CA XCOM™ Data Transport® for z/OS

Installation Guide

Release 11.6

CA Technologies Product References

This document references the following CA products:

- CA ACF2® Security (CA ACF2)
- CA Common Services for z/OS
- CA Roscoe® (CA Roscoe)
- CA TCPaccess™ Communications Server (CA TCPaccess Communications Server)
- CA Top Secret® Security for z/OS (CA Top Secret)
- CA XCOM™ Data Transport® (CA XCOM Data Transport)
- zIIP Enablement Services (CA Common Services for z/OS)

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

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

Contents

Chapter 1: Overview

This guide describes how to install and implement CA XCOM Data Transport for z/OS.

This section contains the following topics:

Audience

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

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

You may need to work with the following personnel:

- Systems programmer for z/OS and VTAM definitions
- Storage administrator, for DASD allocations

How the Installation Process Works

The following steps describe the installation process:

1. Prepare for the installation by confirming that your site meets all installation requirements.
2. Acquire the product using one of the following methods:
   - CA MSM

     Note: If you do not have CA MSM, you can download it from the Download Center at the CA Support Online website. Follow the installation instructions in the CA Mainframe Software Manager documentation bookshelf on the CA Mainframe Software Manager product page.
   - Pax-Enhanced Electronic Software Delivery (ESD)
   - Tape
3. Install the product-based on your acquisition method.
4. Install the CA Common Services using the pax files that contain the CA Common Services you need at your site. All sites should install all CA Common Services contained in the Required CA Common Service bundle.
5. Apply maintenance, if applicable.
6. Configure your product.

Chapter 2: Preparing for Installation

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

This section contains the following topics:

Hardware Requirements

CA XCOM Data Transport for z/OS runs on any IBM or compatible processor running under a supported release of z/OS described in the following section.

Software Requirements

The following software is required for CA XCOM Data Transport for z/OS:

- IBM supported release of z/OS 1.11 or above.

  Note: IBM APAR OA35432: METAL-C RTL HEAP STORAGE NOT REUSED AFTER FREE. Is required. Without this APAR, running compression routines will cause memory leaks, eventually leading to an out of memory condition on the CA XCOM Data Transport server

- SMP/E
- For transfers using SNA, scheduling transfers over SNA, or using the CICS interface, CA XCOM Data Transport for z/OS requires the following:
  - Any currently supported version of ACF/VTAM

Note: The panels for the CICS interface for XCOM have been deprecated. The ISPF interface for XCOM is used instead.

- For transfers using TCP/IP, or scheduling transfers over TCPIP, CA XCOM Data Transport for z/OS requires one of the following:
  - Any version of TCP/IP supported by IBM
  - Any version of CA TCPaccess Communications Server

  Note: TCP/IP components use OpenEdition. The use of these components requires that the XCOM STC have an OpenEdition (OMVS) user ID and group defined. For more information, see the IBM *z/OS Communications Server: IP Configuration Guide*.

- If the CA XCOM CICS Interface is installed, any supported version of CICS with Intersystem Communication (ISC) support enabled

Note: The panels for the CICS interface for XCOM have been deprecated. The ISPF interface for XCOM is used instead.

- Any supported version of TSO/ISPF
- IBM Parallel Sysplex Coupling Facility (required only for deprecated XCOMPLEX environment)
- IBM Parallel Sysplex Signaling Services
- IBM APAR OA35432: METAL-C RTL HEAP STORAGE NOT REUSED AFTER FREE. Without this APAR, running compression routines will cause memory leaks, eventually leading to an out of memory condition on the CA XCOM Data Transport server.
- A valid LMP license key
- For History residing in a Database
  - DB2 for z/OS v9 or v10 running New Function Mode

CA Common Services Requirements

The following CA Common Services are used with CA XCOM Data Transport for z/OS:

- CA CAIRIM
- CA LMP
- CA Health Checker Common Service
- CA zIIP Enablement Services
- CA Easytrieve Services

If other CA products are installed at your site, some of these services could already be installed

Before you install CA XCOM Data Transport for z/OS, we recommend that you install CA Common Services for z/OS Version 14.0/14.1. Quality Assurance is certified with this release. Minimally, you must have CA Common Services r12 plus APARs RO20081 and RO27110 or r14 plus APAR RO36618 before applying this product package.

Note: If the full version of CA Easytrieve r11.0 SP3 is used instead of the CA Common Services version, solution RO30595 must be applied.

Security Requirements

To complete the tasks in this guide, you may need the following security privileges, depending upon the features used:

- A valid OMVS user ID is required to set up and use the OpenSSL encryption facilities provided by CA XCOM Data Transport
- Authority to allocate and update PDS and VSAM data sets on DASD volumes

Important! Make sure that you have READ access to resources BPX.FILEATTR.APF and BPX.FILEATTR.PROGCTL. This access is required to set the proper attributes for the secure socket components.

Storage Requirements

There is a Server Storage Usage Worksheet for Release 11.6 available on the CA XCOM Data Transport web pages for the z/OS platform at http://ca.com/support. Filling out this worksheet allows you to calculate the approximate storage usage required for CA XCOM Data Transport Release 11.6.

Concurrent Releases

You can install this release of CA XCOM Data Transport for z/OS and continue to use an older release for your production 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.
- 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 157).

This section contains the following topics:

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

CA MSM Documentation

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

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

Getting Started Using CA MSM

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

How to Use CA MSM: Scenarios

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

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

How to Acquire a Product

The *Product Acquisition Service (PAS)* facilitates the acquisition of mainframe products and the service for those products, such as program temporary fixes (PTFs). The PAS retrieves information about 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 25), 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 26). 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 27).

   After you find your product in the catalog, you can download the product installation packages (see page 27).

   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 75) for those systems.
   c. Set up the target systems (Non-Sysplex (see page 53), Sysplex or Monoplex (see page 54), Shared DASD Cluster (see page 55), and Staging (see page 56)), and validate them.
   d. Add FTP (see page 65) information, including data destination information, to each system registry entry.
2. Set up methodologies (see page 104).

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 120), products (see page 95), custom data sets (see page 96), and methodologies (see page 104), 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 107) 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 107) and type of copy. Type of copy can be either a container copy or a file-by-file copy.

You can add a custom data set (see page 97).

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 105), 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 39) 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 40).

3. Apply the maintenance (see page 43).

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

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

Access CA MSM Using the Web-Based Interface

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

Follow these steps:

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

   The login page appears.

   Note: If the Notice and Consent Banner appears, read and confirm the provided information.

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

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

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

3. Click New.

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

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

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

   You are prompted to review your user settings.

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

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

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

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

Acquiring Products

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

Update Software Catalog

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

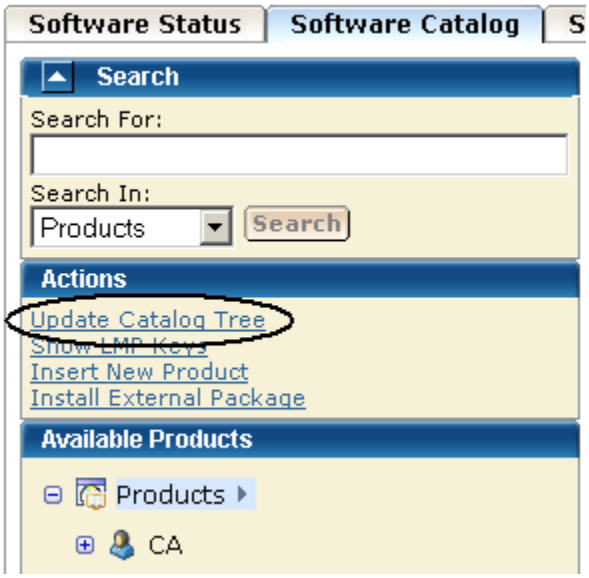
If you update the catalog tree and some changes are missing, check your user settings on the CA Support Online website.

Follow these steps:

1. Click the Software Catalog tab.

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

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



   You are prompted to confirm the update.

3. Click OK.

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

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

Download Product Installation Package

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

Follow these steps:

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

   CA MSM uses the credentials to access the CA Support Online website.

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

   The product releases are listed.

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

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

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

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

   The product packages are downloaded.

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

Migrate Installation Packages Downloaded External to CA MSM

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

Migrating these packages to CA MSM provides a complete view of all your product releases. After a package is migrated, you can use CA MSM to install the product (see page 31).

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.

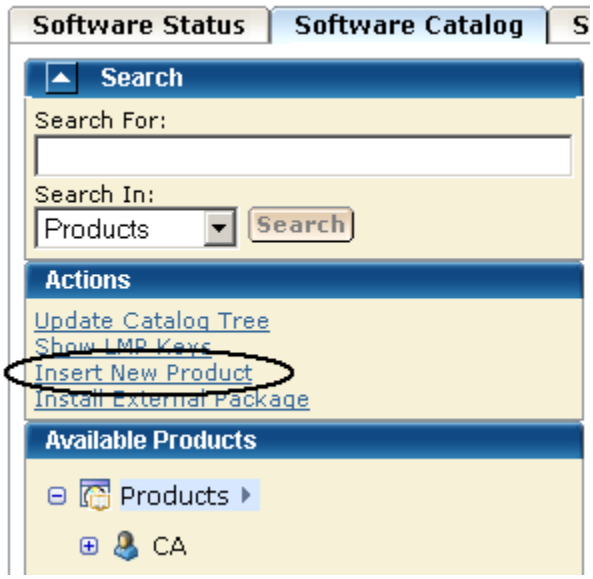
   Note: To see the added package, refresh the page.

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 30).

   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 29) (or set of maintenance files (see page 41)) 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.

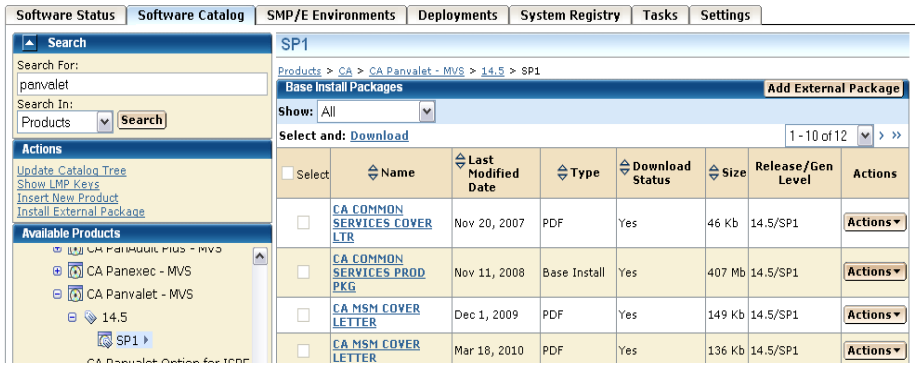
During installation, you select the CSI where the product is to be installed, and specify its zones. You can either specify target and distribution zones to be in the existing CSI data sets, or create new data sets for each zone.

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 34).

   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 31). 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.

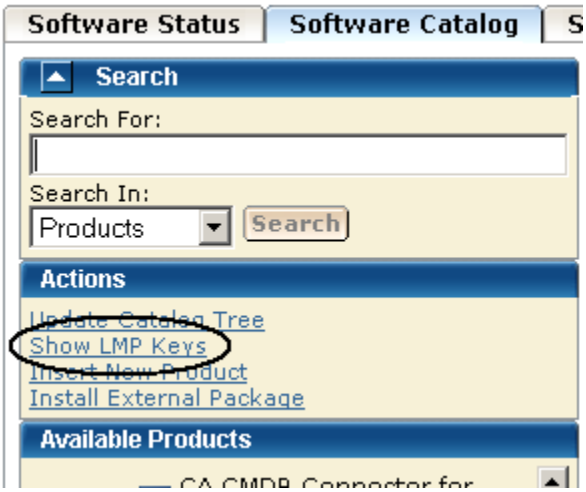
   You are prompted to specify any additional parameters. A new CSI is specified.

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 39)
   - Download Product Maintenance Packages for Old Product Releases and Service Packs (see page 40)
   - Manage Maintenance Downloaded External to CA MSM (see page 41)

   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:

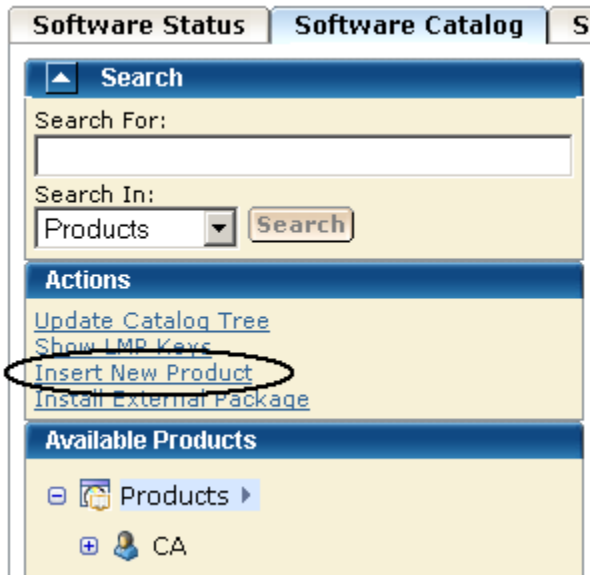
Download Maintenance Packages for Old Product Releases and Service Packs (see page 40)

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 43).

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 30).

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 43)

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.

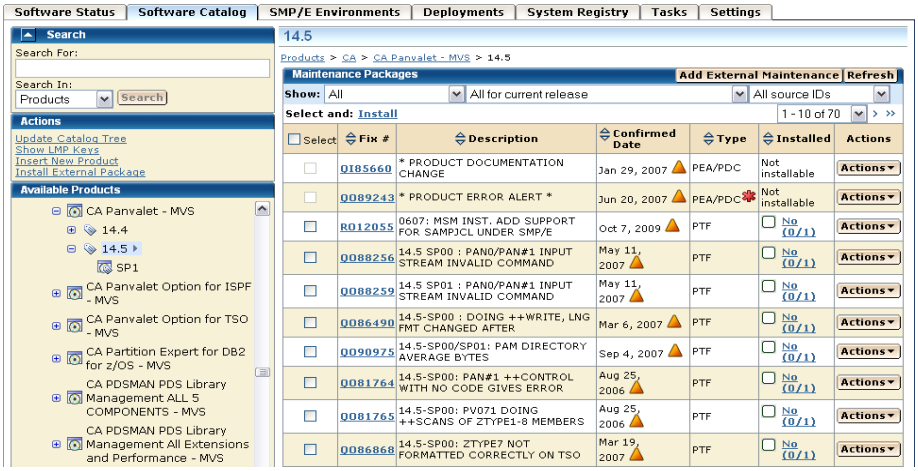
   Maintenance information appears at the right for the releases you have.

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

   The maintenance information is updated.

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

   The maintenance packages are listed, for example:



   Red asterisks identify HIPER maintenance packages.

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

   The Maintenance Package Details dialog appears, identifying any prerequisites.

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

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

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

   The Introduction tab of the wizard appears.

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

   The packages to install are listed.

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

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

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

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

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

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

    - If prerequisites exist and are available, review them and click Next. CA MSM installs these prerequisites as part of the process. If a prerequisite is *not* available, the wizard cannot continue. You must acquire the prerequisite and restart the process.
    - If HOLDDATA (see page 147) entries exist, review and select them, and click Next.

    SMP/E work DDDEFs of SMPWRK*x* and SYSUT*x*, with their allocation parameters, are listed.

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

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

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

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

       A pop-up window opens.

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

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

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

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

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

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

14. Click Next.

    A summary of the task appears.

15. Review the summary, and click Install.

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

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

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

More information:

Download Product Maintenance Packages (see page 39)
Download Maintenance Packages for Old Product Releases and Service Packs (see page 40)

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 41).

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 Introduction tab of the wizard 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.

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.

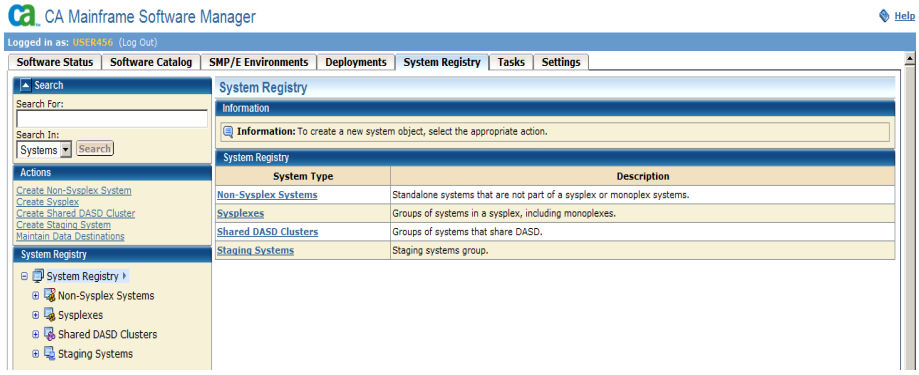
View a System Registry

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.

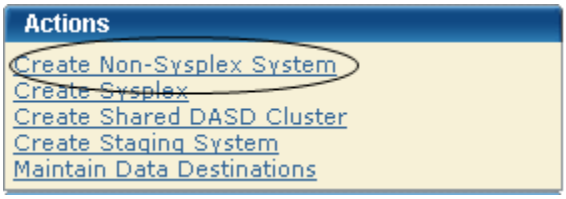


Create a Non-sysplex System

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:

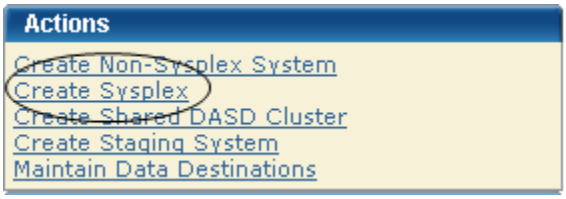
```
Property Name: z/OS LPAR Name, Value: ** Not Applicable **.
```

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.

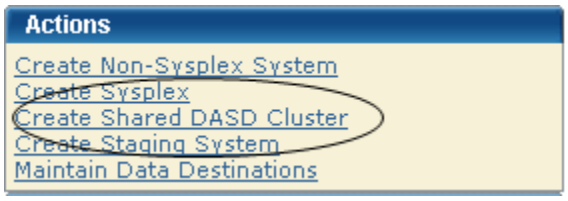
5. Detail the nonstaging system.

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.

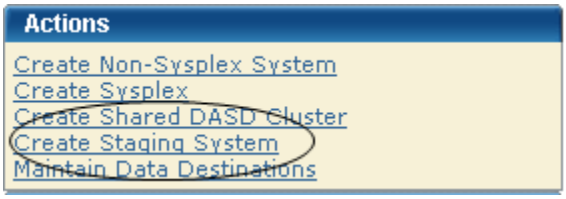
3. Right-click the newly added DASD cluster name and select Add System or Sysplex to this Shared DASD Cluster. Select the systems or sysplexes that you want to add to the DASD cluster.

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 53), Sysplex (see page 54), Shared DASD Cluster (see page 55), or Staging System (see page 56).

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 63), 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 64).

     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 61).

   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 61).

Not Validated

Indicates that this system has not been validated yet.

Not Accessible

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

Validation Conflict

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

Error Details

When there is a validation conflict, the Error details button appears. Click this button to find the reason for this conflict. You can investigate the failed validation (see page 61).

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 61).

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 61)
- Investigate a Failed Validation Immediately After a Validation (see page 62)
- Download a Message Log (see page 62)
- Save a Message Log as a Data Set (see page 63)
- View Complete Message Log (see page 63)

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.

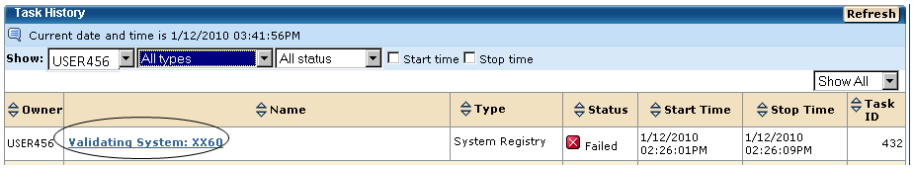
Investigate a Failed Validation Using Task Output Browser

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

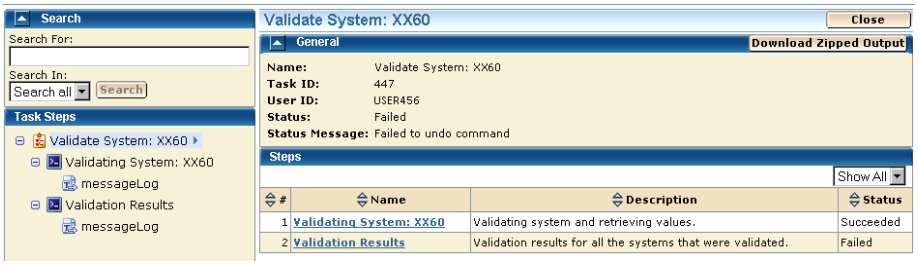
Follow these steps:

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 Validate System Task Output Browser appears.



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

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

   Note: You can analyze the error results and 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 65) Locations lists the current FTP locations for this system. You can add (see page 65), edit (see page 67), set default (see page 68), or remove (see page 68) FTP (see page 65) 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 65) 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 67)
Set FTP Location Default (see page 68)
Delete FTP Locations (see page 68)

Edit FTP Locations

You can edit FTP (see page 65) 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 65) 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 65) 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 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 64).

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.

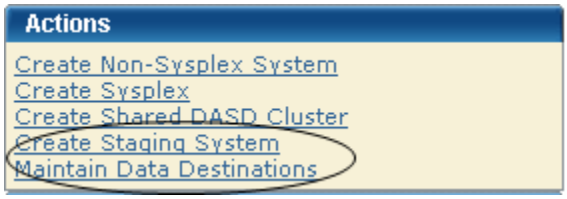
   The data destinations are added to the system.

Maintain Data Destinations

You can maintain, delete (see page 74), or create (see page 70) 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 64).

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 75), edit (see page 76), or delete (see page 77) 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

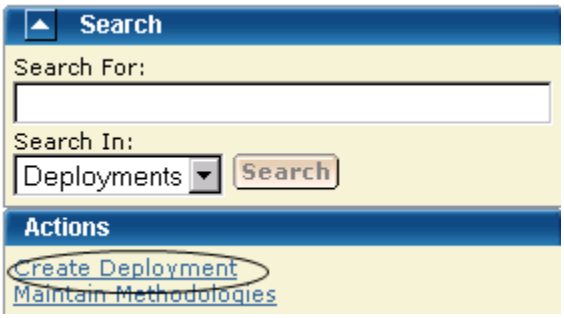
The deployment creation process consists of the following steps:

1. Initiate deployment creation (see page 80).
2. Define a name and description (see page 80).
3. Select an SMP/E environment (see page 81).
4. Select a product (see page 81).
5. Select a custom data set (see page 82).
6. Select a methodology (see page 82).
7. Select a system (see page 84).
8. Preview and save (see page 84).

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 85) 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 85) 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 85) 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 85) until a successful snapshot has been created.

Select a Custom Data Set

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

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 97).

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 85) until a successful snapshot has been created.

More information:

Add a Custom Data Set (see page 97)

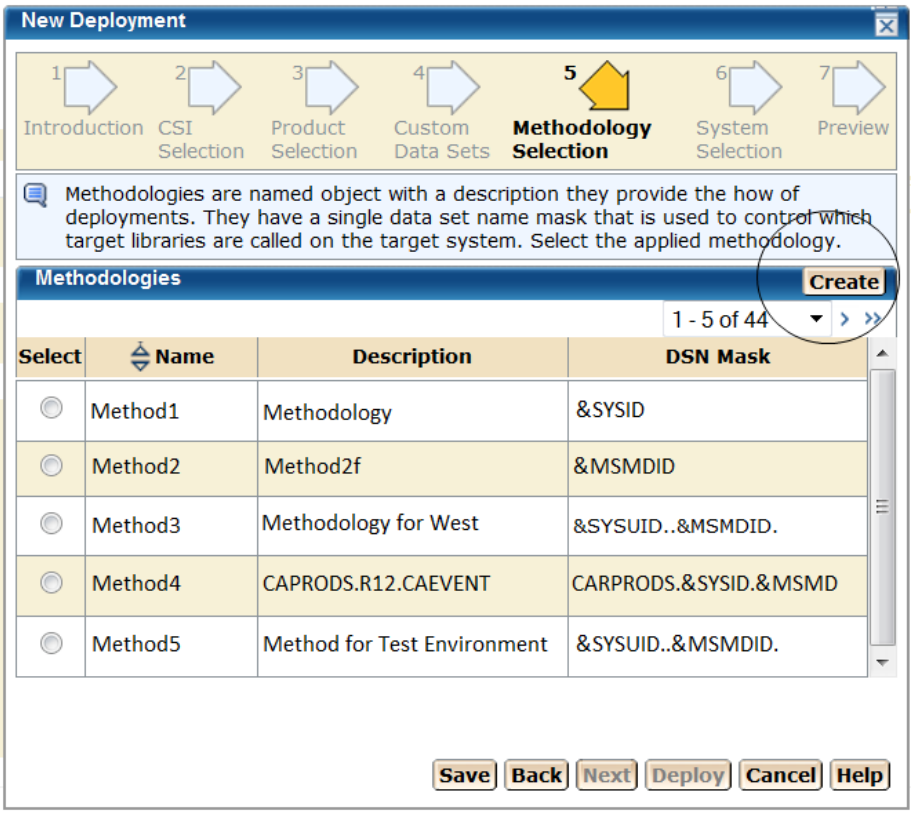
Select a Methodology

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 105).



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 85) until a successful snapshot has been created.

More information:

Create a Methodology (see page 105)

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 85) 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 78).
4. To change a methodology, select a methodology from the drop-down list and click Edit.

   The Edit Methodology window (see page 117) appears. The Deployment ID is the value of the MSMID variable.

   Note: You can perform the following actions:

   - You can select (see page 95), add (see page 95), or remove (see page 96) a product, and .
   - You can select (see page 121), add (see page 121), or remove (see page 122) a system.
   - You can select (see page 97), add (see page 97), or remove (see page 103) 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 93)

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 91)

You can reset a deployment status when the deployment has a status of *snapshot in progress*, *transmitting*, or *deploying*. See reset status (see page 91) for a list of deleted files.

7. Click Save on the Deployment Details window.

   You changes are saved.

More information:

Edit a Methodology (see page 117)
View the Product List (see page 95)
Add a Product (see page 95)
Remove a Product (see page 96)
View a System List (see page 121)
Add a System (see page 121)
Remove a System (see page 122)
Confirm a Deployment (see page 93)

Deployment Maintenance

You can maintain a deployment in the following ways:

- Adding
  - System (see page 121)
  - Product (see page 95)
  - Custom data sets (see page 97)
- Delete
  - Deployment
- Removing
  - System (see page 122)
  - Product (see page 96)
  - Custom data sets (see page 103)

- Editing
  - Maintain deployments (see page 85)
  - Edit a custom data set (see page 100)
  - Edit a methodology (see page 117)
- Viewing
  - System (see page 121)
  - Product (see page 95)
  - Custom data sets (see page 97)

More information:

Add a Custom Data Set (see page 97)
Add a Product (see page 95)
Add a System (see page 121)
Edit a Custom Data Set (see page 100)
Change Deployments (see page 85)
Failed Deployments (see page 88)
Remove a Product (see page 96)
Remove a System (see page 122)
View the Product List (see page 95)
View a System List (see page 121)
View Custom Data Sets (see page 97)

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 89)
- Download a Message Log (see page 62)
- Save a Message Log as a Data Set (see page 63)
- View Complete Message Log (see page 63)

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 62)
Save a Message Log as a Data Set (see page 63)
View Complete Message Log (see page 63)

Investigate a Failed Deployment

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

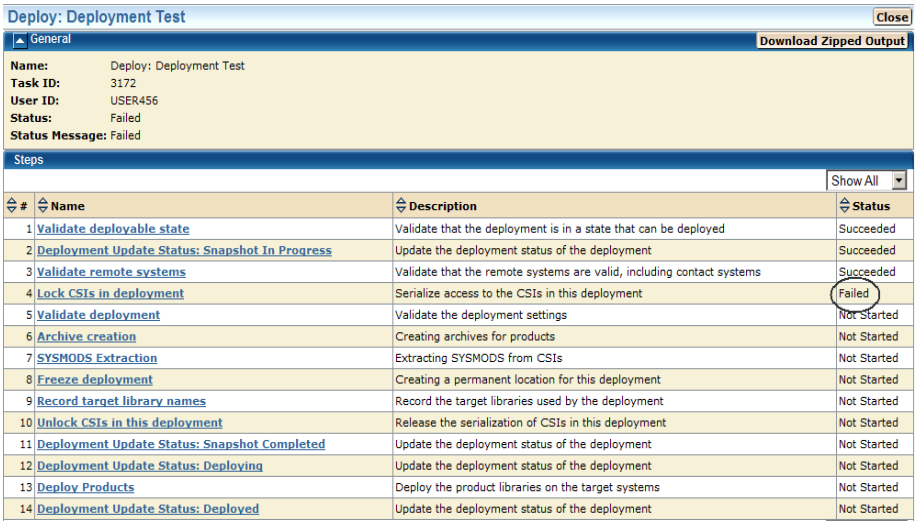
Follow these steps:

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

   Note: You can refine the task list further by selecting task and status types from the drop-down lists, and then sort by Task ID.
4. Find the failed deployment step and click the link in the Name column.

   The Task Output Browser appears.



Deploy: Deployment Test — Close

General — Download Zipped Output

Name: Deploy: Deployment Test
Task ID: 3172
User ID: USER456
Status: Failed
Status Message: Failed

Steps — Show All

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

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

   Note: You can analyze the error results and determine the steps required to troubleshoot them.
6. Correct the issue and deploy again.

More information:

Download a Message Log (see page 62)
Save a Message Log as a Data Set (see page 63)
View Complete Message Log (see page 63)

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 61) 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 many 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 61) 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/D*nnnn* where *nnnn* = Deployment ID automatic number. Application Root is defined in settings under mount point management.

All applicable database records.

Transmit in Error

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

Transmitted

Same as Transmit in Error.

Deploy in Error

Same as Transmitted.

Deployed

Same as Snapshot Completed.

Complete

Same as Snapshot Completed.

Follow these steps:

1. Click the Deployments tab.

   The Deployment window appears.

2. On the right, in the Deployments panel, click the Current Deployments or Complete Deployments link.

   The detailed deployment information appears.

3. Click the deployment name link, and from the Actions drop-down list, select Delete, and then click OK to confirm.

   The deployment is deleted.

Confirm a Deployment

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

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

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

Follow these steps:

1. Click the Deployments tab.

   The Deployment page appears.

2. Click Confirm.

   The Confirmation dialog appears.

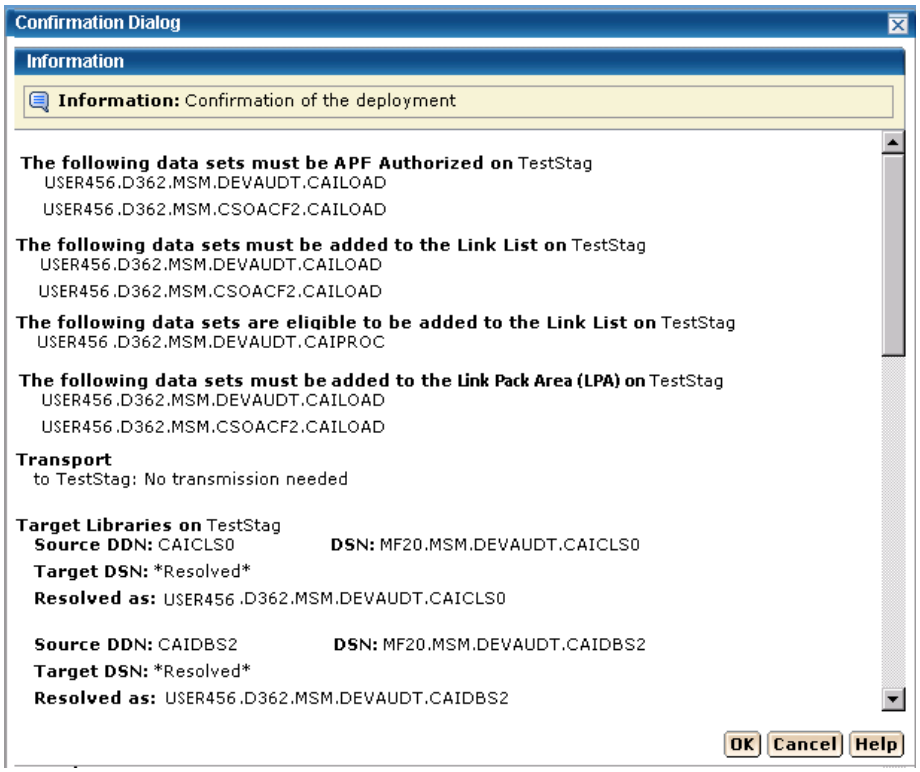
3. Review the confirmation.
4. Click OK when the deployment is correct.

   Note: Click Cancel to exit this procedure without confirming.

   The Deployment Summary window may contain the following:

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

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



Products

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

View the Product List

You can view a product.

Follow these steps:

1. Click the Deployments tab.
2. Select the current deployment from the tree on the left side.

   The detailed deployment information appears on the right side.

Add a Product

You can add a product to a deployment.

Follow these steps:

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

   A list of current deployments appears.
3. Click the deployment name link.
4. In the Product List panel click Add Products.

   The Add Products wizard appears.
5. Select a CSI and click Next.

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

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

   The Custom Data Set Selection appears
10. If needed, select or add a custom data set (see page 97).
11. Click Add Products.

    The Product is added.

Remove a Product

You can remove a product from a deployment.

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

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 97), edit (see page 100), and remove (see page 103) custom data sets from a deployment.

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

- For a z/OS data set, you need to provide a data set name that is the actual existing z/OS data set and a mask that names the data set on the target system. This mask may be set up using symbolic qualifiers (see page 107) 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 107)), 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 107).

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

   Limits: Maximum 64 characters.

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

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

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

   ■

   Two consecutive periods are required to separate the two masks.

9. Enter the Mask and click OK.

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

    Limit: Maximum 255 characters.

    Note: The asterisk indicates that the field is mandatory.

11. Enter the Remote Path and/or click the file icon and select a symbolic name (see page 107). 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 107).

    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 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 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 107).

    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 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 107).

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

    Limit: Maximum 255 characters.

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

    Default: File-by-file Copy
13. Click OK.
14. For Container Copy, enter the container name and/or click the file icon and select a symbolic name (see page 107).

    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 is 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 107).

    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 105), maintain, edit (see page 117), and delete (see page 119) 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 107).

  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 C*reate 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 107).

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

Directory Path

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

Symbolic Substitution

Symbolic substitution, or translation, is a process performed by CA MSM to resolve the mask values specified in the data set name mask and directory path, into real names based upon the contents of the symbolic variables at translation time. A CA MSM symbol is defined in the list of symbols. Each symbol begins with an ampersand (&) and ends with a period (.). For example, the symbol &LYYMMDD. would be completely replaced with its value at translation time, including the ampersand and trailing period. The trailing period is important and is considered part of the symbolic name.

Symbolic Variables

You can use symbolic variables in the construction of a data set name with the value of the symbolic variable to end a data set name segment.

Example: Assume MSMDID is 255.

SYSWORK.D&MSMDID..DATASET

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

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

Numeric Values

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

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

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

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

An incorrect specification of the mask would be:

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

Directory Paths

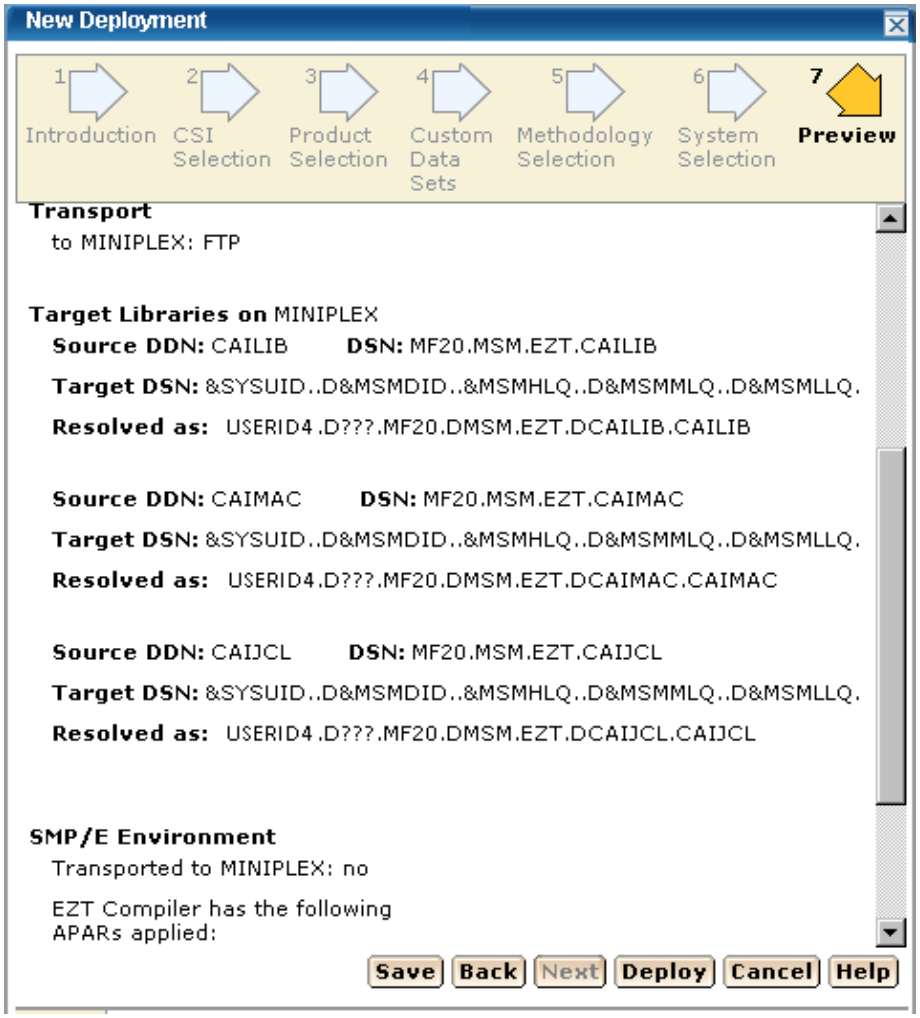
Symbolic substitution works in the same logical way for directory paths. However, directory paths do not typically have periods in them, so you will typically not see the double dots in directory paths.

Example: Assume the target system is SYSZ.

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

Preview Example

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



Symbolic Qualifiers

ID and System Information

MSMDID

This is the CA MSM deployment ID.

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

MSMMPN

This is the CA MSM Mount Point Name. The value is entered into the mount point name field when adding a custom data set (see page 97) with both the USS radio button and the Container copy radio button set. It is of primary value in remote path.

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

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

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

Remote path: &MSMMPN.

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

MSMSYSNM

This is the 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.CAIEXEC
```

Assume the methodology specified a mask of:

```
&SYSUID..D&MSMDID..LIB&MSMDLIBN
```

Assume USERID is USER789, and the deployment ID is 877, then the resolved DSNs would be,

```
Deployed library = USER789.D877.LIB1.CAIPROC
Deployed library = USER789.D877.LIB2.CAILOAD
Deployed library = USER789.D877.LIB3.CAIEXEC
```

Local Date and Time

LYYMMDD

This is the local two-digit year.

YY two-digit year

MM two-digit month (01=January)

DD two-digit day of month (01 through 31)

Example: 100311

LYR2

This is the local two-digit year.

LYR2 two-digit year

Example: 10

LYR4

This is the local four-digit year.

LYR4 four-digit year

Example: 2010

LMON

This is the local month.

LMON two-digit month (01=January)

Example: 03

LDAY

This is the local day of the month.

LDAY two-digit day of month (01 through 31)

Example: 11

LJDAY

This is the local Julian day.

LJDAY three-digit day (001 through 366)

Example: The Julian day for January 11th is 011.

LWDAY

This is the local day of the week.

LWDAY is three characters in length. The days are MON, TUE, WED, THR, FRI, SAT, and SUN.

Example: MON

LHHMMSS

This is the local time in hours, minutes, and seconds.

HH two digits of hour (00 through 23) (am/pm NOT allowed)

MM two digits of minute (00 through 59)

SS two digits of second (00 through 59)

Example: 165148

LHR

This is the local time in hours.

LHR two-digits of hour (00 through 23) (am/pm NOT allowed)

Example: 16

LMIN

This is the local time in minutes.

LMIN two-digits of minute (00 through 59)

Example: 51

LSEC

This is the local time in seconds.

LSEC two-digits of second (00 through 59)

Example: 48

UTC Date and Time

Coordinated Universal Time is abbreviated UTC.

YYMMDD

This is the UTC date.

YY two-digit year

MM two-digit month (01=January)

DD two-digit day of month (01 through 31)

Example: 100311

YR2

This is the UTC two digit year.

YR2 two-digit year

Example: 10

YR4

This is the UTC four digit year.

YR4 four-digit year

Example: 2010

MON

This is the UTC month.

MON two-digit month (01=January)

Example: 03

DAY

This is the UTC day of the month.

DAY two-digit day of month (01 through 31)

Example: 11

JDAY

This is the UTC Julian day.

JDAY three-digit day (001 through 366)

Example: The Julian day for January 11th is 011.

WDAY

This is the UTC day of the week.

WDAY is three characters in length. The days are MON, TUE, WED, THR, FRI, SAT, and SUN.

Example: MON

HHMMSS

This is the UTC time in hours, minutes, and seconds.

HH two-digits of hour (00 through 23) (am/pm NOT allowed)

MM two-digits of minute (00 through 59)

SS two-digits of second (00 through 59)

Example: 044811

HR

This is the UTC time in hours.

HR two digits of hour (00 through 23) (am/pm NOT allowed)

Example: 04

MIN

This is the UTC time in minutes.

MIN two-digits of minute (00 through 59)

Example: 48

SEC

This is the UTC time in seconds.

SEC two-digits of second (00 through 59)

Example: 11

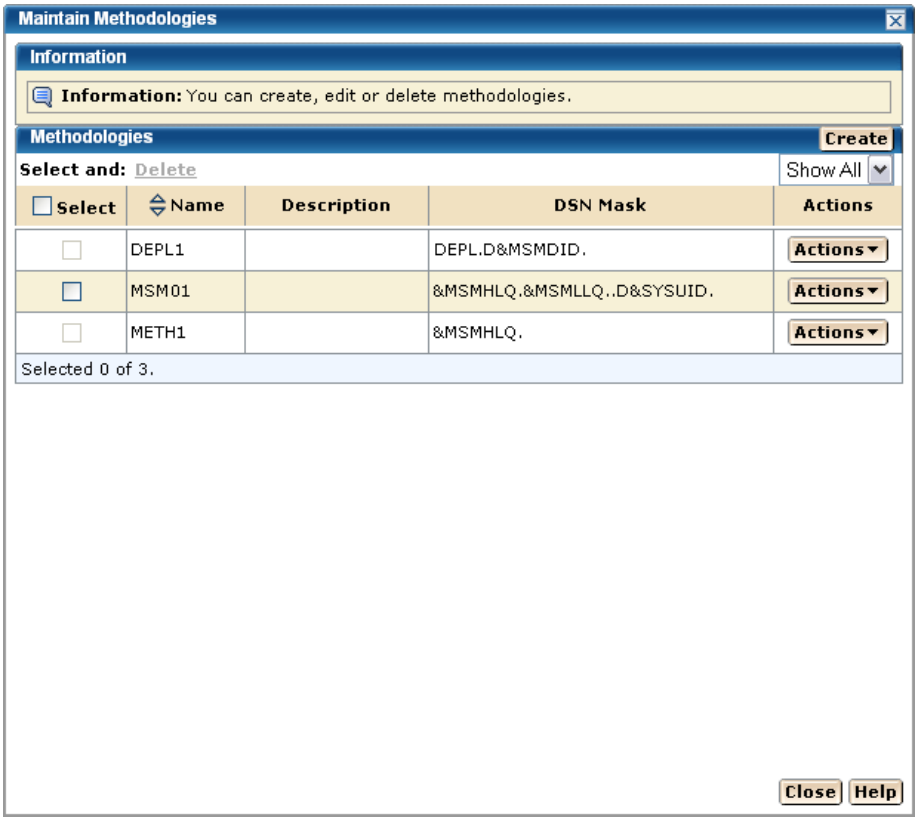
Maintain Methodologies

You can edit, replace, or remove (see page 119) 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 117).

More information:

Delete Methodologies (see page 119)
Edit a Methodology (see page 117)

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 107).

   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 107).

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

Sequential data set or a file in the UNIX file system

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

For a VSAM data set (cluster)

Create or Replace indicates that an existing VSAM cluster should be populated with the data from the source file.

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

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

7. Click Save.

   Your changes are saved.

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

More information:

Symbolic Qualifiers (see page 107)

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 product as they moves 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.

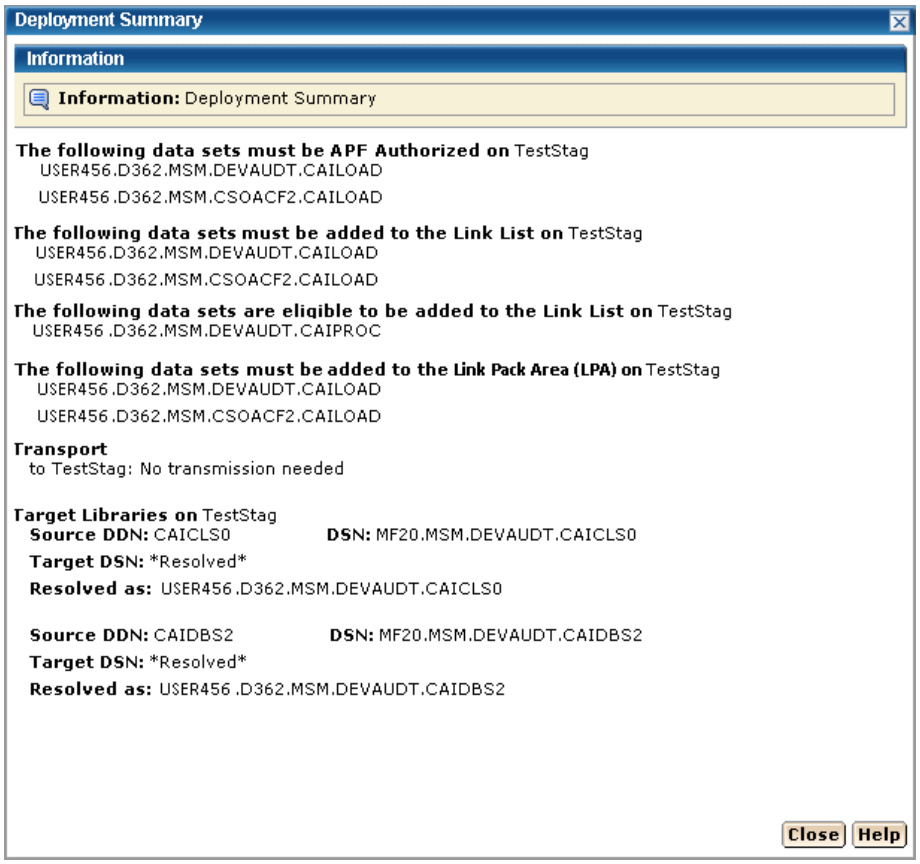
Important! Data sets may need to be APF-authorized and added to the Link List and Link Pack Area. These data sets are identified in this dialog.

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 157).

Chapter 4: Installing Your Product from Pax-Enhanced ESD

This section contains the following topics:

How to Install a Product Using Pax-Enhanced ESD

This section describes the Pax-Enhanced ESD process. We recommend that you read this overview and follow the entire procedure the first time you complete a Pax-Enhanced ESD installation. For experienced UNIX users, the Pax-Enhanced ESD Quick Reference Guide has sufficient information for subsequent installations.

Important! Downloading pax files for the SMP/E installation as part of the Pax-Enhanced ESD process requires write authority to the UNIX System Services (USS) directories used for the ESD process.

If you prefer not to involve all CA Technologies product installers with z/OS UNIX System Services, assign a group familiar with USS to perform Steps 1 through 4 and provide the list of the unpacked MVS data sets to the product installer. USS is not required for the actual SMP/E RECEIVE of the product or for any of the remaining installation steps.

To install files using Pax-Enhanced ESD, use the following process:

1. Allocate and mount the file system. This process requires a USS directory to receive the pax file and to perform the unpack steps. We recommend that you allocate and mount a file system dedicated to Pax-Enhanced ESD and create the directory in this file system. Ensure that all users who will be working with pax files have write authority to the directory.
2. Copy the product pax files into your USS directory. To download files, choose one of the following options:
   - Download a zip file from CA Support Online to your PC, unzip the file, and then upload the product pax files to your USS file system.
   - FTP the pax files from CA Support Online directly to your USS directory.
   - Upload the pax files from the Installation CD/DVD to your USS directory.

   Note: Perform Steps 3 through 6 for each pax file that you upload to your USS directory.
3. Create a product directory from the pax file. Set the current working directory to the directory containing the pax file, and create a new directory in your USS directory by entering the following command:

   ```
   pax -rvf pax-filename
   ```
4. Use the SMP/E GIMUNZIP utility to create z/OS installation data sets. The file UNZIPJCL in the directory created by the pax command in Step 3 contains a sample job to GIMUNZIP the installation package. Edit and submit the UNZIPJCL job.
5. Receive the SMP/E package. For this step, use the data sets created by GIMUNZIP in Step 4. Perform a standard SMP/E RECEIVE using the SMPPTFIN and SMPHOLD (if applicable) DASD data sets. Also, specify the high-level qualifier for the RELFILEs on the RFPREFIX parameter of the RECEIVE command.
6. Proceed with product installation. Consult product-specific documentation, including AREADME files and installation notes to complete the product installation.

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

More Information:

USS Environment Setup (see page 130)
Allocate and Mount a File System (see page 131)
Copy the Product Pax Files into Your USS Directory (see page 134)
Create a Product Directory from the Pax File (see page 139)
Copy Installation Files to z/OS Data Sets (see page 140)

How the Pax-Enhanced ESD Download Works

Important! To download pax files for the SMP/E installation as part of the Pax-Enhanced ESD process, you must have write authority to the UNIX System Services (USS) directories used for the ESD process and available USS file space before you start the procedures in this guide.

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 128) topic explains how the download interface works.

   Note: For traditional installation downloads, see the *Traditional ESD User Guide*. Go to https://support.ca.com/, log in, and click Download Center. A link to the guide appears under the Download Help heading.

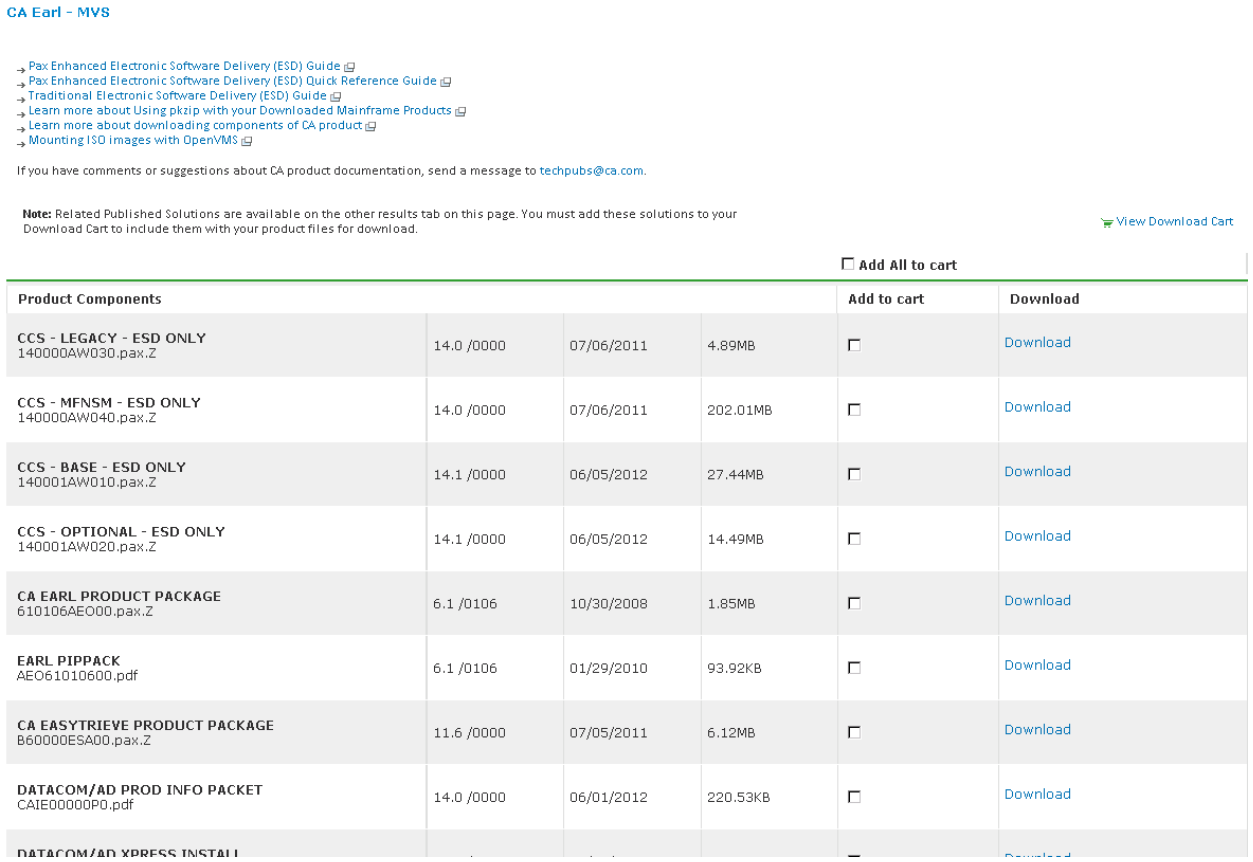
4. Perform the steps to install the product based on the product-specific steps.

   The product is installed on the mainframe.

ESD Product Download Window

CA Technologies product ESD packages can be downloaded multiple ways. Your choices depend on the size of the individual files and the number of files you want to download. You can download the complete product with all components or you can select individual pax and documentation files for your product or component.

The following illustration shows sample product files. It lists all components of the product. You can use the Download Cart by checking one or more components that you need or check the box for Add All to cart. If you prefer to immediately download a component, click the Download link.



CA Earl - MVS

- Pax Enhanced Electronic Software Delivery (ESD) Guide
- Pax Enhanced Electronic Software Delivery (ESD) Quick Reference Guide
- Traditional Electronic Software Delivery (ESD) Guide
- Learn more about Using pkzip with your Downloaded Mainframe Products
- Learn more about downloading components of CA product
- Mounting ISO images with OpenVMS

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

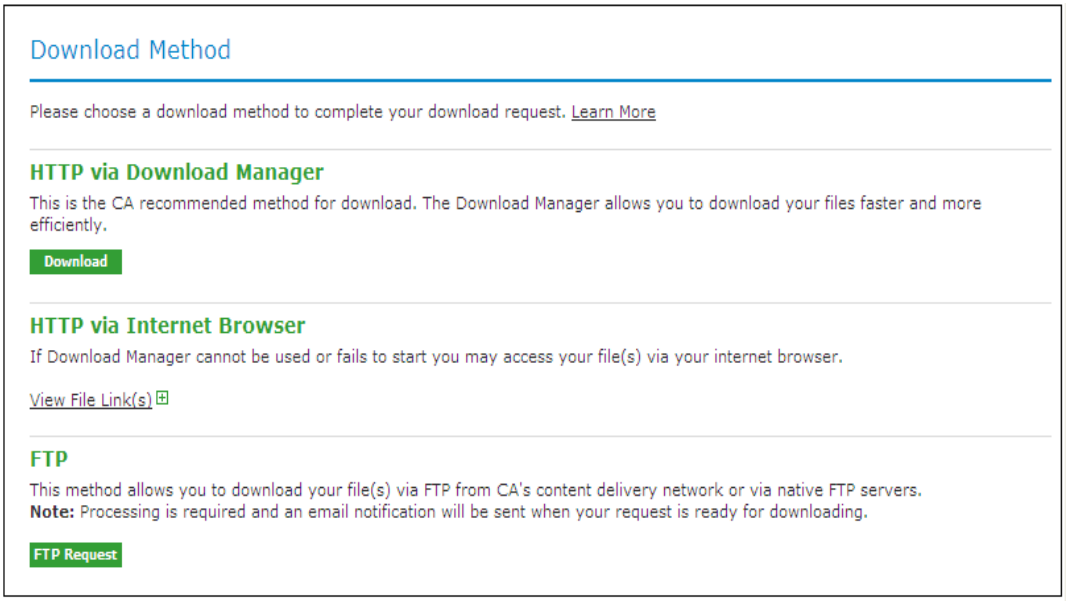
Note: Related Published Solutions are available on the other results tab on this page. You must add these solutions to your Download Cart to include them with your product files for download.

View Download Cart

Add All to cart

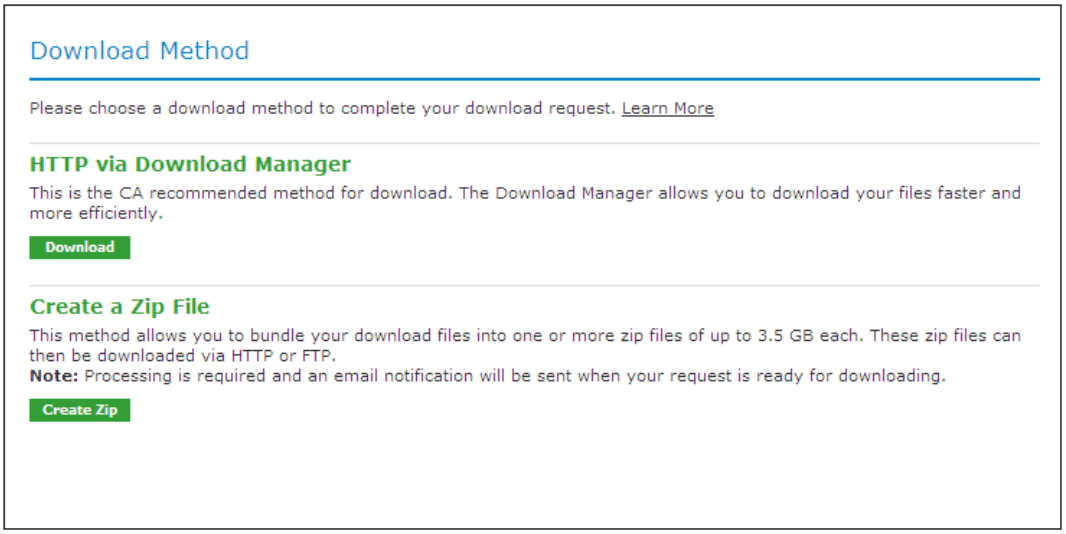
Product Components				Add to cart	Download
CCS - LEGACY - ESD ONLY 140000AW030.pax.Z	14.0 /0000	07/06/2011	4.89MB	☐	Download
CCS - MFNSM - ESD ONLY 140000AW040.pax.Z	14.0 /0000	07/06/2011	202.01MB	☐	Download
CCS - BASE - ESD ONLY 140001AW010.pax.Z	14.1 /0000	06/05/2012	27.44MB	☐	Download
CCS - OPTIONAL - ESD ONLY 140001AW020.pax.Z	14.1 /0000	06/05/2012	14.49MB	☐	Download
CA EARL PRODUCT PACKAGE 610106AEO00.pax.Z	6.1 /0106	10/30/2008	1.85MB	☐	Download
EARL PIPPACK AEO61010600.pdf	6.1 /0106	01/29/2010	93.92KB	☐	Download
CA EASYTRIEVE PRODUCT PACKAGE B60000ESA00.pax.Z	11.6 /0000	07/05/2011	6.12MB	☐	Download
DATACOM/AD PROD INFO PACKET CAIE00000P0.pdf	14.0 /0000	06/01/2012	220.53KB	☐	Download
DATACOM/AD XPRESS INSTALL					

Clicking the link for an individual component takes you to the Download Method page.



Depending on the size and quantity of product files ordered, the Download Method screen could also have these options:

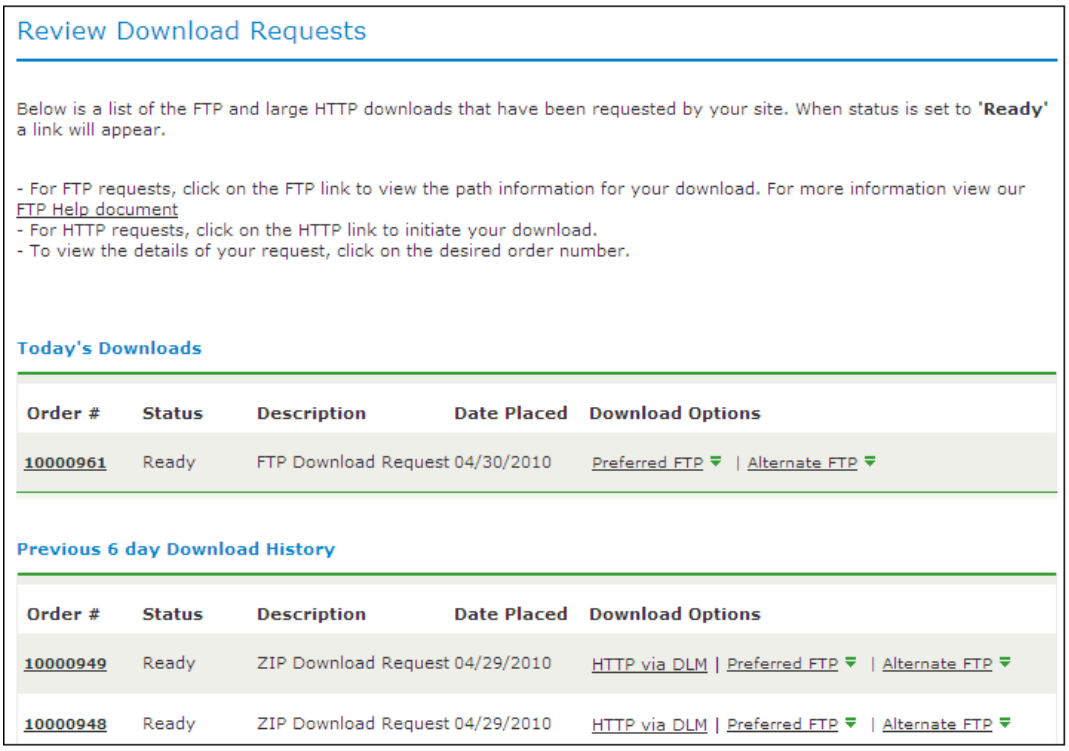
Note: For mainframe downloads using this HTTP method, click the Learn More link.



The HTTP method lets you start downloading immediately. The FTP method takes you to the Review Orders page that displays your order, first in a Pending status changing to Ready when your order has been processed.

Preferred FTP uses the new content delivery network (CDN). Alternate FTP uses the CA Technologies New York-based FTP servers.

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



Review Download Requests

Below is a list of the FTP and large HTTP downloads that have been requested by your site. When status is set to **'Ready'** a link will appear.

- For FTP requests, click on the FTP link to view the path information for your download. For more information view our FTP Help document
- For HTTP requests, click on the HTTP link to initiate your download.
- To view the details of your request, click on the desired order number.

Today's Downloads

Order #	Status	Description	Date Placed	Download Options
10000961	Ready	FTP Download Request	04/30/2010	Preferred FTP | Alternate FTP

Previous 6 day Download History

Order #	Status	Description	Date Placed	Download Options
10000949	Ready	ZIP Download Request	04/29/2010	HTTP via DLM | Preferred FTP | Alternate FTP
10000948	Ready	ZIP Download Request	04/29/2010	HTTP via DLM | Preferred FTP | Alternate FTP

USS Environment Setup

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

- Receive product pax files from CA Support Online.
- Perform utility functions to unpack the pax file into MVS data sets that you can use to complete the product installation.

We recommend that you allocate and mount a file system dedicated to Pax-Enhanced ESD. The amount of space that you need for the file system depends on the following variables:

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

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

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

Allocate and Mount a File System

You can use the zSeries File System (zFS) or hierarchical file system (HFS) for 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 SUPERUSER authority to do this.
- 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's 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_dataset_name) +
       STORAGECLASS(class) +
       LINEAR +
       CYL(primary secondary) +
       SHAREOPTIONS(3,3) +
       )
     /*
     //FORMAT   EXEC PGM=IOEAGFMT,REGION=0M,
     // PARM=('-aggregate your_zFS_dataset_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_dataset_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's requirements:

   - On a zFS, use the following sample:

     ```
     MOUNT FILESYSTEM('your_zFS_dataset_name')
           MOUNTPOINT('yourUSSESDdirectory')
           TYPE(ZFS)  MODE(RDWR)
           PARM(AGGRGROW)
     ```

   - On an HFS, use the following sample:

     ```
     MOUNT FILESYSTEM('your_HFS_dataset_name')
           MOUNTPOINT('yourUSSESDdirectory')
           TYPE(HFS)  MODE(RDWR)
     ```

   The file system is mounted.

4. (Optional) Set security permissions for the directory. You can use the chmod command to let other users access the ESD directory and its files. For example, to allow write access to the ESD directory for other users in your USS group, from the TSO OMVS shell, enter the following command:

   ```
   chmod -R 775 /yourUSSESDdirectory/
   ```

   Write access is granted.

   Note: For more information about the chmod command, see the 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's pax file into the USS directory you set up. Use one of the following methods:

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

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

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

Ensure that sufficient free space is available in the USS file system you are using for Pax-Enhanced ESD to hold the product pax file. If you do not have sufficient free space, error messages similar to the following appear:

```
EZA1490I Error writing to data set
EZA2606W File I/O error 133
```

When the download finishes, the pax file size in your USS directory matches the value in the Size column for the corresponding pax file on the CA Technologies Products Download window.

More Information:

How the Pax-Enhanced ESD Download Works (see page 127)
ESD Product Download Window (see page 128)

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://ftpdownloads.ca.com

   Alternate FTP

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

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

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

   Note: 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's statements in this JCL maybe  *
//*    optional at your site. Remove the statements that are not      *
//*    required. For the required statements, update the data set     *
//*    names with the correct site specific data set names.           *
//* 3. Replace "Host" based on the type of download method.           *
//* 4. Replace "YourEmailAddress" with your email address.            *
//* 5. Replace "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 to download the product pax or zip file to your PC. If you download a zip file, first unzip the file to use the product pax files.

   The pax or zip file resides on your PC.

2. Open a Windows command prompt.

   The command prompt appears.

3. Customize and enter the FTP commands with the following changes:

   a. Replace *mainframe* with the z/OS system's IP address or DNS name.

   b. Replace *userid* with your z/OS user ID.

   c. Replace *password* with your z/OS password.

   d. Replace *C:\PC\folder\for\thePAXfile* with the location of the pax file on your PC.

   e. Replace *yourUSSESDdirectory* with the name of the USS directory that you use for ESD downloads.

   f. Replace *paxfile.pax.Z* with the name of the pax file to upload.

   The pax file is transferred to the mainframe.

Example: FTP Commands

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

```
ftp mainframe
userid
password
bin
lcd C:\PC\folder\for\thePAXfile
cd /yourUSSESDdirectory/
put paxfile.pax.Z
quit
exit
```

Create a Product Directory from the Pax File

Use the sample job attached to the PDF file as Unpackage.txt to extract the product pax file into a product installation directory.

Important! To simplify the Pax-Enhanced ESD process, the PDF version of this guide includes 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 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.

   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 y*ourHLQ* to the high-level qualifier (HLQ) for z/OS data sets used by the installation process. We suggest that you use a unique HLQ for each expanded pax file to identify uniquely the package. Do *not* use the same value for y*ourHLQ* as you use for the SMP/E RELFILEs.

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

6. Submit the UNZIPJCL job.

   The UNZIPJCL job completes with a zero return code. Messages GIM69158I and GIM48101I in the output and IKJ56228I in the JES log are acceptable.

   GIMUNZIP creates z/OS data sets with the high-level qualifier you specified in the UNZIPJCL job. You use these data sets to perform the product installation. The pax file and product-specific directory are no longer needed.

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

Receiving the SMP/E Package

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

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

- DASD data set names for SMPPTFIN and SMPHOLD (if applicable)
- The HLQ that you used in the UNZIPJCL job on the RFPREFIX parameter on the RECEIVE command

How to Install Products Using Native SMP/E JCL

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

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

Prepare the SMP/E Environment for Pax Installation

The members in this procedure prepare the data sets, initialize the zones, and create the DDDEFs for CA XCOM Data Transport for z/OS. External DDDEF data sets are required. The default is NULLFILE.

Prior to beginning this procedure, confirm whether your product uses UNIX System Services (USS). If it does, establishing a hierarchical file system (HFS) may be required as part of the product installation or required as a feature of the product.

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

To prepare the SMP/E environment for your product

1. Customize the macro BXGSEDIT with your site-specific information and then copy the macro to your syslib location. Replace the rightmost parameters for each ISREDIT CHANGE macro command. Each time you edit an installation member, type BXGSEDIT on the TSO command line, and press Enter to replace the defaults with your specifications.

   The macro is ready to customize the *yourHLQ*.CAI.SAMPJCL members.

   Note: Set the DASD HLQ to the same value specified for *yourHLQ* for the unzip to DASD ESD JCL.

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

2. Open the SAMPJCL member BXG1ALL in an edit session and execute the BXGSEDIT macro from the command line.

   BXG1ALL is customized.

3. Submit BXG1ALL.

   This job produces the following results:

   - The target and distribution data sets for CA XCOM Data Transport for z/OS are created.
   - Unique SMPLTS, SMPMTS, SMPSCDS, and SMPSTS data sets for this target zone are created.

4. If your product requires HFS or if you want to install a feature of the product that requires HFS, complete the following substeps:

   a. Open the SAMPJCL member BXG1ALLU in an edit session and execute the BXGSEDIT macro from the command line.

      Note additional manual edits noted in comments.

      BXG1ALLU is customized.

   b. Submit BXG1ALLU.

      This job allocates your HFS data sets.

   c. Open the SAMPJCL member BXG2MKD in an edit session and execute the BXGSEDIT macro from the command line.

      Note additional manual edits noted in comments.

      BXG2MKD is customized.

   d. Submit BXG2MKD.

      This job creates all directories and mounts the file system.

5. Open the SAMPJCL member BXG2CSI in an edit session and execute the BXGSEDIT macro from the command line.

   BXG2CSI is customized.

6. Submit BXG2CSI.

   This job produces the following results:

   - The CSI data set is defined.
   - The SMPPTS and SMPLOG data sets are allocated.
   - The global, target, and distribution zones are initialized.
   - The DDDEF entries for your product are created.
   - The DDDEFs for the required SMP/E data sets are created.

7. If your product requires HFS or if you want to install a feature of the product that requires HFS, complete the following substeps:

   a. Open the SAMPJCL member BXG3CSIU in an edit session and execute the BXGSEDIT macro from the command line.

      Note additional manual edits noted in comments.

      BXG3CSIU is customized.

   b. Submit BXG3CSIU.

      This job customizes the CSI by adding the DDDEFs associated with the directory.

Run the Installation Jobs for a Pax Installation

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

Follow these steps:

1. Open the SAMPJCL member BXG3RECD in an edit session, and execute the BXGSEDIT macro from the command line.

   BXG3RECD is customized.

2. Submit the *yourHLQ*.CAI.SAMPJCL member BXG3RECD to receive SMP/E base functions.

   CA XCOM Data Transport for z/OS is received and now resides in the global zone.

3. Open the SAMPJCL member BXG4APP in an edit session, and execute the BXGSEDIT macro from the command line.

   BXG4APP is customized.

4. Submit the *yourHLQ*.CAI.SAMPJCL member BXG4APP to apply SMP/E base functions.

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

5. Open the SAMPJCL member BXG5ACC in an edit session, and execute the BXGSEDIT macro from the command line.

   BXG5ACC is customized.

6. Submit the *yourHLQ*.CAI.SAMPJCL member BXG5ACC to accept SMP/E base functions.

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

Clean Up the USS Directory

Important! This procedure is optional. Do not use this procedure until you complete the entire installation process.

To free file system disk space for subsequent downloads after downloading and processing the pax files for your CA Technologies product, we recommend removing the files from your USS directory and deleting unnecessary MVS data sets. You can delete the following items:

- Pax file
- Product-specific directory created by the pax command and all of the files in it
- SMP/E RELFILEs, SMPMCS, and HOLDDATA MVS data sets

  These data sets have the HLQ that you assigned in the UNZIPJCL job.

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

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 created by the pax command.

   The product-specific directory is deleted.

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

Apply Maintenance

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

Follow these steps:

1. Check CA Support Online and download any PTFs and HOLDDATA published since this release was created. If the base release was created recently, no PTFs or HOLDATA will have been published yet.
2. Transfer the downloaded files to two separate FB 80 sequential data sets. Use one data set to contain the PTFs and the other to contain the HOLDDATA.

   The PTFs and HOLDDATA become accessible to the *yourHLQ*.CAI.SAMPJCL maintenance members.

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

4. Open the SAMPJCL member BXG6RECP in an edit session and execute the BXGSEDIT macro from the command line.

   BXG6RECP is customized with your JOB statement, CSI location, and zone names.

5. Customize the BXG6RECP SMPPTFIN and SMPHOLD DD statements to reference the FB 80 data sets for the PTFs and HOLDDATA.

6. Submit BXG6RECP.

   The PTFs and HOLDDATA are received.

7. Open the SAMPJCL member BXG7APYP in an edit session and execute the BXGSEDIT macro from the command line.

   BXG7APYP is customized.

8. Submit BXG7APYP.

   The PTFs are applied.

9. (Optional) Open the SAMPJCL member BXG8ACCP in an edit session and execute the BXGSEDIT macro from the command line.

   BXG8ACCP is customized.

10. (Optional) Submit *yourHLQ*.CAI.SAMPJCL member BXG8ACCP.

    The PTFs are accepted.

    Note: You do not have to submit the job at this time. You can accept the PTFs according to your site policy.

Note: We recommend that you check for available maintenance; however, you may find that none is available.

HOLDDATA

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

Note: When you have completed the procedures in this section, go to Configuring Your Product (see page 157).

Chapter 5: Installing Your Product from Tape

This section contains the following topics:

Unload the Sample JCL from Tape

To simplify the process, the PDF version of this guide includes a sample JCL job that you can copy directly to the mainframe. To access this job, click the paper clip icon at the left of the PDF reader. A window displaying attachments opens. Double-click the UnloadJCL.txt file to view the sample JCL job.

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

Follow these steps:

1. Run the following sample JCL:

```
//COPY      EXEC PGM=IEBCOPY,REGION=4096K
//SYSPRINT  DD   SYSOUT=*
//SYSUT1    DD   DSN=CAI.SAMPJCL,DISP=OLD,UNIT=unitname,VOL=SER=nnnnnn,
//          LABEL=(1,SL)
//SYSUT2    DD   DSN=yourHLQ.SAMPJCL,
//          DISP=(,CATLG,DELETE),
//          UNIT=sysda,SPACE=(TRK,(15,3,6),RLSE)
//SYSUT3    DD   UNIT=sysda,SPACE=(CYL,1)
//SYSIN     DD   DUMMY
```

unitname

Specifies the tape unit to mount the tape.

nnnnnnn

Specifies the tape volume serial number.

yourHLQ

Specifies the data set prefix for the installation.

sysda

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

The SAMPJCL data set is created and its contents are downloaded from the tape.

2. Continue with one of the following options:
   - If you already have set up the SMP/E environment, go to Run the Installation Jobs for a Tape Installation.
   - If you have *not* set up the SMP/E environment, go to Prepare the SMP/E Environment for Tape Installation.

How to Install Products Using Native SMP/E JCL

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

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

Prepare the SMP/E Environment for Tape Installation

The members in this procedure prepare the data sets, initialize the zones, and create the DDDEFs for CA XCOM Data Transport for z/OS. External DDDEF data sets are required. The default is NULLFILE.

Prior to beginning this procedure, confirm whether your product uses UNIX System Services (USS). If it does, establishing a hierarchical file system (HFS) may be required as part of the product installation or required as a feature of the product.

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

To prepare the SMP/E environment for your product

1. Customize the macro BXGSEDIT with your site-specific information and then copy the macro to your syslib location. Replace the rightmost parameters for each ISREDIT CHANGE macro command. Each time you edit an installation member, type BXGSEDIT on the TSO command line, and press Enter to replace the defaults with your specifications.

   The macro is ready to customize the BXG.SAMPJCL members.

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

2. Open the SAMPJCL member BXG1ALL in an edit session and execute the BXGSEDIT macro from the command line.

   BXG1ALL is customized.

3. Submit BXG1ALL.

   This job produces the following results:

   - The target and distribution data sets for CA XCOM Data Transport for z/OS are created.
   - Unique SMPLTS, SMPMTS, SMPSCDS, and SMPSTS data sets for this target zone are created.

4. If your product requires HFS or if you want to install a feature of the product that requires HFS, complete the following substeps:

   a. Open the SAMPJCL member BXG1ALLU in an edit session and execute the BXGSEDIT macro from the command line.

      BXG1ALLU is customized.

   b. Submit BXG1ALLU.

      This job allocates your HFS data sets.

   c. Open the SAMPJCL member BXG2MKD in an edit session and execute the BXGSEDIT macro from the command line.

      BXG2MKD is customized.

d. Submit BXG2MKD.

   This job creates all directories and mounts the file system.

5. Open the SAMPJCL member BXG2CSI in an edit session and execute the BXGSEDIT macro from the command line.

   BXG2CSI is customized.

6. Submit BXG2CSI.

   This job produces the following results:

   - The CSI data set is defined.
   - The SMPPTS and SMPLOG data sets are allocated.
   - The global, target, and distribution zones are initialized.
   - The DDDEF entries for your product are created.
   - The DDDEFs for the required SMP/E data sets are created.

7. If your product requires HFS or if you want to install a feature of the product that requires HFS, complete the following substeps:

   a. Open the SAMPJCL member BXG3CSIU in an edit session and execute the BXGSEDIT macro from the command line.

      BXG3CSIU is customized.

   b. Submit BXG3CSIU.

      This job customizes the CSI by adding the DDDEFs associated with the directory.

Run the Installation Jobs for a Tape Installation

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

Follow these steps:

1. Open the SAMPJCL member BXG3RECT in an edit session and execute the BXGSEDIT macro from the command line.

   Note: Comment out any unwanted FMIDs.

   BXG3RECT is customized.

2. Submit the *yourHLQ*.SAMPJCL member BXG3RECT to receive SMP/E base functions.

   CA XCOM Data Transport for z/OS is received and now resides in the global zone.

3. Open the SAMPJCL member BXG4APP in an edit session and execute the BXGSEDIT macro from the command line.

   Note: Comment out any unwanted FMIDs.

   BXG4APP is customized.

4. Submit the *yourHLQ*.SAMPJCL member BXG4APP to apply SMP/E base functions.

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

5. Open the SAMPJCL member BXG5ACC in an edit session and execute the BXGSEDIT macro from the command line.

   Note: Comment out any unwanted FMIDs.

   BXG5ACC is customized.

6. Submit the *yourHLQ*.SAMPJCL member BXG5ACC to accept SMP/E base functions.

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

Apply Maintenance

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

Follow these steps:

1. Check CA Support Online and download any PTFs and HOLDDATA published since this release was created. If the base release was created recently, no PTFs or HOLDATA will have been published yet.
2. Transfer the downloaded files to two separate FB 80 sequential data sets. Use one data set to contain the PTFs and the other to contain the HOLDDATA.

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

3. The BXGSEDIT macro was customized in the installation steps. Verify that you still have the values from the base install.
4. Open the SAMPJCL member BXG6RECP in an edit session and execute the BXGSEDIT macro from the command line.

   BXG6RECP is customized with your JOB statement, CSI location, and zone names.

5. Customize the BXG6RECP SMPPTFIN and SMPHOLD DD statements to reference the FB 80 data sets for the PTFs and HOLDDATA.
6. Submit BXG6RECP.

   The PTFs and HOLDDATA are received.

7. Open the SAMPJCL member BXG7APYP in an edit session and execute the BXGSEDIT macro from the command line.

   BXG7APYP is customized.

8. Submit BXG7APYP.

   The PTFs are applied.

9. (Optional) Open the SAMPJCL member BXG8ACCP in an edit session and execute the BXGSEDIT macro from the command line.

   BXG8ACCP is customized.

10. (Optional) Submit *yourHLQ*.SAMPJCL member BXG8ACCP.

    The PTFs are accepted.

    Note: You do not have to submit the job at this time. You can accept the PTFs according to your site policy.

Note: We recommend that you check for available maintenance; however, you may find that none is available.

HOLDDATA

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

Note: When you have completed the procedures in this section, go to Configuring Your Product (see page 157).

Chapter 6: Configuring Your Product

This section describes the minimum configuration tasks needed before CA XCOM Data Transport for z/OS can be started, customized, and used in your environment.

This section contains the following topics:

Configure CA XCOM Data Transport for z/OS

You need to perform the following steps to configure CA XCOM Data Transport for z/OS. For more information about them, see the chapter “Configuring and Customizing Your Product” in the *CA XCOM Data Transport for z/OS Administration Guide*.

To configure CA XCOM Data Transport for z/OS

1. Define CA XCOM Data Transport to VTAM (as a VTAM application) (optional).
2. Define the logon mode table entries (optional).
3. Define the CA XCOM Data Transport Global options in the CONFIG member.

   Note: The CONFIG member should be used as the CA XCOM Data Transport Default Options Table is deprecated.
4. Configure CEEOPTS data set or PDS member to set and define the Language Environment runtime option.
5. Reassemble the CA ACF2 Security module (optional)
6. Define the libraries and install the TSO/ISPF facility.
7. Review and modify the CA XCOM Data Transport SSL configuration file, configssl.cnf, so that the settings meet your site standards for the server and client connections (optional).

   Important! When you install CA XCOM Data Transport, the SSL certificates are automatically generated. So you do not have to generate them as part of configuring CA XCOM Data Transport.

   For more information, or if you need to regenerate these certificates at any time, see the chapter "Generating SSL Certificates" in the *CA XCOM Data Transport for z/OS Administration Guide*.
8. Install and configure the CICS interface (panels have been deprecated - optional)
9. Assemble and link edit CA XCOM Data Transport user exits (optional).
10. Define the CA XCOM Data Transport destinations (optional).
11. Customize the code page conversion tables (optional).
12. Define the CA XCOM Data Transport system administrator table (optional).
13. Define the CA XCOM Data Transport server in a standalone or Plex environment.
14. Assemble and link edit the JES dependent module (based on JES release) (optional).
15. Configure for LSR Support (optional).
16. Verify the installation.

Set and Define the Language Environment Runtime Options (Optional)

The Language Environment Runtime Options are configured via control statements in a sequential data set or PDS member referenced by the CEEOPTS DD statement in the CA XCOM JCL.

Setting the IBM Language Environment Runtime Options is important because IBM/C uses these settings to determine the amount of memory that will be allocated for each transfer, as well as its location – either above or below the 16MB line. If more storage is allocated than CA XCOM Data Transport uses, the result is increased overall memory usage, which may lead to storage shortages and unpredictable or undesirable results.

The member CEEOPTS in library *yourhlq*.CBXGPARM contains the Runtime Options as distributed with CA XCOM Data Transport by default.

Important! For more information about the application-specific Runtime Options (CEEOPTS) as it relates to your version of the IBM operating system, see the Language Environment customization guide for your system.

Generate Exits and Tables used by CA XCOM Data Transport

Sample JCL and source statements are provided in libraries *yourhlq*.CBXGJCL and *yourhlq*.CBXGSAMP, which can be used to set the configuration parameters that control the execution of CA XCOM Data Transport servers.

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

To generate tables used by CA XCOM Data Transport

Important! To simplify future product updates and to preserve the original versions of sample modules, it is recommended that load modules generated for product tables and user exits be placed in a private library, rather than in the SMP/E controlled CA XCOM Data Transport target libraries.

1. You can assemble your customized #DFLTAB member using the JCL in member ASM#TBLS in library *yourhlq*.CBXGJCL. There are new parameters for the CA XCOM Data Transport default options table for r11.6. Be sure to customize and assemble the r11.6 version of this table. Modify this JCL to include your CA XCOM Default Options Table source, uncomment the DFLT job step, change the M= parameter to match the name of your CA XCOM Default Options source member, and submit the JCL for execution. Every effort has been made to provide reasonable defaults for new keyword parameters of the #DFLTAB macro, but you should review the *CA XCOM Data Transport for z/OS Administration Guide* and evaluate the new parameters on an individual basis.

   Important! The CA XCOM Default option table is deprecated. Instead, the global parameter customization should take place using the yourhlq.CBXGPARM(XCOMCNFG) member. For more information see the *CA XCOM Data Transport for z/OS Administration Guide*.

2. If you use CA XCOM-specific SNA LOGMODE entries at your installation, you can use the JCL in member ASM#TBLS in library *yourhlq*.CBXGJCL to generate the table that holds these entries. Uncomment the TABL job step and change the M= parameter to match the name of your SNA LOGMODE table source. The resultant LOAD module must be placed in a LOAD library which is accessible by the Communication Server (VTAM). The Communication Server (VTAM) must be recycled to pick up the newly-generated LOGMODE table.

3. You can also use member ASM#TBLS in library *yourhlq*.CBXGJCL to assemble and link the sample user exits which that are shipped as part of CA XCOM Data Transport. Do not remove the RN=RENT specification from the EXEC statements on which it is specified. Some of the user exits must be generated as reentrant. Failure to do so results in abends in the CA XCOM Data Transport server or other unpredictable and undesirable results.

Reassemble the CA ACF2 Security Module (CA ACF2 Security Users Only)

All CA XCOM Data Transport installations using CA ACF2 Security as their security interface must reassemble the CA ACF2 Security module of CA XCOM Data Transport.

Important! To enable CA ACF2 Security with CA XCOM Data Transport, set SECURITY=ACF2 in the XCOMDFLT table. For more information, see the chapters "Configuration Parameters" and "Security Considerations" in the *CA XCOM Data Transport for z/OS Administration Guide*.

Member ASMACF2U in *yourhlq*.CBXGJCL provides an example of assembling and linking this CA ACF2 Security module (see the appendix "Sample Files" in the *CA XCOM Data Transport for z/OS User Guide*).

Define the Libraries and Install the TSO/ISPF Facility

This step of the installation process involves several sub-steps, which are described in the following sections along with pertinent background information.

A. Authorize the Load Library

The CA XCOM Data Transport load modules, user exits, and tables are contained in the CA XCOM Data Transport load library called *yourhlq*.CBXGLOAD. This library must be APF authorized by specifying it in the IEAAPFxx member of SYS1.PARMLIB.

Note: If LNKAUTH=LNKLST is specified in the IEASYS*xx* member of SYS1.PARMLIB, the CA XCOM Data Transport load library name can be specified in the LNKLST*xx* member, instead of the IEAAPF*xx* member. This is useful if you want the CA XCOM Data Transport library to be part of the system link list. In either case, changes are not active until the next IPL.

A linklist can be updated dynamically by using the following:

1. SETPROG LNKLST,DEFINE,NAME=*name*,COPYFROM=CURRENT
2. SETPROG LNKLST,ADD,NAME=*name*,DSNAME='cailib',VOLUME=*volser*
3. SETPROG LNKLST,ACTIVE,NAME=*name*

For more information about load library authorization, see IBM's *MVS Initialization and Tuning* manual.

Important! CA XCOM Data Transport modules, and the XCF (Coupling Facility) modules, should not be copied into an authorized library containing modules from other software packages, because that would make upgrading to new releases very difficult and module name conflicts could occur.

Note: CA XCOM Data Transport will not start if the libraries are not APF authorized.

B. Concatenate the TSO/ISPF Libraries

Concatenate the CA XCOM Data Transport TSO/ISPF libraries listed in the following table with the proper libraries for your installation.

Library	Contents
yourhlq.CBXGPNL0	CA XCOM Data Transport Menu Interface (TSO/ISPF) panels
yourhlq.CBXGMSG0	CA XCOM Data Transport TSO/ISPF messages
yourhlq.CBXGCLS0	CLISTs that invoke the ISPF dialogs
yourhlq.CBXGLOAD	CA XCOM Data Transport load library is also required for the TSO/ISPF interface
yourhlq.CBXGTBL0	CA XCOM Data Transport ISPF table
yourhlq.CBXGPARM	Contains CEEOPTS member with Runtime Options and the XCOMCNFG with global CA XCOM parameter options

C. Install the TSO/ISPF Facility

You need to install version 4.2 or higher of ISPF to use the TSO/ISPF facility (menu interface) of CA XCOM Data Transport. To install the TSO/ISPF dialog for CA XCOM Data Transport, libraries for CA XCOM Data Transport must be concatenated to the ISPPLIB, ISPMLIB, STEPLIB, ISPLLIB, ISPTLIB, and SYSPROC DD statements in your TSO logon procedures. The JCL in the following section shows how this is done.

To install the TSO/ISPF Facility

1. Provide correct data set names on the lines indicated by the bold type in the JCL. If the CA XCOM Data Transport load library was not added to the link list, a STEPLIB must be added to the logon procedure.

```
//$LOGON   EXEC PGM=IKJEFT01,REGION=3092K,
//         DYNAMNBR=50
//*
//STEPLIB  DD  DSN=CAI.CBXGLOAD,DISP=SHR
//         DD  DSN=CAI.CBXGPARM,DISP=SHR
//SYSHELP  DD  DISP=SHR,DSN=SYS1.HELP
//ISPLLIB  DD  DSN=CAI.CBXGLOAD,DISP=SHR
//ISPPLIB  DD  DSN=SYS1.ISPF.ISPPLIB,DISP=SHR,DCB=BLKSIZE=23440
//         DD  DSN=CAI.CBXGPNL0,DISP=SHR
//ISPSLIB  DD  DSN=SYS1.ISPF.ISPSLIB,DISP=SHR,DCB=BLKSIZE=23440
//ISPMLIB  DD  DSN=SYS1.ISPF.ISPMLIB,DISP=SHR,DCB=BLKSIZE=23440
//         DD  DSN=CAI.CBXGMSG0,DISP=SHR
//ISPTLIB  DD  DSN=CAI.CBXGTBL0,DISP=SHR,DCB=BLKSIZE=23440
//         DD  DSN=SYS1.ISPF.ISPTLIB,DISP=SHR
//SYSPROC  DD  DSN=SYS1.ISPF.SYSPROC,DISP=SHR
//         DD  DSN=CAI.CBXGCLS0,DISP=SHR
//CEEOPTS  DD  DSN=CAI.CBXGPARM(CEEOPTS),DISP=SHR
//SYSLBC   DD  DSN=SYS1.BRODCAST,DISP=SHR
//SYSPRINT DD  TERM=TS,SYSOUT=Z
//SYSTERM  DD  TERM=TS,SYSOUT=Z
//SYSIN    DD  TERM=TS
//SYSDUMP  DD  SYSOUT=Q
```

2. When inserting CA XCOM Data Transport libraries into the TSO logon procedure, the library block size must be large enough to accommodate the CA XCOM Data Transport library block size. For example, if the CA XCOM Data Transport panel library, *yourhlq*.CBXGPNL0, is concatenated last under the ISPPLIB DD statement, the block size of the other data sets concatenated under ISPPLIB must be equal to or greater than the block size of *yourhlq*.CBXGPNL0. (This requirement can be circumvented by coding a DCB=BLKSIZE parameter to a value equal to the largest block size.)

Important! Be aware that the CA XCOM Data Transport SYSPROC is distributed in fixed block format. Occasionally, users find that their existing SYSPROCs use variable block format. The CA XCOM Data Transport SYSPROC and your other concatenated SYSPROCs must be defined as one or the other. There cannot be a combination of the two formats.

IBM TCP/IP Support

CA XCOM Data Transport provides you with an option to use TCP/IP instead of VTAM for scheduling and inquiry.

The following requirements apply to IBM TCP/IP support:

- The following libraries must be in the link list or the STEPLIB:

  ```
  DSN=CEE.SCEERUN
  ```

  (The library name may be different at your installation.)

  Note: DSN=CEE.SCEERUN2 is not needed for the CA XCOM TSO/ISPF Facility. It is also not needed for CA XCOM Data Transport to do transfers.

- The following DD statement should be added to the TSO LOGON proc:

  ```
  //SYSTCPD DD DSN=TCPIP.DESV.PROFILE(TCPDATA)
  ```

Allowing TYPE=EXECUTE Transfers of PDSE Program Libraries

To allow users to perform TYPE=EXECUTE transfers of PDSE program libraries, you must add XCOMJOB to the AUTHPGM and the AUTHTSF tables of IKJTSO00 module in SYS1.PARMLIB. The CA XCOM Data Transport libraries used in your CLIST for the CA XCOM Data Transport ISPF interface must all be APF authorized also.

You can also refresh the TSO library using the TSO UPDATE PARMLIB(00) member. For more information, see IBM's *TSO/E Customization* manual.

Note: The following DD statement should be added to the TSO LOGON proc:

```
//XCOMPRNT  DD    TERM=TS,SYSOUT=Z
```

Allowing TYPE=EXECUTE Transfers with SECURITY=SAF Specified in XCOM Default Option Table

To allow users to perform TYPE=EXECUTE transfers when using SAF security, you must add XCOMJOB to the AUTHPGM and the AUTHTSF tables of IKJTSO00 module in SYS1.PARMLIB. The CA XCOM Data Transport libraries used in your CLIST for the CA XCOM Data Transport ISPF interface must all be APF authorized also.

You can also refresh the TSO library using the TSO UPDATE PARMLIB(00) member. For more information, see IBM's *TSO/E Customization* manual.

Allowing TYPE=OPER (Operator) Requests from ISPF to the PLEXQ

To allow users to perform TYPE=OPER transfers of PDSE program libraries, add XCOMPLEX to the AUTHPGM and the AUTHTSF tables of IKJTSO00 module in SYS1.PARMLIB. The CA XCOM Data Transport libraries used in your CLIST for the CA XCOM Data Transport ISPF interface must all be APF authorized also.

You can also refresh the TSO library using the TSO UPDATE PARMLIB(00) member. For more information, see the *IBM TSO/E Customization manual*.

D. Customize the ISPF Dialogs

The ISPF Primary Option Menu (or any other ISPF panel) can be modified to include an option for calling the CA XCOM Data Transport Primary Option Menu (XCOMPRIM) by inserting the lines shown in bold in the following sample primary panel definition. Also, the XCOM62 CLIST supplied in the data set *yourhlq*.CBXGCLS0 can invoke the CA XCOM Data Transport TSO/ISPF dialog. For Japanese support, see the appendix Japanese ISPF Panel Support.

```
%----------------------ISPF/PDF PRIMARY OPTION MENU---------------------------
%OPTION   ===_ZCMD                                                            +
%                                                                 +USERID    &ZUSER
%   0    +ISPF PARMS    Specify terminal and user parameters     +TIME      &ZTIME
%   1    +BROWSE        Display source data or output listings   +TERMINAL  &ZTERM
%   2    +EDIT          Create or change source data             +PFKEYS    &ZKEYS
%   3    +UTILITIES     Perform utility functions
%   4    +FOREGROUND    Invoke language processors in foreground
%   5    +BATCH         Submit job for language processing
%   6    +COMMAND       Enter TSO command or CLIST
%   7    +DIALOG TEST   Perform dialog testing
%   8    +LM UTILITIES  Perform library administrator utility functions
%   9    +IBM PRODUCTS  Additional IBM program development products
%   XC   +XCOM          Multiplatform file transfer application
%   C    +CHANGES       Display summary of changes for this release
%   T    +TUTORIAL      Display information about ISPF/PDF
%   X    +EXIT          Terminate ISPF using log and list defaults
%
+Enter %END+ command to terminate ISPF.
%
)INIT
  .HELP=ISR00003
  &ZPRIM=YES             /*ALWAYS A PRIMARY OPTION MENU*/
  &ZHTOP=ISR00003        /*TUTORIAL TABLE OF CONTENTS*/
  &ZHINDEX=ISR91000      /*TUTORIALINDEX 1STPAGE*/
  VPUT (ZHTOP,ZHINDEX) PROFILE
)PROC
&ZQ=&Z
  IF (&ZCMD^='')
    &ZQ=TRUNC(&ZCMD,'.')
    IF(&ZQ='')
     .MSG=ISRU000
 &ZSEL=TRANS(&ZQ
             0,'PANEL(ISPOPTA)'
             1,'PGM(ISRBRO)PARM(ISRBRO01)'
             2,'PGM(ISREDIT)PARM(P,ISREDM01)'
             3,'PANEL(ISRUTIL)'
             4,'PANEL(ISRFPA)'
             5,'PGM(ISRJB1)PARM(ISRJPA)NOCHECK'
             6,'PGM(ISRPTC)'
             7.'PGM(ISRYXDR) NOCHECK'
             8,'PANEL(ISRLPRIM)'
             9,'PANEL(ISRDIIS)'
             C,'PGM(ISPTUTOR)PARM(ISR00005)'
             T,'PGM(ISPTUTOR)PARM(ISR00000)'
             XC,'PANEL(XCOMPRIM)NEWAPPL(XCOM)'
             ' ',' '
             X,'EXIT
             *,'?')
  &ZTRAIL=.TRAIL
)END
```

Install and Configure the CICS Interface

Important! The existing CICS facility panels have been deprecated. The following information is provided for backward compatibility only. All new installations should use the ISPF facility. Existing CICS users should migrate to the TSO/ISPF facility.

This step needs to be performed only if the CA XCOM Data Transport CICS interface is being installed.

About Installing the CICS Interface

The CA XCOM Data Transport CICS interface is easy to install. No authorized libraries are required. While gaining full CA XCOM Data Transport CICS functionality requires bringing CICS down and then up, it is possible to run the product without bringing CICS down.

Installing the CA XCOM Data Transport CICS interface requires both of the following:

- Creating the XCOMDFLT VSAM file
- Updating the CICS DFHCSD data set with CA XCOM Data Transport CICS entries

These tasks are described in the following sections.

About the XCICCHLP Macro

A new sample program, XCICCHLP (available in the library *yourhlq*.CBXGSAMP) is also distributed with the installation files. The XCICCHLP program is a macro that lets you modify the help text when there are language considerations. This sample program contains the default help text.

Note: There is no need to compile the sample program unless there are language considerations. Compiling the sample program, without change, produces load module XCICCHLP exactly as distributed in *yourhlq*.CBYCLOAD.

The XCICCHLP macro is as follows:

```
XCICCHLP TYPE=BEGIN,SCREEN=xxxxxxxx

XCICCHLP TYPE=DATA,ENDROW=nn,ENDCOL=nn,SEQ=nn,STROW=nn,STCOL=nn,X

TEXT='text'

XCICCHLP TYPE=END
```

Notes:

- TYPE=BEGIN is coded once for each screen containing help text.
- TYPE=DATA is coded as follows:
  - For every field, for field help.
  - For every screen, for screen help.
- TYPE=END is coded only once, as the last statement.
- ENDROW=, ENDCOL=, STROW=, and STCOL= are used for field help.
- ENDROW=99 and ENDCOL=99 are used for screen help.

Language considerations:

- If there are language considerations, you can modify the text values and then must assemble and link the XCICCHLP module into a library pointed to by the DFHRPL DD statement.
- If there are no language considerations, then you do not have to be concerned with the XCICCHLP macro and program.

Create the XCOMDFLT VSAM File

The XCOMDFLT VSAM file allows CA XCOM Data Transport CICS to save the information that you enter on CA XCOM Data Transport screens, so that it is displayed on the screen the next time you are engaged in a CA XCOM Data Transport transaction.

The JCL needed to define the XCOMDFLT file is located in the sample library member DEFDFLT, which is available in the library *yourhlq*.CBXGJCL.

The DEFDFLT member JCL is listed in the following procedure and a copy is provided also in the appendix "Sample Files" in the *CA XCOM Data Transport for z/OS User Guide*.

To create the XCOMDFLT VSAM file

1. Modify member DEFDFLT in library *yourhlq*.CBXGJCL as noted in the JCL comments.

   The first JCL step creates a temporary file, which the system copies to the VSAM cluster in the second step.

2. There are two parameters that you can enter as input to the XCICCICI installation program, SERVER APPLID and OPER TRAN:

   - SERVER APPLID defines the default CA XCOM Data Transport server with which CICS communicates. Although CA XCOM Data Transport CICS communicates with many CA XCOM Data Transport servers, the SERVER APPLID is the APPLID that CA XCOM Data Transport displays on the Primary Menu (XCICPRIM) screen (see the chapter “The Menu Interface” in the *CA XCOM Data Transport for z/OS User Guide*) when you log on to CA XCOM Data Transport for the first time. You can change that value on the XCICPRIM screen and CA XCOM Data Transport reflects the changes on your default parameter profile only. The default for this parameter is SERVER APPLID=XCOMAPPL.
   - OPER TRAN defines the CA XCOM Data Transport CICS transaction that gives the equivalent CA XCOM Data Transport security access to TSO OPER capability. For more information about this parameter, see the chapter “Security Considerations” in the *CA XCOM Data Transport for z/OS Administration Guide*. The parameter's default is OPER TRAN=XCOM.

   The second step executes the IDCAMS utility and logically performs these three functions:

   - Deletes the old XCOMDFLT data set if it exists.
   - Defines the XCOMDFLT VSAM cluster.
   - Copies the temporary file created in Step 1 to the VSAM cluster.

Note: To change the global default data without deleting user profiles, you can run this step without deleting and defining the XCOMDFLT file to simply update the global default record on the file.

About Configuring the CICS Interface

CA XCOM Data Transport CICS requires standard resource definitions be made in the CICS DFHCSD data set. CA XCOM Data Transport CICS requires no modifications of any sort. The following types of definitions are required to run CA XCOM Data Transport CICS:

- FCT adds CA XCOM Data Transport file definitions
- PCT adds CA XCOM Data Transport transaction definitions
- PPT adds CA XCOM Data Transport program definitions
- TCT adds CA XCOM Data Transport server definitions

Sample member XCOMCSD invokes IBM CICS utility DFHCSDUP to add the entries to the DFHCSD data set. XCOMCSD is provided in the library yourhlq.CBXGJCL and appendix Sample Files in the CA XCOM Data Transport for z/OS User Guide.

CICS JCL Updates

You must ensure that the CA XCOM Data Transport CICS load modules are available. You can accomplish this in one of two ways:

- Add *yourhlq*.CBYCLOAD to the DFHRPL concatenation.
- Move the modules in *yourhlq*.CBYCLOAD into a library already in the DFHRPL concatenation.

You must add the CA XCOM Data Transport CICS XCOMDFT file to the CICS JCL if the file is defined without the DSN and DISP parameters in its DFHCSD definition. Remember that the file definition statements provided in the sample JCL do not contain the DSN= and DISP= parameters.

Chapter 7: Starting Your Product

This section describes what you need to do to start CA XCOM Data Transport for z/OS.

This section contains the following topics:

Execute CAIRIM to Install LMP (Non-MSM Install Only)

CAIRIM, the Resource Initialization Manager, is used to provide product licensing for CA XCOM Data Transport. CAIRIM is one of the CA Common Services for z/OS. CAIRIM prepares your operating system environment for CA z/OS products and components and executes them.

CAIRIM routines are grouped under CA MVS Dynamic Service Code S910. Review the CA Common Services for z/OS (CCS) documentation for further details about the features and associated utilities of CAIRIM.

Using CA LMP

CA XCOM Data Transport for z/OS requires CA LMP (License Management Program), one of the CA Common Services (CCS), to initialize correctly. CA LMP also provides a standardized and automated approach to the tracking of licensed software.

Examine the CA LMP Key Certificate you received with your CA XCOM Data Transport for z/OS installation or maintenance tape. The certificate contains the fields shown in the following table.

CPU ID

The code that identifies the specific CPU for which installation of your CA XCOM Data Transport for z/OS is valid

CPU Location

The address of the building where the CPU is installed.

Execution Key

An encrypted code required by CA LMP for CA XCOM Data Transport for z/OS initialization. During installation, it is referred to as the LMP Code

Expiration Date

The date (ddMONyy as in 20OCT03) when your license for CA XCOM Data Transport for z/OS expires.

MIS Director

The name of the Director of MIS, or the person who performs that function at the site. If the title, but not the individual's name, is indicated on the Certificate, you should supply the actual name when correcting and verifying the Certificate.

Product Name

The trademarked or registered name of the CA XCOM Data Transport for z/OS licensed for the designated site and CPUs.

Product Code

A two character code that corresponds to CA XCOM Data Transport for z/OS.

Supplement

The reference number of your license for CA XCOM Data Transport for z/OS, in the format nnnnnn nnn. This format differs slightly inside and outside North America, and in some cases may not be provided at all.

Technical Contact

The name of the technical contact at your site who is responsible for the installation and maintenance of the designated CA XCOM Data Transport for z/OS. This is the person to whom CA addresses all CA LMP correspondence.

CA LMP is provided as an integral part of CAIRIM (Resource Initialization Manager), a component of CA Common Services. Once CAIRIM has been installed or maintained at the Service Level specified in the cover letter for this product release, CA LMP support is available for all CA LMP supported software solutions.

The CA LMP execution key, provided on the Key Certificate, must be added to the CAIRIM parameters to ensure proper initialization of the CA software solution. To define a CA LMP execution key to the CAIRIM parameters, modify member KEYS in OPTLIB data set.

The parameter structure for member KEYS is presented below:

PROD(*pp*) DATE(*ddmmmyy*) CPU(*tttt mmmm/ssssss*) LMPCODE(*kkkkkkkkkkkkkkkk*)

The parameters are as follows:

pp

Specifies the two-character product code. For any given CA LMP software solution, this code agrees with the product code already in use by the CAIRIM initialization parameters for earlier genlevels of CA XCOM Data Transport for z/OS. This is a required parameter.

ddmmmyy

The CA LMP licensing agreement expiration date.

tttt mmmm

Specifies the CPU type and model (for example, 3090 600) on which the CA LMP software solution is to run.

If the CPU type or model requires less than four characters, blank spaces are inserted for the unused characters. This is a required parameter.

ssssss

Specifies the serial number of the CPU on which the CA LMP software solution is to run. This is a required parameter.

kkkkkkkkkkkkk

Specifies the execution key needed to run the CA LMP software solution. This CA LMP execution key is provided on the Key Certificate shipped with each CA LMP software solution. This is a required parameter.

Example:

In the following example of a control statement for the CA LMP execution software parameter, the CA LMP execution key value is invalid and provided as an example only.

PROD(FX) DATE(01JAN03) CPU(3090 600 /370623) LMPCODE(52H2K06130Z7RZD6)

For more information about the procedure for defining the CA LMP execution key to the CAIRIM parameters, see the *CA Common Services for z/OS Administrator Guide*.

Allocate the Request Queue

This step allocates and initializes the CA XCOM Data Transport request queue. The request queue contains one record for each locally initiated transfer request. It is also used to store checkpoint/restart information for each remotely initiated transfer request. Ensure that the number of records in the file defined by the RECORDS parameter is large enough to accommodate all of the transfer requests which may be queued at any one time. This includes locally initiated pending and active queued file transfers and remotely initiated requests that contain restart information.

To allocate the request queue

1. Assign the cluster name assigned to this VSAM RRDS file to the XCOMRRDS DD statement also in the CA XCOM Data Transport server JCL.

   yourhlq.CBXGJCL(DEFRRDS) on the distribution tape provides sample JCL for this step (see the appendix “Sample Files” in the CA XCOM Data Transport for z/OS User Guide).

2. Edit this file, specifically the VOL, RECORDS, and NAME statements, to comply with your installation requirements. Note that this sample JCL indicates a maximum file size of 1500 records.

Note: Attempting to use an XCOMRRDS data set from a prior release of CA XCOM Data Transport can result in abnormal terminations of the server, or other unpredictable and undesirable results.

Define/Migrate the VSAM History File

This step creates or migrates an existing CA XCOM Data Transport VSAM history file and its alternate indices and paths. In creating alternate indices, you must use the primary cluster to limit the size of the history data. This process creates a secondary allocation space for the alternate indices. These JCL DD statements are associated with the CA XCOM Data Transport history file:

- XCOMHIST
- XCOMREQ
- XCOMUSER
- XCOMINDT
- XCOMRECP
- XCOMSYST

To define a new History file

yourhlq.CBXGJCL (DEFHIST) provides sample JCL for this step (see the appendix "Sample Files" in the *CA XCOM Data Transport for z/OS User Guide*). Modify this JCL, specifically the NAME and space related statements, to comply with your installation requirements.

To migrate an existing History file

yourhlq.CBXGJCL (XCOMH116) provides sample JCL for this step (see the appendix Sample Files in the CA XCOM Data Transport for z/OS User Guide). Modify this JCL, specifically the NAME and space related statements, to comply with your installation requirements. This JCL invokes the XCOMUTIL History File utility to increase the size of existing history records while optionally allowing older records to be removed. Please refer to Chapter 8: Migration Information for more information on history file migration.

Note: Attempting to use an XCOMHIST data set from a prior release of CA XCOM Data Transport can result in abnormal terminations of the server, or other unpredictable and undesirable results.

Define/Migrate the DB2 History Database

Releases of CA XCOM Data Transport for z/OS prior to r11.5 SE1 only wrote history records into a VSAM file. Starting with r11.5 SE1, CA XCOM Data Transport for z/OS can record history in a relational database, using ODBC. The supported database is DB2 for z/OS, version 9 or higher.

Also provided with this feature is the ability to write history records when TYPE=EXECUTE transfers are performed by XCOMJOB.

When this feature is installed, you can choose to continue to record History Records using VSAM (the default) instead of ODBC. In this case, TYPE=EXECUTE transfers do not record any history records.

You can convert your current CA XCOM Data Transport history VSAM files to a relational database by using the new conversion program, XCV2ODBC.

Currently, each CA XCOM Data Transport server must have its own VSAM file for history. If you choose is to use ODBC then servers can share the same relational database. That is, z/OS, Windows, and UNIX can all be using the same relational database.

Create and Administer the DB2 Database

To set up a relational database to house CA XCOM Data Transport history records, the following administrative tasks are required:

- Add settings for new parameters in the CA XCOM Data Transport Default Options Table.
- Create the database, tables, and indexes for CA XCOM Data Transport history.
- Grant database permissions to users.
- To access a DB2 database on a remote system, establish a bind plan to allow CA XCOM Data Transport to access the database.
- Create a data set to store ODBC configuration parameters.
- Modify JCL for the CA XCOM Data Transport started task, Admin Server, and XCOMJOB to include additional data sets required for ODBC processing.

Parameters

The following parameters have been added to the Default Options Table to describe the information required to connect and work with ODBC history:

- HISTORY
- SYSID
- SYSNAME
- XCOMHIST
- XCOMHIST_OWNER
- XCOMHIST_PASSWORD
- XCOMHIST_TBL
- XCOMHIST_USER

Notes:

- By default, history will be stored in a VSAM file, as is the case with the current version of CA XCOM Data Transport for z/OS.
- For descriptions of these parameters, please refer to the CA XCOM Data Transport for z/OS Administrator Guide.

Create a Database (Optional)

The history table needs to reside in a database.

You can do one of the following:

- Use an existing database.
- Create a new database specifically for CA XCOM Data Transport history. You can select any name for this database. You can specify additional options according to the needs of your installation.

To create a new database

```
CREATE DATABASE database_name <additional_options>;
```

Create a Tablespace (Optional)

A tablespace is the storage mechanism used by DB2 for storing table data. Tablespaces are implicitly created when creating a table, but can be explicitly created in order to customize or optimize storage.

To create a tablespace

```
CREATE TABLESPACE tablespace_name <additional_options>;
```

Create the History Table

Note: The history table name can be selected by the installation.

CA XCOM Data Transport history requires a single database table and three indexes, which are used for history queries. The DDL is provided in member HISTDDL in the CBXGSAMP data set provided by the CA XCOM Data Transport installation (see the appendix Sample Files in the CA XCOM Data Transport for z/OS User Guide). HISTDDL can be used as input to SPUFI.

To customize HISTDDL

1. If the default database name is not desired or additional options are needed, customize the DDL statement as desired.

   Note: If an existing database is to be used, then you need to comment out the statements or remove them.

2. If a customized tablespace is desired, include the DDL to create the tablespace, following the database and before the creation of the table.
3. Change the DDL for the table creation to include the desired schema name, table name, database name, and, if defined, tablespace name.
4. Change the DDL for the indexes to include the desired schema name and index name.
5. If desired, create additional indexes to improve the performance of history searches, based on the fields commonly used for searches.

   You can include the following columns in indexes:

   - user_name
   - error_message
   - initiated_by
   - remote_system
   - invoking_jobname
   - volume
   - local_volume
   - file
   - lfile
   - rluname
   - conversation_type
   - byte_count

Notes:

- Not all columns are used by all operating systems. The subset of fields used by CA XCOM Data Transport for z/OS are those fields defined in the HSTDSECT control block.
- Column names cannot be modified or deleted.

Grant Database Permissions

Note: This step is required only if the creator of the table is not the user ID that will be used to access the table.

Example:

User TSOUSER creates the XCOM_HISTORY_TBL, but does not want to put his or her encrypted password into the CA XCOM Data Transport Default Options Table. So a user called XCOMUSER is created, only having access to the DB2 system.

Therefore the default table would have the following values:

- XCOMHIST_OWNER=TSOUSER
- XCOMHIST_USER=XCOMUSER
- XCOMHIST_PASSWORD=(the 70-character encrypted password of XCOMUSER)

Access must be granted by TSOUSER (or another user with authority) to XCOMUSER, as follows:

```
GRANT ALL ON XCOMHIST.XCOM_HISTORY_TBL TO XCOMUSER;
```

Establish a Bind Plan

Because CA XCOM Data Transport is an ODBC application with no imbedded SQL, you can run CA XCOM Data Transport using the default plan DSNACLI. For more information, see member DSNTIJCL in the DB2 SDSNSAMP dataset for binding the DSNACLI plan.

The DSNACLI plan uses a package list that includes all of the ODBC packages. If your CA XCOM Data Transport server is to be run on the same processor where this plan is bound, then using the default plan is sufficient. However, if your CA XCOM Data Transport server is to be run on a processor that is not where the table is defined, then you will have to create your own plan for CA XCOM Data Transport.

Example:

```
DSN SYSTEM(D91B)
BIND PLAN(XCOMODBC)                    -
  PKLIST(DSNAOCLI.DSNCLICS             -
         DSNAOCLI.DSNCLINC             -
         DSNAOCLI.DSNCLIRR             -
         DSNAOCLI.DSNCLIRS             -
         DSNAOCLI.DSNCLIUR             -
         DSNAOCLI.DSNCLIC1             -
         DSNAOCLI.DSNCLIC2             -
         DSNAOCLI.DSNCLIF4             -
         DSNAOCLI.DSNCLIMS             -
         DSNAOCLI.DSNCLIQR             -
D91APTIB.DSNAOCLI.DSNCLINF             )
END
```

This example shows two processors, CA11 and CA31. The DB2 system D91B runs on CA11, but the XCOM_HISTORY_TBL is defined on system D91A on CA31. There is an entry in SYSIBM.LOCATIONS for D91BPTIB, pointing to the DB2 on CA31.

Create the XCOMODBI Data Set

DB2 for z/OS uses an initialization file DSNAOINI for setting ODBC configuration options.

To allow CA XCOM Data Transport to run on any processor capable of handling DB2 requests, an XCOMODBI data set must be defined to contain model ODBC configuration statements. A sample data set is provided in member DSNAOINI of the CBXGSAMP data set when you install CA XCOM Data Transport (see the appendix Sample Files in the CA XCOM Data Transport for z/OS User Guide).

XCOMODBI allows you to specify the appropriate DB2 subsystem ID, based on the processor that CA XCOM Data Transport has been started on. You can specify substitution parameters to allow configuration information to be tailored based on the system that CA XCOM Data Transport is running on. On startup of CA XCOM Data Transport, the data set is processed and appropriate configuration statements are written to DSNAOINI for ODBC initialization.

You can add special control statements as needed, in the following format:

```
;CONVERT SMFID,DB2ID
```

Example:

```
;CONVERT CA11:D91B
;CONVERT CA31:D91A
[COMMON]
MVSDEFAULTSSID=*
APPLTRACE=1
APPLTRACEFILENAME=DD:APPTRACE
DIAGTRACE=1
; EXAMPLE SUBSYSTEM STANZA FOR D91B SUBSYSTEM  - CA11
[*]
MVSATTACHTYPE=CAF
PLANNAME=XCOMODBC
```

Notes:

- When these statements are processed, MVSDEFAULTSSID=* is translated to one of the following values:
  - MVSDEFAULTSSID=D91A if CA XCOM Data Transport is started on CA31
  - MVSDEFAULTSSID=D91B if CA XCOM Data Transport is started on CA11
- [*] is changed to one of the following values:
  - [D91A] if CA XCOM Data Transport is started on CA31
  - [D91B] if CA XCOM Data Transport is started on CA11

- The above statements are used by DSNAOCLI to establish a connection to the appropriate database in conjunction with the ODBC data source name specified by the XCOMHIST= parameters defined in the CA XCOM Data Transport Default Options Table.
- Use of this file is required when CA XCOM Data Transport is writing to a database on a remote system, because the DSNAOCLI bind plan generated in the previous step needs to be specified.
- When writing to a database on the local system, this file is not required, and can be allocated as a dummy file in JCL (//XCOMODBI DD DUMMY).

To create the XCOMODBI data set

1. Copy the sample CBXGSAMP(DSNAOINI) to a desired location and edit it.
2. Code your XCOMODBI statements (as shown in the example above).
3. Add the following statement:

   ```
   //XCOMODBI DD DISP=SHR,DSN=your.hlq.DSNAOINI
   //DSNAOINI DD UNIT=SYSDA,SPACE=(TRK,(1)),DISP=(,DELETE)
   ```

   CA XCOM Data Transport initializes the startup file using the XCOMODBI statements described above.

Note: For a complete description of the contents of this startup file, see the IBM manual DB2 V9.1 for z/OS ODBC Guide and Reference.

Modify JCL for CA XCOM Data Transport

To allow for the writing of history records to an ODBC database, you need to modify the JCL for all of the following:

- The CA XCOM Data Transport started task
- The CA XCOM Data Transport Admin Server
- XCOMJOB batch processing

To modify the JCL

1. Add data sets to //STEPLIB for ODBC processing, as follows:

```
// DD  DISP=SHR,DSN=DB2.DB2910.GA.SDSNEXIT
//*    This data set usually contains the user-defined DSNHDECP module.
// DD  DSN=DB2.DB2910.GA.SDSNLOAD,DISP=SHR contains the DB2/ODBC load modules.
// DD  DSN=CEE.SCEERUN,DISP=SHR
// DD  DSN=CBC.SCLBDLL,DISP=SHR
```

   Note: The SDSNEXIT and SDSNLOAD data sets are installation-dependent, based on the version and maintenance level of DB2 for z/OS. You need to modify the names accordingly.

2. Add DD definitions for ODBC initialization, as follows:

```
//XCOMODBI  DD  DISP=SHR,DSN=XCOM.MODEL.&SYSNAME..DSNAOINI
//* SYSNAME is provided by z/OS when the operator issues a start procedure command.
//* &SYSNAME will only be resolved in the server, as it is valid only for started
tasks.
//* XCOMJOB JCL will require the actual dataset name
//*XCOMODBI  DD  DISP=SHR,DSN=XCOM.MODEL.CA11.DSNAOINI  *For XCOMJOB
// DSNAOINI  DD  UNIT=SYSDA,SPACE=(TRK,(1)),DISP=(,DELETE)
// XCOMHOVR  DD  DISP=SHR,DSN=&PREFIX..XCOMHOVR
//* This sequential data set is used for overflow records when the database is
not available.
//* Refer to CBXGJCL(DEFHOVR) for sample allocation JCL.
```

Changes for ISPF

To allow for the writing of history records to an ODBC database with an immediate execution of file transfers from ISPF (Queue for Execution = N), the CLIST used to invoke the ISPF panel requires additional data set allocations to be included. These data sets are for the DB2 libraries, ODBC initialization, and CA XCOM Data Transport history overflow. The optional global data set, created in CBXGJCL(DEFQSAM) allows this (see the appendix “Sample Files” in the CA XCOM Data Transport for z/OS User Guide).

You need to add the following statements need to be added to the CLIST to allow writing history to the database:

Following the START: label

```
ALLOCATE DD(DSNAOINI) NEW SPACE(1,1) TRACKS DELETE UNIT(SYSDA)
ALLOCATE DD(XCOMODBI) DA(‘your.hlq.DSNAOINI’)SHR
ALLOCATE DD(XCOMHOVR) DA(‘your.hlq.XCOMHOVR’) SHR
ALLOCATE DD(XCOMGLOB) DA(‘your.hlq..XCOMGLOB’) SHR REUSE
ALLOCATE DD(APPTRACE) DUMMY
ALLOCATE DD(DSNTRACE) DUMMY
```

At the end of the CLIST

```
FREE
DD(DSNAOINI,XCOMGLOB,XCOMODBI,XCOMHOVR,APPTRACE,DSNTRACE)
```

You also need to add the following data sets to the STEPLIB:

- DB2.DB2910.GA.SDSNEXIT
- DB2.DB2910.GA.SDSNLOAD

Note: The names of these data sets are installation-specific, based on the version and maintenance level of DB2.

Database Availability

When the DB2 database is unavailable to CA XCOM Data Transport for writing history records. To maintain history data while the database is not available, CA XCOM Data Transport writes information to a sequential overflow data set named XCOMHOVR. The INSERT statements that are executed against the database are written to this file and are used later to update the database when it becomes available.

The data set definition must be present in the JCL when using ODBC history. The DD statement is as follows:

```
//XCOMHOVR DD DISP=SHR,DSN=your.hlq.dataset
```

Sample allocation JCL is provided in CBXGJCL(DEFHOVR) (see the appendix Sample Files in the CA XCOM Data Transport for z/OS User Guide). On startup of CA XCOM Data Transport, a message is issued indicating how many records currently exist in the overflow file, as follows:

```
XCOMM0862I XCOMHOVR contains  1 records at startup
```

This message is also issued for every ten records that are written to the overflow file.

Security

The user ID defined in the Default Options Table with parameter XCOMHIST_USER must be granted use of the history table defined with parameters XCOMHIST_TBL and XCOMHIST_OWNER.

With VSAM history files, each CA XCOM Data Transport server worked with its own history file. However, using a relational database to store CA XCOM Data Transport history records allows multiple CA XCOM Data Transport servers (including CA XCOM Data Transport systems running on Windows and UNIX) to share the database. So you need to be able to restrict access to rows in the database, so that a user on system A is not allowed to see history for system B unless the user is given explicit permission. To provide this level of security, CA XCOM Data Transport Command Security has been enhanced with an additional ALLHIST command resource.

CA XCOM Data Transport implements command security through the parameters OPERSEC and EXIT13, which are coded in the Default Options Table.

If OPERSEC=SAF is coded in the Default Options Table, CA XCOM Data Transport makes a standard SAF call to a security package (CA ACF2, IBM RACF, or CA Top Secret) to determine whether the user has access to the ALLHIST command resource. This resource, when permitted to a user, allows that user to view history records for any system that is maintaining history in that database. If the user is not permitted to this resource then the user is allowed to see history records for the system of the originating request only.

Command: ALLHIST

Access: READ

Resource Name: XCOM.applsec.ALLHIST

applsec

The identifier for the CA XCOM Data Transport server as defined in the Default Options Table, unless it is NONE, in which case the expression XCOM appears in this position. This component of the security call identifies the CA XCOM Data Transport server.

Note: If OPERSEC=NONE is coded in the Default Options Table, CA XCOM Data Transport runs with no security check, giving the user unrestricted access to view history records for any system that is maintaining history in that database.

This level of security is in addition to the current security provided by CA XCOM Data Transport, as documented in the *CA XCOM Data Transport for z/OS Administration Guide*.

Upgrade Existing DB2 History Database

CA XCOM Data Transport r11.6 has added additional fields into the history record. As a result of these new fields, corresponding columns have been added to the history table. This requires that existing users of database history update the history table definition. The DDL is provided in CBXGSAMP(HISTUPD) when you install CA XCOM Data Transport (see the appendix Sample Files in the CA XCOM Data Transport for z/OS User Guide). HISTUPD can be used as input to SPUFI. It will add the new columns to the history table and provide default values for these columns for the existing rows in the table.

Migrate VSAM History to a DB2 Database

You can optionally convert one or more existing VSAM history data sets to a DB2 relational table by using the new CA XCOM Data Transport conversion program XCV2ODBC. Sample JCL is provided in CBXGJCL(XCV2ODBC) when you install CA XCOM Data Transport (see the appendix “Sample Files” in the CA XCOM Data Transport for z/OS User Guide).

Input to XCV2ODBC is a control data set that describes the relational environment. This data set is called SYSIN01.

To define the existing CA XCOM Data Transport history file to convert, use the following format:

```
//XCOMHIST DD disp=shr,dsn=your.vsamfile
```

Input Example:

```
//SYSIN01  DD  *
XCOMHIST=D91APTIB
XCOMHIST_USER=XCOMUSER
XCOMHIST_PASSWORD=SECRET
XCOMHIST_OWNER=MALMA12
XCOMHIST_TBL=XCOM_HISTORY_TBL
SYSNAME=XCOMPM
SYSID=CA11
SSID=D91A
DEBUG=N
```

XCOMHIST=

Specifies the name of the ODBC Data Source location as defined in SYSIBM.LOCATIONS; is analogous to the CA XCOM Data Transport Default Options Table parameter. This parameter is required.

Range: 1 to 128 characters

XCOMHIST_USER=

Names the authorization ID to use when doing the connect. This parameter is required.

Range: 1 to 128 characters

XCOMHIST_PASSWORD=

Is the plain text password of the authorized user. If the XCOMHIST_USER does not require a password, this parameter is specified as a null value (' '). This parameter is required.

Range: 1 to 8 characters

XCOMHIST_OWNER=

(Optional) If XCOMHIST_USERS creates the table, specifies the owner of the table and can be omitted. If not specified XCOMHIST_USER is used as the table owner.

Range: 1 to 128 characters

XCOMHIST_TBL=

Specifies the 1 through 128-character table name to insert rows in. This parameter is required.

SYSNAME= / SYSID=

If the existing history record does not contain that information, specifies the system name and SMFID used. If you are converting a CA XCOM Data Transport r11 VSAM history database, this information is not present. Identifies the CA XCOM Data Transport server from which this data originated.

SYSNAME (one to eight characters) is generally the name of the CA XCOM Data Transport started task.

SYSID is the four-character SMFID on the system that the CA XCOM Data Transport started task runs on.

These parameters are required.

SSID=

Specifies the DB2 subsystem ID used at connect time.

This parameter is optional but is required for remote database connections.

DEBUG=

(Optional) Specifies whether to collect trace information for CA Technologies Technical Support.

Range: Y or N

Note: Y is specified only when CA Technologies Technical Support directs.

SYSNAME/SYSID Example 1:

The CA XCOM Data Transport started task XCOMPM is started on system CA11. When converting the history file this task writes, specify the following values:

```
SYSNAME=XCOMPM
SYSID=CA11
```

Any existing VSAM record not containing values for SYSNAME and SYSID uses these specifications when inserting the row into the relational database.

SYSNAME/SYSID Example 2:

The CA XCOM Data Transport started task XCOMDMP is started on system CA31. When converting the history file this task writes, specify the following values:

```
SYSNAME=XCOMDMP
```

```
SYSID=CA31
```

Any existing VSAM record not containing values for SYSNAME and SYSID uses the above specifications when inserting the row into the relational database.

Note: You can convert one or more VSAM history files to the same relational table. Run the job for each VSAM history file that is converted, modifying the XCOMHIST DD statement to reflect the appropriate file.

//STEPLIB DD

//STEPLIB DD should contain the following:

```
//STEPLIB  DD  DISP=SHR,DSN=your.XCOM.load.library
//         DD  DISP=SHR,DSN=D91A.PRIVATE.SDSNEXIT  (CA11)
//         DD  DSN=DB2.DB2910.GA.SDSNEXIT,DISP=SHR
//         DD  DSN=DB2.DB2910.GA.SDSNLOAD,DISP=SHR
//         DD  DSN=CEE.SCEERUN,DISP=SHR
//         DD  DSN=CBC.SCLBDLL,DISP=SHR
//SYSPRINT DD SYSOUT=*
```

Note: The SDSNEXIT and SDSNLOAD data sets are installation dependent, based on the version and maintenance level of DB2. You need to modify the names accordingly.

Define the Optional Sequential Files

At the user's option, two sequential data sets, XCOMGLOB and XCOMREST (described below), can be used by the batch interface for non queued (TYPE=EXECUTE) file transfers:

XCOMGLOB

XCOMGLOB is a global data set used by all non queued transfers. It contains a number to be assigned to the next transfer request. If this data set is not used, CA XCOM Data Transport assigns request number 2000 to all non-queued transfers

XCOMREST

The XCOMREST data sets are unique for each batch job. They are used to save checkpoint information for non-queued transfers

The member DEFQSAM in *yourhlq*.CBXGJCL provides an example of the definition and initialization of these data sets (see the appendix “Sample Files” in the *CA XCOM Data Transport for z/OS User Guide*).

Note: Attempting to use an XCOMGLOB, XCOMREST, or XCOMINQ data set from a prior release of CA XCOM Data Transport can result in abnormal terminations of the XCOMJOB utility, or other unpredictable and undesirable results.

Chapter 8: Migration Information

This section contains the following topics:

Migration Considerations

We recommend that your site use a different CSI and zones for installation of CA XCOM Data Transport release 11.6. Release 11.5 and release 11.6 cannot co-exist in the same CSI even though the module names are the same for most of the modules. The release 11.6 functions (FMIDs) include deletes for the release 11.5 functions, so with both versions in the same CSI, it would not be possible to apply maintenance to release 11.5.

Library Name Changes

Important! The names of our SMP/E target libraries have changed. The following table provides a cross reference of the old names to their new counterparts:

Old Name	New Name	Comments
CAILIB	CBXGLOAD	(Base Product)
CAILIB	CBYCLOAD	(CICS Interface)
CINB5MAC	CBXGMAC	
CINB5SPL	CBXGPNL0	
CINB5SPJ	CBXPPJPN	
CINB5SCL	CBXGCLS0	
CINB5SML	CBXGMSG0	
CINB5TBL	CBXGTBL0	
CINB5SAM	CBXGJCL	
CINB5CTL	CBXGPARM	

Update CSD Definitions

Sample member XCOMCSD contains the CSD definitions necessary to add the CA XCOM Data Transport TCT entries. XCOMCSD is provided in the library yourhlq.CBXGJCL and appendix Sample Files in the CA XCOM Data Transport for z/OS User Guide.

You can change the following parameters before assembling the TCT:

- NETNAME to point to the CA XCOM Data Transport server
- SYSIDNT to point to any valid Term ID
- MODENAM to point to a valid CA XCOM Data Transport mode name

You can add as many CA XCOM Data Transport TCT entries as you want. Typically, you define one TCT entry for each CA XCOM Data Transport server with which you want to communicate.

Example:

You can define TCT entries for the New York Production CA XCOM Data Transport, the New York VM CA XCOM Data Transport, the Chicago CA XCOM Data Transport, the Tokyo CA XCOM Data Transport, and so on.

Default Options Table

There are new parameters for the CA XCOM Data Transport default options table for Release 11.6. As the default options table is being deprecated this release, the configuration member must be used in order to specify any new parameter added for release 11.6. An existing default options table will automatically be converted to a configuration member in the XCOMCNTL dataset upon first use by an XCOM Server or Job.

XCOMRRDS

The use of the IBM LSR (Local Shared Resources) for the XCOMRRDS is supported for Release 11.6. You must create a new RRDS for Release 11.6. Using this facility increases performance when queuing and processing transfer requests; however, using LSR for the RRDS is optional. This feature is activated by making modifications to the CA XCOM Data Transport server JCL. The IBM BLSR region must also be started.

If you are using LSR for the XCOMRRDS, it is important to consider how to configure the DEFERW parameter. This parameter indicates whether VSAM deferred write (DFR) is to be used for the XCOMRRDS. Setting this parameter to NO causes data to be written to disk, ensuring that transfer information is not lost if an abnormal termination occurs. However, setting this parameter to NO also decreases performance, because data is written to disk instead of to memory. Setting DEFERW to YES improves performance, but if an abnormal termination occurs with this parameter set to YES, data that is written to memory is lost because it is not written out to the XCOMRRDS data set.

Note: LSR is recommended only for installations with very high volumes of scheduled transfers that are being run concurrently. For more information, see the chapter "Configuring and Customizing Your Product" in the *CA XCOM Data Transport for z/OS Administration Guide*.

History File

Modifications to the format of the VSAM history file cluster have been implemented for Release 11.6. The modifications require either defining a new VSAM history file cluster or migrating an existing one. The XCOMUTIL History File utility has been modified to perform a conversion of an existing release 11.5 VSAM history file cluster to the new 11.6 format. For more details, refer to the CA XCOM Data Transport for z/OS User Guide for the description of the XCOMUTIL utility. The format changes implemented for release 11.6 are as follows:

- The maximum length of the history record has been increased to 3030 bytes from 2020-in previous releases to allow for recording of additional transfer information.
- The alternate indexes have been made unique and use the same date and time values as are in the primary key to enforce the uniqueness.
- A new unique alternate index based on the TCP/IP name has been added.

XCOMGLOB and XCOMREST

XCOMGLOB

An existing XCOMGLOB data set from Release 11.5 may be used with Release 11.6.

XCOMREST

A new XCOMREST restart data set needs to be created when used in Release 11.6 due to the change in the record length for the XCOMRRDS file.

If you attempt to initiate a TYPE=EXECUTE file transfer, when a new XCOMREST is not recreated after upgrading to Release 11.6, the file transfer fails, with an error 0219E.

You need to use the DEFQSAM sample JCL to create the new XCOMREST to ensure that the correct LRECL is used. For Release 11.6, the LRECL and BLKSIZE for the Restart data set have changed to 3030.

Configuration

There is a Server Storage Usage Worksheet for Release 11.6 available on the CA XCOM Data Transport web pages for the z/OS platform at http://ca.com/support. Filling out this worksheet allows you to calculate the approximate storage usage required for CA XCOM Data Transport Release 11.6.

Appendix A: Japanese ISPF Panel Support

CA XCOM Data Transport distributes a version of the ISPF Panels in Japanese as part of the base product. The following shows how to make those panels accessible to an ISPF terminal session.

This section contains the following topics:

Customize the ISPF Dialogs (see page 199)

Customize the ISPF Dialogs

The CBXGPJPN target library needs to be added to your ISPF proc:

```
//ISPPLIB DD       DSN=
//                 DD  DSN=CAI.CBXGPJPN,DISP=SHR
//                 DD  DSN=CAI.CBXGPNL0,DISP=SHR
```

Index

/

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

X

Z