directory.
2. Delete the pax file by entering the following command:

```
rm paxfile
```

***paxfile***

Specifies the name of the CA Technologies pax file that you downloaded.

The pax file is deleted.

3. Delete the product-specific directory by entering the following command:

```
rm -r product-specific_directory
```

***product-specific\_directory***

Specifies the product-specific directory that the pax command created.

The product-specific directory is deleted.

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

**Note:** When you have completed the procedures in this section, go to [Configuring Your Product](#) (see page 153).



# Chapter 5: Installing Your Product From Tape

---

This section describes how to install CA TPX.

**Important!** Before installing the product, be sure to review the list of technical considerations that you received with the distribution tape from CA Technologies. This information is vital to performing a successful installation.

**Note:** Use TPX.C... DATA SETS. Use TPX.A... DATA SETS for reference only. TPX.C... DATA SETS are revised to meet installation needs.

The following list contains sample TPX A... LIBRARIES:

- TPX.ABOVDATV
- TPX.ABOVJCL
- TPX.ABOVLOAD
- TPX.ABOVMAC
- TPX.ABOVPENU
- TPX.ABOVSCRI
- TPX.ABOVSRC

The following list contains sample TPX C... LIBRARIES:

- TPX.CBOVDATV
- TPX.CBOVJCL
- TPX.CBOVLOAD
- TPX.CBOVMAC
- TPX.CBOVPENU
- TPX.CBOVSCRI

TPX.CBOVSRC

This section contains the following topics:

[Gather Information](#) (see page 150)

[Copy the INSTALL Data Set](#) (see page 151)

[Access the Online Documentation](#) (see page 152)

[Customize the Installation JCL](#) (see page 152)

## Gather Information

In this task you gather the information needed during the installation process. Record your values in the following table:

Information Required	Value
The job card options you want to use:	
<ul style="list-style-type: none"><li>■ The job name</li><li>■ Accounting information (optional)</li><li>■ The job class</li><li>■ The message class</li><li>■ The user ID for the NOTIFY parameter</li><li>■ The time</li></ul>	
The SMP/E parameters:	
<ul style="list-style-type: none"><li>■ The UNIT name for the SMP/E data sets</li><li>■ The VOLSER for the SMP/E data sets</li><li>■ The data set names for the SMP/E target and distribution load libraries</li><li>■ The data set names for the SMP/E target and distribution GENLIBs</li><li>■ The WORK UNIT and WORK VOLSER for the SMP/E temporary files</li></ul>	
The parameters for all CA TPX non-VSAM data sets:	
<ul style="list-style-type: none"><li>■ A high level qualifier</li><li>■ A UNIT</li><li>■ A VOLSER</li><li>■ A TAPE UNIT for install</li></ul>	
The parameters for all CA TPX VSAM administration data sets:	
<ul style="list-style-type: none"><li>■ The high-level qualifier</li><li>■ The share options. If you are using CA-L-Serv, see the appendix <a href="#">VSAM File Sharing With CA-L-Serv</a> (see page 177). If you are not using CA-L-Serv, see the appendix <a href="#">VSAM File Sharing Without CA-L-Serv</a> (see page 175).</li><li>■ The VOLSER</li></ul>	

Information Required	Value
The CA TPX panel libraries to be loaded (when installing CA TPX). You can select English and any of the following languages:	
■ CUA	
■ Belgian French	
■ Brazilian Portuguese	
■ Danish	
■ Dutch	
■ Finnish	
■ French	
■ German	
■ Italian	
■ Japanese	
■ Norwegian	
■ Spanish	
■ Swedish	
■ Swiss French	
■ Swiss German	
■ Uppercase English	

## Copy the INSTALL Data Set

Create and submit an IEBCOPY job similar to the one shown here. This job copies the SAMPJCL data set from the distribution tape to a DASD volume.

You must supply the values shown in italics:

```
//TPXLOAD JOB supply a job card here
//STEP01 EXEC PGM=IEBCOPY
//SYSPRINT DD SYSOUT=*
//INDD DD UNIT=TAPE,
// VOL=SER=supply here the volser shown on tape label,
// LABEL=(1,SL),
// DISP=OLD,
// DSN=CAI.TPX.SAMPJCL
//OUTDD DD DSN=prefix.SAMPJCL,
```

```
// DISP=(NEW,CATLG),  
// UNIT=SYSDA,  
// VOL=SER=supply a DASD volume here,  
// SPACE=(3200,(900,50,30)),  
// DCB=(LRECL=80,RECFM=FB)  
//SYSIN DD *  
  COPY INDD=( (INDD,R) ),OUTDD=OUTDD
```

The task is complete when your IEBCOPY job executes successfully (with a condition code of 0).

## Access the Online Documentation

The CA TPX documentation set is available on the CA website at <http://ca.com/support>.

## Customize the Installation JCL

Customize the installation JCL in the SAMPJCL data set to allocate and load the required data sets.

### To customize the installation JCL

1. Edit and submit the DEFSMPE member of the SAMPJCL data set.  
This job defines and initializes the SMP/E control data sets.
2. Edit and submit the JCL in the INSTTPX member of the SAMPJCL data set.  
Comments in the JCL specify what information you must supply or modify.  
The job executes successfully with a condition code of 0.

**Note:** When you have completed the procedures in this section, go to [Configuring Your Product](#) (see page 153).

# Chapter 6: Configuring Your Product

---

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

This section contains the following topics:

[Calculate VSAM Storage](#) (see page 153)

[Define APPL Statements](#) (see page 154)

[Copy the Logmode Tables](#) (see page 155)

[Copy the Startup Procedure](#) (see page 156)

[Authorize the Load Library](#) (see page 156)

[Install Other Language Panels](#) (see page 157)

## Calculate VSAM Storage

To calculate the number of VSAM storage records needed for the ADMIN2 file use:

$$\text{VSAM storage records} = \text{profs} + \text{professions} + \text{users} + \text{usersessions}$$

where:

***profs***

Indicates number of profiles

***professions***

Indicates total *number* of sessions in all profiles

***users***

Indicates number of *users*

***usersessions***

Indicates total *number* of sessions for all users

Edit and submit the JCL in the DEFVSAM member of the CBOVJCL data set. Comments in the JCL specify the information that you must supply or modify. The job executes successfully with a condition code of 0.

## Define APPL Statements

This task adds APPL statements to your SYS1.VTAMLST data set. The APPL statements define the following logical units to VTAM:

- CA TPX application
- Virtual terminals
- Virtual printers

The definitions allow the product to establish application sessions with virtual terminals and perform pass-through printing. The definitions are contained in the APTPX member of the CBOVSRC data set.

For a description of the APPL statements see the appendix [APPL Statements](#) (see page 185).

For details on virtual terminals and passthrough printing, see the *Administration Guide*.

To copy the APPL statements to your SYS1.VTAMLST data set you can:

- Edit and submit the TPXAPPL member of the CBOVJCL data set.
- Copy the APTPX member of the CBOVSRC data set using the ISPF copy facility.

### Using TPXAPPL

If you use the TPXAPPL member:

1. Specify the following information in the member:
  - An appropriate job card.
  - A name for the member when it is copied to SYS1.VTAMLST. You can give the member a name other than APTPX, as long as it is specified on the TPXAPPL parameter in the startup procedure.
  - Any required changes to the SYSIN data.

The member containing the APPL statements relating to the product must include these comment lines:

```
*TPX, PRIMARY
*TPX, REBIND
*TPX, SHARE
*TPX, GROUP
*TPX, UNIQUE
*TPX, APPLPPS
*TPX, USERPPS
```



## Copy the Startup Procedure

If you are using CA-L-Serv to manage all or some of the VSAM files, you must copy the startup procedure that you modified as described in the appendix [VSAM File Sharing With CA-L-Serv](#) (see page 177). Do not submit TPXPROC.

### To copy the startup procedure to your PROCLIB

1. If you have deviated from the naming conventions used in this guide, modify the JCL in TPXPROC as necessary:
  - Change the PREFIX parameter to match the prefix specified for the data sets when they were loaded.
  - Make sure the name on the PROC statement is unique for each component installed at your site.
  - Make sure the APPL parameter matches the name of the SYS1.VTAMLST member created when you defined APPL statements.
2. Make sure that the JCL:
  - Allows a region size of at least 4 MB to start the product. You may need to adjust this value for production.
  - Specifies the CBOVPENU panel library in addition to any other panel libraries.
3. To write the log to a data set other than SYSOUT, specify a LOG data set with the specifications:
  - LRECL=131
  - RECFM=FBA

**Note:** Do not set the log destination and class parameters in the System Options Table (SMRT) if logging is done to a non-SYSOUT data set.
4. Submit the JCL for the TPXPROC job. The job executes with a condition code of 0.

## Authorize the Load Library

CA TPX must run from an APF-authorized library if you intend to use the following features:

- VTAM Authorized Path Facility
- VSAM file sharing
- VTAM Generic Resource Option
- TCPaccess Telnet Server interface

To authorize the CA TPX load library and any user load library, you must add them to SYS1.PARMLIB using one of the following methods:

- The older Authorized Program Facility List (IEAAPFxx) method
- The newer APF portion of Authorized Program List, Exits, LNKST Sets and LPA (PROGxx) method

**Note:** For detailed information, see the *IBM z/OS MVS Initialization and Tuning Reference* for your release of the operating system.

## Authorize the Load Library Using IEAAPFxx Method

### To authorize the Load Library using the IEAAPFxx method

1. Add the data set name and volume of the load library to SYS1.PARMLIB(IEAAPFxx).
2. Add the data set name and volume of the CA TPX USERLIB to SYS1.PARMLIB(IEAAPFxx).
3. If you have a separate load library that contains your exit routines, add an entry in IEAAPFxx for that library as well.

**Note:** The xx in IEAAPFxx is the suffix of the authorization list specified in IEASYSxx.

## Authorize the Load Library Using PROGxx Method

### To authorize the Load Library using the PROGxx method

1. Add the data set name and volume of the load library using the ADD APF statement to SYS1.PARMLIB(PROGxx).
2. Add the data set name and volume of any CA TPX user library using the ADD APF statement to SYS1.PARMLIB(PROGxx).
3. If you have a separate load library that contains your exit routines, add an entry in PROGxx for that library as well.

**Note:** The xx in PROGxx is the suffix of the authorized program list specified in IEASYSxx.

## Install Other Language Panels

Besides the default English panels, TPX also supports panels in the following languages:

- Belgium French
- Brazilian Portuguese
- Danish

- Dutch
- Finnish
- French
- German
- Italian
- Japanese
- Norwegian
- Swiss French
- Swiss German
- Spanish
- Swedish
- Upper Case English

### **To add one or more panel libraries**

- Installing from files produced by the ESD process

Edit and submit the JCL in the INSTPNLD member of the CBOVJCL data set.

Comments in the JCL specify what information you must supply or modify. The job executes successfully with a condition code of 0.

# Chapter 7: Starting Your Product

---

This chapter describes how to start and log on to CA TPX for the first time.

**Note:** If your site is using CA-L-Serv to manage the VSAM files, you must start CA-L-Serv before you start CA TPX. See the CA Common Services for z/OS documentation.

This section contains the following topics:

[Issue Console Commands](#) (see page 159)

[Log On a Terminal to CA TPX](#) (see page 159)

[Sign On to CA TPX](#) (see page 161)

[Stop CA TPX](#) (see page 161)

## Issue Console Commands

To start the product, issue the console commands:

```
V NET,ACT,ID=APTPX  
S TPX
```

You receive startup messages followed by a message that the product is accepting logons.

**Note:** If your site is using CA-L-Serv to manage the ADMIN1 or ADMIN2 files, and CA-L-Serv is unavailable, the product abends with a U001 abend. If your site is using CA-L-Serv for the NOTES, MAIL, or VIEW files only, the product will start without those files and will wait for CA-L-Serv to become available.

## Log On a Terminal to CA TPX

When you have started the product, establish a connection between it and your terminal by issuing the command:

```
LOGON APPLID(TPX)
```

**Note:** The command you issue can have a different format if the VTAM system programmer at your site has altered the distributed Unformatted System Services (USS).

The USS component of VTAM converts this command to a request to initiate the application. VTAM honors this request as long as you have done both of the following:

- Defined a primary logical unit (PLU) named TPX on an APPL statement in the SYS1.VTAMLST data set.
- Activated the product by issuing the console commands specified in the section Starting CA TPX.

If using the TCPAccess Telnet Server interface, the 3270 emulator settings must specify the host IP address and port assigned to CA TPX in the Server. When the IP session is established, the user will see the TPX logon screen.

## The Default Logo Panel

In response to the logon command, the default Logo panel appears, shown here:

```
          .....          @@@@@@@@@@ @@@@@@@@@@ @@@@@ @@@@
          .              @ @ @ @ @ @ @ @ @ @ @ @ @ @ @ @
cccccc  aaaaaa .      @ @ @ @ @ @ @ @ @ @ @ @ @ @ @ @
cc . c   aa  aa .    @ @ @ @ @ @ @ @ @ @ @ @ @ @ @ @
cc .     aa   aa .   @ @ @ @ @ @ @ @ @ @ @ @ @ @ @ @
cc .     aaaaaa .   @ @ @ @ @ @ @ @ @ @ @ @ @ @ @ @
cc .     aa  aa .   @ @ @ @ @ @ @ @ @ @ @ @ @ @ @ @
cc . c   aa  aaa . @ @ @ @ @ @ @ @ @ @ @ @ @ @ @ @
cccccc  aaaa aa . @ @ @ @ @ @ @ @ @ @ @ @ @ @ @ @
          .          @ @ @ @ @ @ @ @ @ @ @ @ @ @ @ @
          .....          @@@@@@ @@@@@@ @@@@@ @@@@@

          Copyright (c) 2010 CA, INC.
Userid:          (or LOGOFF)          08:16:05
Password:                                     05/15/03
New Password:          TERMID01
Account:              3279-2A
Transfer:              SMRT51

          CA TPX Session Management (TM)

PF1=Help   PF3=Logoff
```

The statements defining this screen initially reside in the T/n0003 member of the language panel data set, where *ln* specifies a language code. For a list of available languages, see [Install Other Language Panels](#) (see page 157).

## Sign On to CA TPX

After the Logo panel appears, you can sign on to the product. Enter the pre-existing administrative user ID, TPXADMIN, which has unlimited authority.

**Note:** If CA TPX is used exclusively to administer CA STX, use the STXADMIN user ID.

If your site has not loaded the administration files, you need to add the TPXADMIN user ID with the Batch facility. JCL in the TPXADMIN member of the TPX.CBOVSRC will add this ID to your administration files.

To sign on to an LU1 terminal, enter the user ID and password, separated by a slash (/).

After the product accepts and processes your user ID, the Menu panel appears as shown in the following sample panel:

```

                                TPX MENU FOR      TPXADMIN
Cmdkey=PF12/24   Jump=PF20      Menu=PF19      Panelid - TEN0041
Print=NONE       Cmdchar=/      Model - ABDC1234
                                System - TPXPROD

      Sessid      Sesskey      Session Description      Status
_  TSO            PF 5        TSO on System1
_  IMS            PF 6        IMS Production
_  CICS           PF 7        CICS Test System
_  TPXADMIN       PF 8        TPX Administration
_  TPXMAIL        PF 9        TPX Mail System
_  TPXNOTES       PF 10       TPX Notepad
_  WINDOWS        PF 2        TPX Windows

Command ==>
PF1=Help  PF7/19=Up  PF8/20=Down  PF10/22=Left  PF11/23=Right  H =Cmd Help

```

After signing on, you can establish virtual terminal sessions with any application in your VTAM network except those that require the terminal to be predefined.

For instructions on using the menu, see the *User Guide*.

## Stop CA TPX

To stop CA TPX, issue the console command:

```
P TPX
```

For information on stopping CA-L-Serv, see the CA Common Services for z/OS documentation.



# Chapter 8: Post-Installation Tasks

---

This chapter gives a brief explanation of customization tasks and describes where you can find detailed information.

This section contains the following topics:

- [Use Authorized Path Facility](#) (see page 163)
- [Define the Coupling Facility Structure](#) (see page 163)
- [Enable the TCPAccess Telnet Server Interface](#) (see page 164)
- [Define Administrators](#) (see page 165)
- [Define System Options and Applications](#) (see page 165)
- [Define Operator Capabilities](#) (see page 166)
- [Define Users](#) (see page 166)
- [Write ACL/E Program](#) (see page 168)
- [Set Up VSAM Sharing](#) (see page 168)
- [Implement a Signon and Signoff Exit](#) (see page 169)
- [MAIL and VIEW Files](#) (see page 169)

## Use Authorized Path Facility

With the load modules in an authorized library, the product can run as a non-swappable application and use the VTAM Authorized Path Facility (APF) and write SMF records. The APF facility saves 20 to 30 percent of your CPU overhead. The APF facility is required for VTAM generic resource support.

### To use VTAM Authorized Path Facility

1. Specify Y in the VTAM Authorized Path Facility field of the Performance Parameters panel.  
  
For information about changing the performance parameters, see the *Administration Guide*.
2. Specify YES on the SRBEXIT parameter of each APPL statement in your major node.

## Define the Coupling Facility Structure

When using CA TPX to operate as a VTAM generic resource, you need to define the Coupling Facility structure.

**Note:** To use this feature, CA TPX must run from an APF-authorized library.

#### To define the Coupling Facility structure

1. Open member CFSTRUCT in the CBOVJCL data set.
2. Define the name of your structure and its size. Note the structure name consists of two parts:
  - An eight-byte prefix, which cannot contain blanks.
  - The generic resource name used for all instances of the product. You may need more than one generic resource name.

**Note:**

Each generic resource name requires its own structure.

For details on determining the structure storage requirements, see the *Programming Guide*.

3. Update the z/OS policy data set to reflect the definition of the structure.
4. Once CA TPX is installed and running, update the generic resource parameters using the System Options Table Menu and then recycle CA TPX. For more information, see the *Administration Guide*.

## Enable the TCPaccess Telnet Server Interface

The TCPaccess Telnet Server interface provides native IP support.

**Note:** To use this feature, CA TPX must run from an APF-authorized library.

Note the following:

- The interface is mutually exclusive with the VTAM Generic Resource Option.
- When using the interface, CA TPX provides TN3270 Server services in coordination with TCPaccess; therefore, the following CA TPX features will not be available when the interface is used:
  - Affinity feature
  - Pass Mode
  - The Pass Option on application definitions

## Customize the JCL

Review the samples of TPXPROC and the CA TPX startup job stream you are using.

The ddname of VTAMLIB must point to the loadlib where the Modetab used to define terminal characteristics resides. This library is usually SYS1.VTAMLIB and is coded as such in the sample; correct it as necessary. The MODETAB parameter on the startup procedure identifies the mode table CA TPX is to use for terminal characteristics. If the MODETAB parameter is omitted, the default value of ISTINCLM is used.

## Activate the Feature

After CA TPX is installed and running, you must set an option in the System Options Table (SMRT) to activate the interface.

Under System Features in the SMRT, specify Y in the Activate TCPAccess Telnet Interface field. For information about setting parameters in the SMRT, see the *Administration Guide*.

Recycle CA TPX to effect the change.

For information about activating the CA TPX interface on the TCPAccess Telnet Server, see the *CA TCPAccess Telnet Server Customization Guide*, the appendix "Native IP Interface."

## Define Administrators

CA TPX allows you to distribute the responsibility for administration among several types of administrators. The capabilities of each administrator are assigned by a Master Administrator. To perform administration, you must define these administrators in an online administration session.

For instructions for defining administrators and running an online administration session, see the *Administration Guide*.

## Define System Options and Applications

System administration gives you control over the operating environment. You must define the components for the VTAM network at your site and provide the product with information about applications, physical terminals, and printers. You also specify default system, application, and user characteristics.

For procedures relating to system administration, see the *Administration Guide*.

For a list of applications that require special customization tasks and the related procedures for these applications, see the *Programming Guide*.

## Define Operator Capabilities

You can define the capabilities of operators by creating and maintaining operator command classes.

For instructions on specifying operator capabilities, see the *Administration Guide*.

To learn about the tasks operators perform in an operator session, see the *Operator Guide*.

For information about messages, see the *Message Reference Guide*.

## Define Users

You can define users by using online or batch administration.

For information about performing user administration using the online facility, see the *Administration Guide*.

For information about performing user administration using the batch facility, see the *Batch Administration Guide*.

How you define user characteristics depends on what type of user you are defining, static or dynamic.

### Static Users

Static users are defined in user administration and recorded in the administration databases. The characteristics of a static user are determined during signon by values in the System Options Tables, Application Definition Tables, and user and profile records.

**Note:** For a description of how user characteristics are determined, see the *Administration Guide*.

### Dynamic Users

Dynamic users are not recorded in the administration databases. The characteristics of dynamic users are determined by profiles assigned in the signon exit. User validation and profile selection can be determined at signon through interaction with an external security package. The default signon exit provides for this method of dynamic user management and almost eliminates the need for ongoing user maintenance in CA TPX.

Options in the System Options Table (SMRT) determine if CA TPX accepts dynamic users. For information about the SMRT, see the *Administration Guide*.

The product also allows saved dynamic users.

Dynamic users cannot be administered because no record of them is kept in the ADMIN2 database. A user is either static or dynamic, and cannot be static for one component and dynamic for the other.

## Allow Dynamic Users

To allow dynamic users, specify Y in the Dynamic Users Allowed field of the System Options Table (SMRT). The signon exit determines the profiles that are assigned to dynamic users.

**Note:** For more information on the signon exit, see the *Programming Guide*.

## Convert Dynamic Users to Static Users

You can convert dynamic users to static users. This conversion can be set to take place automatically when the dynamic users sign on to the product. This procedure can be used to add new static users when they sign on, without having to administer them individually with online or batch administration.

## Convert Users to a Different Type

### To convert dynamic users into static users with signon privileges

1. Set the following fields to Y in the System Options Table (SMRT):
  - Allow Dynamic Users
  - Save Dynamic Users
  - Optional Parameter 18
2. Have users at your site sign on to the product at their convenience. The users will be assigned user characteristics as if they were dynamic users and these values will become their characteristics as static users. As soon as they sign on, they become static users with signon privileges.

A user administrator can also use the Static User field in User Options to determine whether a user is static or dynamic. This applies only to saved dynamic users.

**Important!** Remember to set Optional Parameter 18 to N after your users have become static to prevent spurious user IDs from being stored in your administration file.

## Saved Dynamic Users

Saved dynamic users have the following features:

- Like dynamic users, the profiles specified in the signon exit (and optionally determined through interaction with external security) determine their session options.
- Unlike dynamic users, their user options are saved in the ADMIN2 database and can be modified by a user administrator or through self-maintenance.
- When profiles for a user for which CA TPX maintains user customization are no longer authorized by the signon exit or external security, those customizations are deleted at signon time. User IDs must be deleted manually.

Allowing saved dynamic users at your site gives you the convenience of dynamic users with the additional benefit of being able to administer them.

To allow saved dynamic users at your site, set the Save Dynamic Users option to Y in the System Options Table (SMRT). With this option turned on, all users who sign on dynamically become saved dynamic users.

The Static User field in the User Options panel can be set by a user administrator to change a saved dynamic user into a static user (or conversely). If a saved dynamic user becomes a static user, the profiles that were assigned when the user signed on are recorded in the user record and will be the profiles of the user every time the user signs on. The profiles of the user are no longer determined by the signon exit.

## Write ACL/E Program

The product provides an automated conversation language (ACL/E) to help you automate and simplify information exchanges between users and their applications. The ACL/E program provides input in place of the user during user-application interactions.

For information on developing and using ACL/E programs, see the *ACL/E Programming Guide*.

For information on user interaction with applications through the product, see the *User Guide*.

## Set Up VSAM Sharing

You can set up the product to allow the VSAM administration data sets to be shared. This allows you to run multiple regions and run batch administration while running the product online.

**More information:**

[VSAM File Sharing Without CA-L-Serv](#) (see page 175)

## Implement a Signon and Signoff Exit

You can either use the default signon and signoff user exit, TPXUSNSF, which is distributed in the TPX.CBOVSRC, or use a signon and signoff exit of your own. If you do not specify a signon and signoff exit, the product uses the default exit.

**Note:** For information about the signon and signoff user exit, see the *Programming Guide*.

## MAIL and VIEW Files

The installation procedure included allocation for the MAIL and VIEW files, which are VSAM files used by CA TPX for the Mail and View facilities.

If your site is not authorized to use the View facility or the MAIL facility, you do not need these files and can delete them. However, the VIEW file includes sample session recordings for use with the Record/Playback feature of the View facility. These sample recordings can be played back even if you are not authorized for View. The samples contain examples demonstrating the use of some features.



# Chapter 9: Migration Information

---

This chapter describes considerations when migrating from a previous release of CA TPX.

This section contains the following topics:

[Migration from Releases Prior to r4](#) (see page 171)

[Coupling Facility System Managed Rebuild](#) (see page 171)

[Migration Checklist](#) (see page 171)

## Migration from Releases Prior to r4

r5.3 can share files with r4 and above. Administration should be performed from r5.3. Any settings in r5.3 that are not recognized by older releases are ignored and the associated functionality is not present when executing the older release.

## Coupling Facility System Managed Rebuild

If r5.3 and any release prior to r5.2 are connected to the same Coupling Facility structure, a request to rebuild or alter the structure will be rejected by the operating system. To exploit the system managed rebuilding or altering of the Coupling Facility structure, all instances must be running either r5.2 or r5.3.

## Migration Checklist

Use this checklist when migrating to a new release of CA TPX:

- Use the file allocations from the new CA TPX as delivered.
- Make a backup of your old CA TPX VSAM files.
- Copy the CA TPX VSAM file backups into the new allocated VSAM files.
- Verify that LOADLIB is APF authorized.
- Run RESET INTEGRITY (refer to CBOVSRC library, member BATCHINI).
- Migrate any custom ACL/E programs to the new ACL/E library.
- Migrate any custom PANEL libraries to the new PANEL library.
- Reassemble all custom user exits against the new libraries.
- Modify the new CA TPX startup procedure to refer to tables from migrated files (for example, SMRT, ACT, and so on).

- Review new SMRT parameters:

1. Take screen prints of each SMRT panel in your existing release.
2. Create a new SMRT in the new release and take screen prints of these.
3. Compare both the SMRTs to identify new fields and their defaults.

If you apply no changes to the SMRT in the new release, the defaults will be in effect for any new fields introduced since your existing release.

**Note:** As of r4, VSAM files are upwardly compatible and do not require conversion.

# Chapter 10: Frequently Asked Questions

---

The following questions and answers will help you get started using CA TPX and its various features.

This section contains the following topics:

[FAQs](#) (see page 173)

## FAQs

**Q: What is the recommended dispatch level?**

A: Set the dispatch level to below VTAM and the TN3270 Server, but higher than applications that CA TPX communicates with (CICS, IMS, TSO, and so on), regardless of whether CA TPX is defined as a generic resource.

**Q: Does a new service pack require that I reinstall the software?**

A: No.

**Q: What are the requirements to enable system managed rebuild and the ALTER command for the Coupling Facility structure used by CA TPX?**

A: All instances of CA TPX connected to the structure must be r5.1, r5.2, or r5.3. The operating system and CFLEVEL must support this functionality.

**Q: When signing on, I get message IENS008A (THE SECURITY SYSTEM IS INACTIVE), but RACF is active. What is wrong?**

A: CA TPX has called RACF to validate the user ID and password submitted during signon. An abend occurred in RACF processing that was percolated up to CA TPX. CA TPX recovers from the abend and indicates the external security system is unavailable. This condition should be reviewed. It is likely that the security file was locked at the time and normal processing will resume when the condition is cleared. If it becomes necessary to obtain a dump of this condition, a SLIP trap should be set for the appropriate abend code with the address spaces to be dumped.

**Q: Do I need to code the new switch-in exit (TPXUSWIN)? CA TPX successfully refreshed the screen in my shop.**

A: You do not need to code the exit. CA TPX will use the current methods (that is, those used in r5) to refresh the screen image. The exit is intended for those applications that make heavy use of graphics and have the capability of refreshing the screen image on their own.

**Q: Qualified pass ticket works when my application is running on the same instance of the operating system as CA TPX, but if I move it to another instance, the logons are rejected by the application. What did I do wrong?**

A: The pass ticket profile in the external security system used for pass ticket generation and validation for any given application must be identical. When security systems do not share the same security database, a mismatch can occur resulting in a validation failure for a good ticket.

**Q: Can CA TPX use qualified pass tickets when RACF is the security system on the operating system image on which the target application resides?**

A: Yes. To generate qualified pass tickets, CA TPX requires CA Top Secret or CA ACF2 to be the active security system on the operating system image on which CA TPX is active. An appropriate pass ticket profile must be defined to the eTrust solution. When the appropriate pass ticket profile is defined to RACF for an application, RACF can interpret a qualified pass ticket generated by CA TPX in conjunction with one of the previous eTrust solutions.

**Q: I already have a TN3270 Server from a vendor other than CA. Can CA TPX communicate directly with that server?**

A: No. CA developed a high-speed protocol between CA TPX and TCPaccess Telnet Server to provide the fastest means with the least overhead for transferring data between the solutions and moving the data to its final destination. CA TPX can use standard VTAM LU0 or LU2 sessions to communicate with TN3270 servers from other vendors.

# Appendix A: VSAM File Sharing Without CA-L-Serv

---

This appendix describes VSAM file sharing managed directly by CA TPX and the required setup procedure.

This section contains the following topics:

[How It Works](#) (see page 175)

[Allow VSAM Sharing Without CA-L-Serv](#) (see page 176)

## How It Works

In CA TPX, the VSAM data sets are shared by setting VSAM share options to (4,3). ENQ/DEQ logic manages the sharing process.

The ENQ uses a RESERVE to serialize access to the VSAM data sets. The qname of this ENQ is TPXMS. If the VSAM data set is cataloged in an ICF catalog, the rname is the name of the data set. If the VSAM data set is not cataloged, the rname is the data definition name, ADMIN1, ADMIN2, MAIL, NOTES, or VIEW. Testing has shown that converting the RESERVE using a product such as CA MII is not necessary and increases the overhead associated with the cross-system sharing process.

**Important!** The overhead associated with this serialization causes considerably higher I/O rates to the VSAM data sets.

Sharing information about each VSAM data set is maintained in record zero of the data set (the key consists of 17 "0"s). The VSAM shared information (VSI) for the Data and Index data sets is written to record zero to pass the information cross-system. If any VSAM data set is restored or moved, the information in control record zero becomes inaccurate, so it must be deleted. You can use batch administration to delete control record zero. For more information, see the *Batch Administration Guide*.

If a VSAM data set is coded as DISP=SHR in the DD statement in the startup procedure, that data set will be shared.

## Allow VSAM Sharing Without CA-L-Serv

### To allow VSAM sharing in your system

1. Set the VSAM share options on each VSAM data set to (4,3).
2. Specify DISP=SHR in the DD statement for any data set that is to be shared.
3. Re-evaluate your usage of the option Reserve ACB's at startup on the Performance Parameters panel in the System Options Table (SMRT). If it is set to Y, startup will be slowed down significantly when VSAM sharing is used.

The option Reserve ACB's at startup causes the product to read the entire ADMIN2 data set, searching for user records that have ACB names that are fully qualified (consist of eight characters and no masks). With VSAM sharing this process is slow.

You must set this option to Y only if you have assigned users a fully qualified ACB name through User Administration. If you have assigned users by using masking, the Reserve ACB's at startup option can be set to N.

If you must reserve specific ACBs for specific users, in most cases you can set up masking rules to accomplish this. If you cannot use masking, using either the ACB Selection Exit or the OPENGATE feature can eliminate the need for using the Reserve ACB's at startup option.

4. Authorize the load library on each system that CA TPX runs on.
5. Re-evaluate the placement of the VSAM data sets. You can move them to minimize the effects of the RESERVEs used to serialize access to the data sets.

**Note:** Sharing is not possible for VM systems or non-authorized copies of this product. If you select sharing and do not authorize CA TPX, an abend will occur.

# Appendix B: VSAM File Sharing With CA-L-Serv

---

This appendix briefly discusses CA-L-Serv and explains how to customize CA TPX and CA-L-Serv to allow CA-L-Serv to manage CA TPX VSAM files.

**Note:** For detailed information on CA-L-Serv, see the CCS for z/OS documentation.

This section contains the following topics:

[CA-L-Serv Benefits](#) (see page 177)

[File Sharing With CA-L-Serv](#) (see page 177)

[How to Customize CA TPX](#) (see page 179)

[How to Customize CA-L-Serv for CA TPX](#) (see page 180)

[Installation Checklist](#) (see page 182)

## CA-L-Serv Benefits

CA-L-Serv is a master started task that provides standard services used by many CA products.

CA-L-Serv can simplify VSAM file sharing for different combinations of CA TPX on one or more z/OS systems. CA-L-Serv can:

- Provide easier cross-system VSAM file sharing among multiple copies of CA TPX operating on different systems.
- Improve file security by establishing CA-L-Serv as the only user that can access the VSAM files.
- Provide a log containing the key of each VSAM record that has been updated through CA-L-Serv.
- Provide less disruptive backup and restore operations by allowing maintenance on individual VSAM files without taking down CA TPX.

## File Sharing With CA-L-Serv

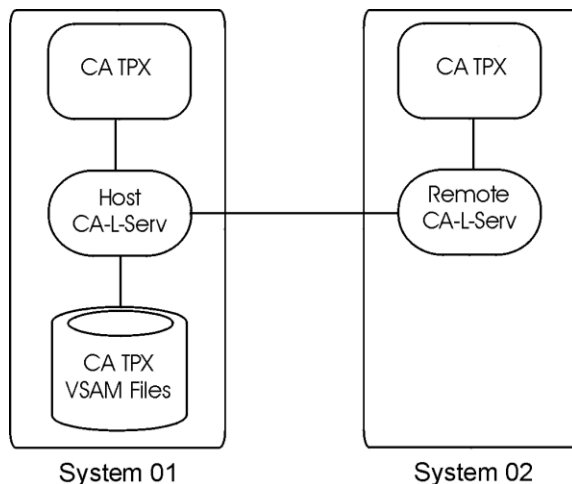
When using CA-L-Serv, CA TPX accesses the VSAM files through the CA-L-Serv file server component. Only CA-L-Serv has direct access to the files. It takes read and write requests from CA TPX and determines the correct VSAM file to access.

Control record zero, which contains VSAM sharing information when CA-L-Serv is not used, is deleted when the VSAM files are opened for update.

## CA-L-Serv Cross-system Sharing

With CA-L-Serv managing the files, you can share VSAM files across systems, even when shared DASD is not available. In this case, CA-L-Serv must exist on each system with the communications server providing cross-system communication.

A single CA-L-Serv, defined as the *host*, manages the VSAM files, while the other CA-L-Servs are defined as *remote*, as in the following illustration:



**Note:** If your site is using one CA-L-Serv on one system, the CA-L-Serv must be defined as *local*.

## If CA-L-Serv Becomes Unavailable

CA TPX will detect when CA-L-Serv or any of the files managed by CA-L-Serv cannot be accessed. CA TPX will mark the affected files as unavailable and periodically attempt to access them.

The period between attempts is the CA-L-Serv Recovery Retry Interval. The default interval is 120 seconds. You can set the interval in the System Options Table (SMRT) after CA TPX has been installed and started.

When the files become available, the CA TPX accesses them and marks them available.

You can determine the status of the VSAM files by issuing the D FILES command in a TPXOPER session.

---

## How to Customize CA TPX

This section explains how to customize the CA TPX startup procedure to allow VSAM file sharing with CA-L-Serv.

### Omit DD Statements

If you want TPX to access a VSAM file through CA-L-Serv, omit the DD statement for that file from the CA TPX startup procedure.

### Identify CA-L-Serv to CA TPX

CA TPX must recognize the CA-L-Serv subsystem name to establish communication. To identify the subsystem name to the product, place the following statement in the startup procedure:

```
//SSN$name DD DUMMY
```

The default subsystem name is LSRV. The subsystem name is assigned to CA-L-Serv when CA-L-Serv is installed.

### Specify the DDname Prefix

You must specify a DD statement in the startup procedure to specify the CA-L-Serv ddname prefix. The prefix is a four-letter code. The VSAM files are defined to CA-L-Serv with the same prefix. CA-L-Serv allows CA TPX to access files with the matching prefix. Different copies of CA TPX can use different prefixes, which allows CA-L-Serv to control the sharing of different file sets concurrently.

Place the following statement in the startup procedure to define the prefix:

```
//DDN$prefix DD DUMMY
```

By specifying the same prefix in the startup procedure of another CA TPX, both copies will share the same VSAM files.

### Specify the ICSN

You can include an ICSN= statement in the JCL EXEC parameters indicating the intercommunications system name of CA TPX. CA-L-Serv uses this name to identify this copy.

The default ICSN is the started-task name.

## How to Customize CA-L-Serv for CA TPX

This section explains how to customize CA-L-Serv to manage the CA TPX VSAM files.

You must modify the startup procedure to specify which files are being managed by which CA-L-Serv.

Also, you must structure the CA-L-Serv parameter data sets, which contain members that provide operating values to CA-L-Serv and issue CA-L-Serv commands.

### Specify the Files CA-L-Serv Manages

You must specify to CA-L-Serv the VSAM files it is managing.

Use the ddname prefix, as described in [Specify the DDname Prefix](#) (see page 179), to identify which files will be accessed by each CA TPX instance.

For example, use the following ddnames for the VSAM files if you are using the ddname prefix **TPXV**:

```
TPXVADM1  
TPXVADM2  
TPXVNOTE  
TPXVMAIL  
TPXVVIEW
```

When using CA-L-Serv to manage file sharing, you must ensure that CA-L-Serv is the *only* address space with update access to the files. To ensure adequate protection, you must carry out the tasks described in the following paragraphs.

### Specify the Disposition and Share Options

To ensure adequate protection for the files, you must carry out the following tasks:

- Set the VSAM share options for managed files to (1,3) or (2,3). This takes advantage of CA-L-Serv performance advantages and is required to ensure restricted access to the managed files.
- Set the VSAM option for managed files to REUSE.
- Set the disposition of managed files to DISP=OLD in the CA-L-Serv startup procedure.

To do this, override the default (DISP=SHR) using the following steps:

1. Code a DD statement explicitly for the file in the CA-L-Serv startup JCL.
2. Code the ADDFILE command for the file with the ddname but *without* the data set name.

Unless you perform these steps, the ADDFILE command will allocate the file with DISP=SHR, and the file can be exposed to unauthorized updates.

When a file is allocated with DISP=OLD, it cannot be browsed online while under CA-L-Serv management, and the CA-L-Serv IFSYS command cannot be used to run multiple copies of CA-L-Serv with the same initialization commands and startup procedures. Using the IFSYS command in this manner would cause the multiple copies of CA-L-Serv to attempt to allocate the same files with DISP=OLD.

## Propagate ENQs

The following ENQs must be propagated across all systems that share the DASD on which the managed files reside:

- The LSERVDSN ENQ. This is issued by CA-L-Serv against a VSAM file when the file is placed under CA-L-Serv management with an ADDFILE command. This ENQ is used to determine whether CA-L-Serv is managing the file.
- The SYSVSAM ENQ. This is issued by VSAM when a VSAM OPEN takes place. Share options of (1,3) or (2,3) use this ENQ to restrict update access to the file.
- The SYSDSN ENQ. This is issued by z/OS when an OPEN takes place against a data set that is coded DISP=OLD.

You can use a product that propagates ENQ requests globally, such as CA MII Data Sharing. Your site probably already has methods to propagate the SYSVSAM and SYSDSN ENQs.

## Use Private Buffer Pools

We recommend that you use private buffer pools. Private buffer pools are used by default-you do not have to specifically assign files to them. Do not use local shared resource (LSR) buffer pools.

## Sample Members

The CBOVJCL data set includes the following members that pertain to CA-L-Serv:

### LSVTPX

CA-L-Serv startup commands for CA-L-Serv managed access to all VSAM files for the component of CA TPX.

### LSNVIMG

CA-L-Serv log messages indicating the beginning and end of sessions with CA-L-Serv.

## Installation Checklist

The following tables provide a checklist for installing and customizing the CA-L-Serv and the CA TPX components:

General	Completed
VSAM files that are managed by CA-L-Serv are managed by a single CA-L-Serv.	
Each VSAM file is accessed through CA-L-Serv or directly by TPX, but not both.	
Implement a security package to restrict access to the VSAM files.	
Ensure that the LSERVDSN, SYSVSAM, and SYSDSN ENQs are propagated as necessary.	
CA-L-Serv Installation	Completed
CA-L-Serv startup parameters match those in sample CA-L-Serv startup members, after any required customization for your site.	
The CA-L-Serv that is managing the product files is defined as <i>host</i> if you are cross-system sharing or <i>local</i> if you are not.	
All CA-L-Servs defined as remote have the same z/OS subsystem name as the host CA-L-Serv	
The CA-L-Serv file server is active on each CA-L-Serv system.	
If your site is performing file sharing with more than one CA-L-Serv, the CA-L-Serv communications server is active on each CA-L-Serv system.	
Each CA-L-Serv communication server has the correct VTAM applid.	

---

<b>CA-L-Serv Installation</b>	<b>Completed</b>
All VSAM files that are managed by CA-L-Serv have VSAM sharing options of (1,3) or (2,3).	
An ADDFILE command is present for each file that CA-L-Serv is managing.	
Each file that CA-L-Serv is managing has a DD statement specifying DISP=OLD in the startup procedure of the local or host CA-L-Serv.	
<hr/>	
<b>CA TPX Startup Procedure</b>	<b>Completed</b>
The CA-L-Serv subsystem name specified in the startup procedure matches that of the CA-L-Serv system with which the product must communicate.	
The ddname prefix specified in the startup procedure matches that used in the CA-L-Serv ADDFILE commands.	
A DD statement is present for each VSAM file that is to be accessed directly by TPX	
.The Intercommunications System Name (ICSN), which identifies each component to CA-L-Serv, is correct.	

---



# Appendix C: APPL Statements

---

This chapter describes the APPL statements contained in the TPXAPPL member.

This section contains the following topics:

[Primary APPL Statement](#) (see page 185)

[Rebind APPL Statement](#) (see page 185)

[APPL Statements for Shared Virtual Terminals](#) (see page 185)

## Primary APPL Statement

This is the primary APPL statement:

```
TPX APPL AUTH=(ACQ,PASS),MODETAB=TPXLGMOD. . .
```

This statement identifies a primary logical unit (PLU) named TPX. A PLU is the application that your 3270-type terminals communicate with directly. Each product installed at your site must have a different name on its primary APPL statement.

## Rebind APPL Statement

This is the rebind APPL statement:

```
TPXRBIND APPL AUTH=(ACQ,PASS),MODETAB=TPXLGMOD. . .
```

This statement identifies an ACB that the product uses to perform a rebind function that has been specified either by a user exit or by a terminal options table parameter. Using an extra ACB for the rebind process allows the product to rebind to connections that disconnect immediately upon receiving an UNBIND (such as TCP/IP connections).

## APPL Statements for Shared Virtual Terminals

This is the APPL statements for shared virtual terminals:

```
TPXSHARE APPL MODETAB=TPXLGMOD,DLOGMOD=T3278M2. . .
```

This statement identifies a parallel secondary logical unit (SLU) named TPXSHARE. It can be used for applications such as TSO that can communicate with many different users who share one virtual terminal.

**Note:** This statement is not used in PASS mode.

If the product is connecting to an application using its VTAM generic name, the TPXSHARE APPL should not be used. VTAM routes all sessions with a particular generic resource to the same instance of that application. We recommend that you use Group Virtual terminals as defined next.

## APPL Statements for Group Virtual Terminals

These are the APPL statements for group virtual terminals:

```
TPXGR001 APPL MODETAB=TPXLGMD2,DLOGMOD=T3278M2. . .
TPXGR002 APPL MODETAB=TPXLGMD2,DLOGMOD=T3278M2. . .
.
.
.
TPXGR020 APPL MODETAB=TPXLGMD5,DLOGMOD=T3278M5. . .
```

These statements identify the virtual terminals TPXGR001 through TPXGR020, each of which is an identical, *non-parallel* SLU. The product uses these statements for applications such as IMS and CICS, which can have many different users but permit only limited sharing of virtual terminals. With these applications, a virtual terminal can establish only one session with a particular application (for example, CICS). However, that virtual terminal can be shared by a group of users, as long as the users are accessing different applications through that terminal.

**Note:** These statements are not used in PASS mode.

## APPL Statements for Unique Virtual Terminals

These are the APPL statements for unique virtual terminals:

```
TPXUN001 APPL MODETAB=TPXLGMD2,DLOGMOD=T3278M2. . .
TPXUN002 APPL MODETAB=TPXLGMD2,DLOGMOD=T3278M2. . . . .
.
.
.
TPXUN020 APPL MODETAB=TPXLGMD2,DLOGMOD=T3278M5. . .
```

These statements identify the virtual terminals TPXUN001 through TPXUN020. Each of these can support a single session between one user and one application; it cannot be shared among several applications or users.

Any application that is not predefined in the Application Characteristics Table (ACT) must use one of these virtual terminals exclusively.

**Note:** These statements are not used in PASS mode.

**Important!** If you access the IBM Information Network, you must make your virtual terminal LU names unique for your site.

## APPL Statements for Application Passthrough Printing

These are the APPL statements for application passthrough printing:

```
TPXAP001 APPL MODETAB=TPXLGMOD,DLOGMOD=PLU1TPX. . .
TPXAP002 APPL MODETAB=TPXLGMOD,DLOGMOD=PLU3M2. . .
.
.
.
TPXAP006 APPL MODETAB=TPXLGMOD,DLOGMOD=PLU0M2. . .
```

These statements identify the virtual printers TPXAP001 through TPXAP006, used for Application Passthrough Printer Support (APPL PPS). For APPL PPS, you associate a pool of real printers with a virtual printer.

## APPL Statements for User Passthrough Printing

These are the APPL statements for user passthrough printings:

```
TPXUP001 APPL MODETAB=TPXLGMOD,DLOGMOD=PLU1TPX. . .
TPXUP002 APPL MODETAB=TPXLGMOD,DLOGMOD=PLU3M2. . .
.
.
.
TPXUP006 APPL MODETAB=TPXLGMD5,DLOGMOD=PLU0M2. . .
```

These statements identify the virtual printers TPXUP001 through TPXUP006. The product uses these statements for User Passthrough Printer Support (USER PPS). For USER PPS, you associate a virtual printer with the virtual terminal from which the user requested a print function.



# Appendix D: Tape Contents

---

This appendix describes the contents of the product distribution tape.

This section contains the following topics:

[Data Sets on the Product Tape](#) (see page 189)

## Data Sets on the Product Tape

The following table lists the data sets in the order they appear on the tape:

Data Set Number	File Name	Type	Description
1	CAI.SAMPJCL	PDS	Installation JCL for components
2	CAI.RESERVED.S002	N/A	Reserved for future use
3	CAI.HOLDDATA	PDS	SMP/E HOLDDATA (if any)
4 to 8	CAI.RESERVED.Snnn	N/A	Reserved for future use
9	CAI.TPX.V2TCNTL	PDS	Vman to TPX conversion JCL and source
10	CAI.TPX.V2TLOAD	PDS	Vman to TPX LOADLIB
11 to 31	CAI.RESERVED.Snnn	N/A	Reserved for future use
32	CAI.SMPMCS	SEQ	MCS control file for SMP/E
33	CAI.CB0V530.F1	SEQ	TPX distribution library for SMP/E
34	CAI.CB0V530.F2	PDS	Macros
35	CAI.CB0V530.F3	PDS	ACL/E samples
36	CAI.CB0V530.F4	PDS	JOB samples
37	CAI.CB0V530.F5	PDS	Source samples
38	CAI.CB0V530.F6	PDS	Unloaded VSAM files
39	CAI.CB0V530.F7	PDS	MSM deployment XML
40	CAI.CB0V531.F1	PDS	English language panels
41	CAI.CB0V532.F1	PDS	Belgian French
42	CAI.CB0V533.F1	PDS	Brazilian Portuguese
43	CAI.CB0V534.F1	PDS	Danish language panels

<b>Data Set Number</b>	<b>File Name</b>	<b>Type</b>	<b>Description</b>
44	CAI.CB0V535.F1	PDS	Dutch language panels
45	CAI.CB0V536.F1	PDS	Finnish language panels
46	CAI.CB0V537.F1	PDS	French language panels
47	CAI.CB0V538.F1	PDS	German language panels
48	CAI.CB0V539.F1	PDS	Italian language panels
49	CAI.CB0V53A.F1	PDS	Japanese language panels
50	CAI.CB0V53B.F1	PDS	Norwegian language panels
51	CAI.CB0V53C.F1	PDS	Swiss French language panels
52	CAI.CB0V53D.F1	PDS	Swiss German language panels
53	CAI.CB0V53E.F1	PDS	Spanish language panels
54	CAI.CB0V53F.F1	PDS	Swedish language panels
55	CAI.CB0V53G.F1	PDS	Uppercase English language panels

# Appendix E: Data Set Name Changes

---

This Appendix describes the name changes of the data sets starting in release 5.3 of CA TPX.

This section contains the following topics:

[New Data Set Names](#) (see page 191)

## New Data Set Names

New Name	Old Name	RELFILE	Description
CBOVDATV	N/A	CB0V530.F6	Unloaded VSAM files
CBOVJCL	INSTALL	CB0V530.F4	Post installation jobs and samples
CBOVLOAD	LOADLIB	CB0V530.F1	The distributed object modules
CBOVMAC	GENLIB	CB0V530.F2	TPX macros available for user exits
CBOVPDAN	PANELDA	CB0V534.F1	HDA... & TDA... panels
CBOVPDES	PANELSG	CB0V53D.F1	HSG... & TSG... panels
CBOVPDEU	PANELGE	CB0V538.F1	HGE... & TGE... panels
CBOVPENP	PANELUP	CB0V53G.F1	HUP... & TUP... panels
CBOVPENU	PANELEN/PANE LCU	CB0V531.F1	HCU... , HEN... , TCU... & TEN... panels
CBOVPESP	PANELSP	CB0V53E.F1	HSP... & TSP... panels
CBOVPFIN	PANELFI	CB0V536.F1	HFI... & TFI... panels
CBOVPFRA	PANELFR	CB0V537.F1	HFR... & TFR... panels
CBOVPFRB	PANELBF	CB0V532.F1	HBF... & TBF... panels
CBOVPFRS	PANELSF	CB0V53C.F1	HSF... & TSF... panels
CBOVPITA	PANELIT	CB0V539.F1	HIT... & TIT... panels
CBOVPJPN	PANELJP	CB0V53A.F1	HKA... & TKA... panels
CBOVPNLD	PANELDU	CB0V535.F1	HDU... & TDU... panels
CBOVPNOR	PANELNO	CB0V53B.F1	HNO... & TNO... panels
CBOVPPTB	PANELBP	CB0V533.F1	HBP... & TBP... panels
CBOVPSVE	PANELSW	CB0V53F.F1	HSW... & TSW... panels

<b>New Name</b>	<b>Old Name</b>	<b>RELFIL</b>	<b>Description</b>
CBOVSCRI	ACLLIB	CBOV530.F3	Supplied ACL/E scripts
CBOVSRC	SAMPLIB	CBOV530.F5	Sample exits and more
SAMPJCL	N/A	SAMPJCL	Jobs to install the product

# Index

---

## A

- ACB • 185
- ACB See also Reserve ACB's at startup option • 176
- ACL/E • 168
- ADMIN data sets • 175
- ADMIN2 data set • 153
- administration facility • 165
- administrators
  - defining • 165
- allocating DASD and VSAM storage • 153
- APPL statements • 154, 185
- audience for guide • 11
- Authorized Path Facility (APF) • 163

## B

- batch facility • 166
- buffer pools in CA-L-Serv • 181

## C

- CA Common Services • 13
- CA LMP • 13, 14
- CA MII • 175, 181
- CAIRIM • 13
- CA-L-Serv • 159, 177
  - sample members • 182
- CBOVPlng data set • 150
- control record zero • 175
- Coupling Facility • 16, 171
  - structure, defining • 163
- cross-system sharing with CA-L-Serv • 178
- customizing the installation JCL • 152

## D

- data set naming conventions • 16
- data sets
  - ADMIN1 • 175
  - ADMIN2 • 153, 175
  - CBOVPlng • 150
  - DEFSMPE member of SAMPJCL • 152
  - MAIL • 169
  - NOTES • 175
  - on distribution tape • 189
  - SAMPJCL • 151
  - SYS1.VTAMLST • 154

- VIEW • 169

- ddname prefix for use with CA-L-Serv • 179
- DEFSMPE member of SAMPJCL data set • 152
- DISP=OLD parameter • 180
- dispatch level • 173
- documentation
  - online • 152
- dynamic users • 166, 167

## E

- ENQ propagation • 181

## F

- file sharing
  - with CA-L-Serv • 177
  - without CA-L-Serv • 175
- frequently asked questions • 173

## G

- group virtual terminals • 186

## I

- ICSN statement • 179
- information needed for installation • 150

## J

- JCL • 155, 156, 164
  - customizing the installation • 152

## L

- language support • 150
- LMPSee CA LMP • 14
- load library • 156
- logging on a terminal • 159
- logmode tables, copying • 155
- LSERVDSN ENQ • 181
- LSVNVIMG member of CBOVJCL data set • 182
- LSVTPX member of the CBOVJCL data set • 182

## M

- MAIL file • 169
- migration • 171
  - checklist • 171

---

## N

new features • 173  
NOTES data set • 175

## P

panel language • 150  
PASS mode • 185  
pass ticket • 173  
post-installation • 163

## R

RACF • 173  
Reserve ACB's at startup option • 176

## S

SAMPJCL data set • 151  
sample IEBCOPY job • 151  
saved dynamic users • 168  
service pack • 173  
shared virtual terminals • 185  
signing on • 161  
signon and signoff exit • 169  
SMP/E procedure • 152  
starting the product • 159  
startup procedure • 156, 179  
statements, application definition • 154  
static users • 166  
stopping the product • 161  
switch-in exit • 173  
SYS1.VTAMLST data set • 154  
SYSDSN ENQ • 181  
system managed rebuild • 171, 173  
system options • 165  
SYSVSAM ENQ • 181

## T

TCPAccess Telnet Server • 173  
TCPAccess Telnet Server interface • 159  
    enabling • 164  
terminal  
    group virtual • 186  
    logging on • 159  
    shared virtual • 185  
    unique virtual • 186  
TN3270 Server • 173  
TPXAPPL member • 185  
TPXPROC • 156

TPXUSWIN exit • 173

## U

unique virtual terminals • 186  
user  
    administration • 166  
    types • 166  
users, defining • 166

## V

VIEW file • 169  
VM • 176  
VSAM file management  
    share options • 168, 180  
    sharing information (VSI) • 175, 177  
    with CA-L-Serv • 177  
    without CA-L-Serv • 175  
VSAM storage, calculating • 153  
VTAM generic resource • 16, 163, 164, 173