CA Deliver™

Installation Guide

Release 12.2

CA Technologies Product References

This document references the following CA Technologies products:

- CA 11®
- CA ACF2™
- CA Common Services
- CA Roscoe®
- CA Top Secret® for z/OS
- CA View™

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 section contains the following topics:

Audience

This guide is targeted to the systems programmer who installs, uses, and maintains CA Deliver.

This guide assumes you are familiar with CA Deliver, CA View, and IBM computer system terms and concepts. You should also have a working knowledge of MVS online facilities such as ISPF, because the CA Deliver panels behave in a similar fashion.

How the Installation Process Works

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

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

CA Chorus™ Software Manager (CA CSM) - formerly known as CA Mainframe Software Manager™ (CA MSM) - is an intuitive web-based tool that can automate and simplify many CA Technologies product installation activities on z/OS systems. This application also makes obtaining and applying corrective and recommended maintenance easier. A web-based interface enables you to install and maintain your products faster and with less chance of error. As a best practice, we recommend that you install mainframe products and maintenance using CA CSM. Using CA CSM, someone with limited knowledge of JCL and SMP/E can install a product.

Note: If you do not have CA CSM, you can download it from the Download Center at http://ca.com/support. Follow the installation instructions in the CA Chorus Software Manager documentation bookshelf on the CA Chorus Software Manager product page.

You can also complete the standardized installation process manually using pax files that are downloaded from http://ca.com/support or a product DVD.

To install your product, do the following tasks:

1. Prepare for the installation by confirming that your site meets all installation requirements.
2. Verify that you acquired the product using one of the following methods:
   - Download the software from http://ca.com/support using CA CSM.
   - Download the software from http://ca.com/support using Pax-Enhanced Electronic Software Delivery (Pax ESD).
   - Order a product DVD. To do so, contact your account manager or a CA Technologies Support representative.
3. Perform an SMP/E installation using one of the following methods:
   - If you used CA CSM to acquire the product, start the installation process from the SMP/E Environments tab in CA CSM.
   - If you used Pax ESD to acquire the product, you can install the product in the following ways:
     - Install the product manually.
     - Complete the SMP/E installation using the Add Product option in CA CSM.
   - If you used a DVD, install the product manually.

   Note: If a CA Recommended Service (CA RS) package is published for your product, install it before continuing with deployment.
4. Deploy the target libraries using one of the following methods:
   - If you are using CA CSM to configure your products, a CA CSM deployment is required.
   - If you are using a manual configuration process, a manual deployment is an optional step.

   Note: Deployment is considered part of starting your product.
5. Configure your product using CA CSM or manually.

   Note: Configuration is considered part of starting your product.

Installation Considerations

Before you begin the installation, you must prepare your system, assemble your materials, and then follow the installation steps exactly and in order. Use this list as a guide for the installation process.

1. Be certain that CA Common Services are installed on your system, and that the required hardware, software, and libraries are prepared.

   CA Deliver uses the CAI Resource Initialization Manager CAIRIM portion of the CA Common Services. CAIRIM prepares the operating system for CA products and components, and then executes them.

   CA DRAS requires the CAIENF (Event Notification Facility) and the CAICCI (Common Communications Interface) components of the CA Common Services.

   Note: For more information about system requirements, see the chapter "System Requirements".

2. Install CA Deliver using one of these methods:
   - CA CSM
   - PAX Enhanced ESD
   - Product DVD installation
3. Use options and initialization parameters to customize CA Deliver according to the needs of your site, as follows:
   - Configure your CA Deliver system.
   - Install the online interfaces including the cross-memory and online retrieval options for ISPF, TSO, VTAM, CA Roscoe Interactive Environment (CA Roscoe), CICS and IMS.
   - Install the features

More information:

Installing Online Interfaces (see page 97)
Installing the Features (see page 189)

First Time Installation or Upgrade

Use the tasks presented in this chapter, and in the Installing Online Interfaces and Installing Features sections of the "Configuring Your Product" chapter. These tasks are valid whether you are installing CA Deliver Release 12.2 for the first time or upgrading from a previous release, as follows:

- If you are installing for the first time, perform:

  All steps in this chapter as indicated, and the tasks in the Installing Online Interfaces and Installing Features chapters to install the optional online interfaces and features appropriate for your site.

- If you are upgrading from a previous release, perform:

  All steps as indicated and the tasks in the "Configuring Your Product," "Installing Online Interfaces" and "Installing Features" chapters as appropriate for your site. Some steps must be performed exactly as presented; several steps must be modified according to the instructions in the Upgrading from a Previous Release section.

Important! *Be sure that you retain your previous CA Deliver JCL files and load libraries*.

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

Use the tables in this section to estimate the storage required for the target libraries, the distribution libraries, and the EBC (Extended Base Component) libraries.

Supported Operating Systems

IBM z/OS 1.9 and higher is the minimum software required to run this release of CA Deliver and meet the performance requirements.

CA Deliver Target Libraries

This table lists the amount of disk space needed to install the target libraries.

Library Name	Blksize	Tracks	Dir Blks	Description
CAI.CVDEJCL	27920	87	51	Common JCL library
CAI.CVDELOAD	32760	141	83	Common load library
CAI.CVDEPROC	27920	39	24	Common procedure library
CAI.CVDEOPTN	27920	45	24	Common options library
CAI.CVDESRC	27920	44	24	Common source library
CAI.CVDEMAC	27920	66	33	Common macro library

Library Name	Blksize	Tracks	Dir Blks	Description
CAI.CVDECLS0	27920	20	12	Common CLIST library
CAI.CVDEPNL0	27920	39	24	Common ISPF panels library
CAI.CVDETBL0	27920	20	12	Common ISPF table library
CAI.CVDEPENU	27920	120	400	Common online panels (English)
CAI.CVDED133	32718	29	12	Deliver model banner page library
CAI.CVDEXML	32760	196	24	CA CSM Deployment and Configuration Services

Important! Do not reblock the libraries listed previously—storage problems might occur.

CA Deliver Distribution Libraries

This table lists the amount of disk space needed to install the distribution libraries.

Library Name	Blksize	Tracks	Dir Blks	Description
CAI.ABRNJCL	27920	87	51	JCL library
CAI.ABRNMOD	32760	83	112	Load library
CAI.ABRNPROC	27920	39	24	Procedure library
CAI.ABRNOPTN	27920	45	24	Options library
CAI.ABRNSRC	27920	34	24	Source library
CAI.ABRNMAC	27920	66	33	Macro library
CAI.ABRNCLS0	27920	20	12	CLIST library
CAI.ABRNPNL0	27920	39	24	ISPF panels library
CAI.ABRNTBL0	27920	20	12	ISPF table library
CAI.ABRNPENU	27920	311	217	Online panels (English)
CAI.ABRNDATA	32718	29	12	Model banner page library
CAI.ABRNXML	32760	196	24	CA CSM Deployment and Configuration Services

EBC Distribution Libraries

This table lists the amount of disk space needed to install the EBC distribution libraries.

Library Name	Blksize	Tracks	Dir Blks	Description
CAI.ABROMOD	32760	41	68	Load library
CAI.ABROPROC	27920	39	24	Procedure library
CAI.ABROOPTN	27920	45	24	Options library
CAI.ABROSRC	27920	44	24	Source library
CAI.ABROMAC	27920	66	33	Macro library
CAI.ABROPNL0	27920	39	24	ISPF panels library
CAI.ABROJCL	27920	87	51	JCL library
CAI.ABROXML	32760	196	24	CA CSM Deployment and Configuration Services

Software Requirements

This section lists the CA Deliver Release 12.2 component SYSMODs.

Common Component SYSMODs

The CBROC20 SYSMOD is the EBC common component.

Note: The optional EBC CICS FMID has been incorporated into the EBC common component FMID in Release 12.2.

CA Deliver Components

CBRNC20 is the CA Deliver base product component.

CA Common Services Component

The CAIRIM component supports CA LMP.

CA Common Services Requirements

We recommend that you maintain CA Common Services at a current maintenance level to ensure compatibility. For the latest information about maintenance requirements, go to CA Support Online.

Note: If you intend to use CA CSM for your installation and maintenance tasks, there might be additional CA Common Service requirements. For more information, see the Software Requirements section in the *CA Chorus™ Software Manager Product documentation*.

These CA Common Services are used with CA Deliver:

- CAICCI
- CAIRIM
- CA LMP
- CAISDI Service
- CA Health Checker Common Service

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

CA Common Services Installation Considerations

Before you proceed with this installation, be certain that CA Common Services are installed on your machine.

Note: For more information, see the *CA Common Services Getting Started Guide*.

CAIRIM

CAIRIM (CAI Resource Initialization Manager) is the common driver for a collection of dynamic initialization routines that eliminate the need for user SVCs, SMF exits, subsystems, and other installation requirements that are commonly encountered when you install systems software. CAIRIM prepares the operating system for CA products and components, then executes them.

CAIRIM does the following:

- Obtains SMF data
- Verifies proper software installation
- Installs MVS interfaces

- Starts CA and other vendor's products automatically
- Provides proper timing and order of initialization

Note: CA Deliver requires CAIRIM to run the required CA LMP.

CA LMP

The CA License Management Program (CA LMP) tracks licensed software in a standardized and automated way. It uses common, real-time enforcement software to validate the user's configuration. CA LMP reports on activities related to the license, usage, and financials of CA Technologies products.

CA LMP features include the following:

- A Common Key Data Set that can be shared among many CPUs.
- Check digits that are used to detect errors in transcribing key information.
- Execution keys that can be entered without affecting any CA Technologies software products that are already running.
- No special maintenance is required.

CA Deliver is licensed with an LMP key. Acquire the LMP key using one of these methods:

- From your product media
- With ESD
- From CA Support

Library Authorization

CA Deliver and the EBC subsystem contain authorized programs. To run successfully, these programs must be executed from an authorized library. We recommend that you authorize the CAI Common Load Library (CVDELOAD).

Note: If other CA products have been installed, CVDELOAD may already be authorized.

To authorize the CVDELOAD library, modify the appropriate member PROG*xx* in SYS1.PARMLIB to add an entry for CVDELOAD as follows:

```
APF ADD DSNAME(CAI.CVDELOAD) VOLUME(xxxxxx)
```

where CAI.CVDELOAD is the data set name for the CAI Common Load Library, and *xxxxxx* is the volume serial number on which it resides. Use MVS system command SET PROG=xx to activate update to PROGxx.

Security Requirements

For security requirements related to the ability to access data within the CA Deliver database, see the "Security" chapter in the CA Deliver Reference Guide.

Storage Requirements

Ensure that you have the following storage available:

- If you are installing with ESD, 80 cylinders for the downloaded files.
- For installation and setup:
  - Installation = 100 cylinders
  - SMP/E temporary libraries = 10 cylinders]

USS Space Requirements

Ensure that you have sufficient free space in the USS file system that you are using for Pax ESD to hold the directory that the pax command and its contents create. You need approximately 3.5 times the pax file size in free space.

If you do not have sufficient free space, you receive error message EDC5133I.

Other Requirements

This section describes SVC Dumps and JCL procedures:

SVC Dump Data Sets

CA Deliver issues SVC dumps (SDUMP) for certain types of abends. These dumps are written to the MVS SYS1.DUMP*nn*. data sets. Contact your systems programmer to verify that the data sets are allocated with at least 100 cylinders.

Dump Analysis and Elimination

The SDUMP program supports MVS dump analysis and elimination processing. This MVS feature eliminates the possibility that duplicate SVC dumps might be written to the SYS1.DUMP*nn*. data sets.

To use this MVS feature, the SYS1.DAE data set must be allocated and the following parameter members must be updated in SYS1.PARMLIB:

IEACMD*xx*
SET DAE = *xx*

where *xx* identifies the ADYSET*xx*. member

ADYSET*xx*
DAE=START,RECORDS(*sss*),SVCDUMP(MATCH,UPDATE,SUPPRESS)

where *sss* is the number of records in SYS1.DAE.

System Dump Parameters

CA Deliver allocates storage from MVS subpool 230.

For this storage area to be dumped correctly, the IEADMR*xx*. member in SYS1.PARMLIB should contain the SDATA RGN parameter:

SDATA=(...,RGN,...)

The IEADMP*xx*. member in SYS1.PARMLIB should contain the SDATA LSQA parameter:

SDATA=(...,LSQA,...)

Important! If these dump parameters are not specified as shown in the previous example, certain storage areas might be missing from dumps, which can hinder support efforts.

JCL Procedures

During product installation, the procedures are copied into CVDEPROC, the CA Deliver Procedure Library. These procedures are used later during normal execution of CA Deliver.

We recommend that you add the CVDEPROC library to the system PROCLIB concatenation.

Concurrent Releases

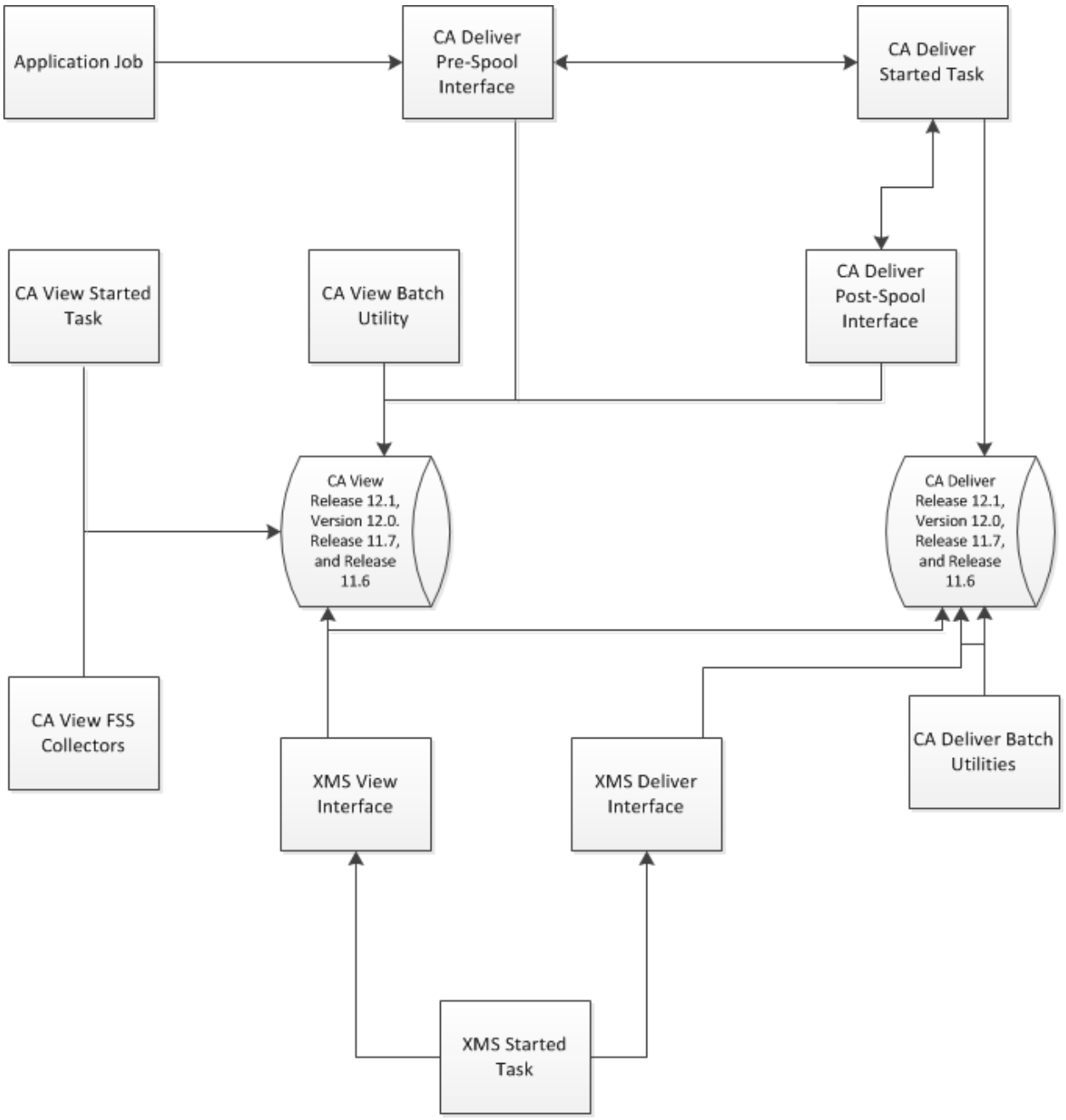
You can install this release of your product and continue to use an older release in another SMP/E environment. If you plan to continue to run a previous release, consider the following points:

- When you install the product into an existing SMP/E environment, this installation deletes previous releases in that environment.
- If you acquired your product with Pax 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 CSM installs a product into a new SMP/E environment by default. You can select an existing SMP/E environment from your working set. For more information, see the online help that is included in CA CSM.
- 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.

Relationship between Versions of CA View and CA Deliver

The following diagram shows the relationship between multiple versions of CA View and CA Deliver:



Chapter 3: Installing Your Product Using CA CSM

How to Install Your Product Using CA CSM

As a system programmer, your responsibilities include acquiring, installing, maintaining, deploying, and configuring CA Technologies mainframe products on your system.

CA CSM is an application that simplifies and unifies the management of your CA Technologies mainframe products on z/OS systems. As products adopt the CA CSM services, you can install your products in a common way according to industry best practices.

This scenario describes the steps for a system programmer to acquire, install, deploy, and configure products and maintenance. Not all tasks may apply to your organization. For example, you may decide not to deploy and configure products. In this case, do not perform the product deployment task and the product configuration task.

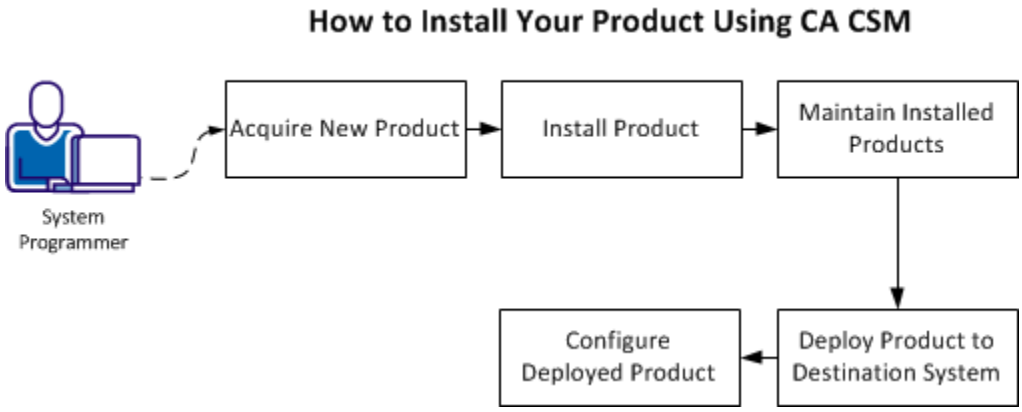
Before you use this scenario, you must have CA CSM installed at your site. If you do not have CA CSM installed, you can download it from the Download Center at http://ca.com/support. This web page also contains links to the complete documentation for CA CSM.

You access CA CSM (see page 24) from a web browser.

Note: This scenario applies to the latest version of CA CSM. If you are using an earlier version, see the appropriate bookshelf on the CA Chorus Software Manager product page.

This scenario is a high-level overview of steps that you perform using CA CSM. For more detailed information, use the online help that is included in CA CSM.

You perform the following tasks to install products and manage them on your system:



1. Acquire a new product (see page 25).
2. Install the product (see page 26).
3. Maintain the installed products (see page 28).
4. Deploy the product to the destination system (see page 29).
5. Configure the deployed product (see page 30).

Access CA CSM Using the Web-Based Interface

You access CA CSM using the web-based interface.

You need the URL of CA CSM from the CA CSM 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.

   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.

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

   You are prompted to review your user settings.

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

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

   A dialog opens, which 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.

Acquire a New Product

Acquisition allows you to download products and product maintenance from the CA Support Online website at http://ca.com/support to a USS directory structure on your system. The products to which your site is entitled and the releases available are displayed in the Available Products section on the Products page.

You perform the following high-level tasks to acquire a product using CA CSM:

1. Set up a CA Support Online account at http://ca.com/support.

   To use CA CSM to acquire or download a product, you must have a CA Support Online account. If you do not have an account, create one on http://ca.com/support.

2. Determine the CA CSM URL for your site.

   To access CA CSM (see page 24), you require its URL. You can get the URL from your site CA CSM administrator and log in using your z/OS credentials. When you log in for the first time, you are prompted to create a CA CSM account with your credentials that you use to access http://ca.com/support. This account enables you to download product packages.

3. Log in to CA CSM and go to the Products page to locate the product that you want to acquire.

   After you log in to CA CSM, you can see the products to which your organization is entitled on the Products tab.

   If you cannot find the product that you want to acquire, update the product list. CA CSM refreshes the product list through http://ca.com/support using the site IDs associated with your credentials.

4. Download the product installation packages.

   After you find your product in the product list, you can download the product installation packages. To do so, use the Update Product Release action.

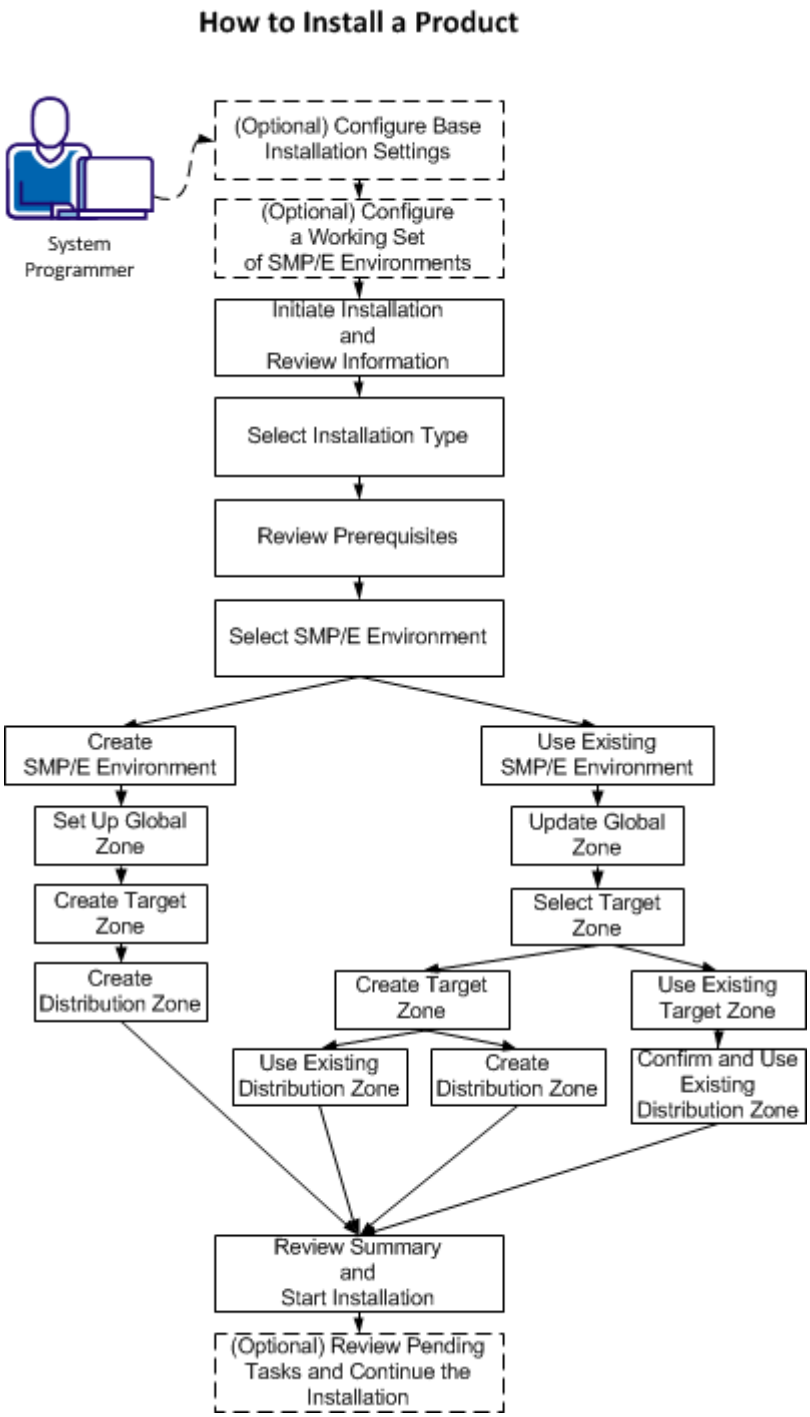
   CA CSM downloads (acquires) the packages (including any maintenance packages) from the CA Support Online website.

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

Install a Product

CA CSM simplifies and manages SMP/E installation tasks. You can browse and install a product that you acquired and that is available in the product list on the Products page. You can also install the maintenance for the products that are currently installed in a managed SMP/E environment on the driving system.

You perform the following high-level tasks to install a product using CA CSM:



1. (Optional) On the Settings tab, click Software Installation under System Settings, and configure base installation settings.
2. (Optional) Click the SMP/E Environments tab, and configure a working set of SMP/E environments.
3. Click the Products tab and select a product that you want to install. Start the installation wizard and review product information.
4. Select an installation type.
5. Review installation prerequisites if any are presented.
6. Take *one* of the following steps to select an SMP/E environment:
   - Create an SMP/E environment:
     a. Set up the global zone.
     b. Create a target zone.
     c. Create a distribution zone.
   - Use an existing SMP/E environment from your working set:
     a. Update the global zone.
     b. Set up the target zone: Create a target zone or use an existing target zone.
     c. Set up the distribution zone: Create a distribution zone or use an existing distribution zone.

     Note: If you install a product or its components into an existing target or distribution zone, older versions are *deleted* from the zone and associated data sets. We recommend that you use new target and distribution zones for this installation so that you can apply maintenance to your current version, if necessary.
7. Review the installation summary and start the installation.
8. (Optional) Review pending tasks for the SMP/E environment where you are installing your product. Continue the installation, if applicable.

   CA CSM installs the product.

After the installation process completes, check for and install available product maintenance. The product is ready for you to deploy. Sometimes, there are other steps to perform manually outside of CA CSM before continuing.

Maintain the Installed Products

You can migrate existing SMP/E environments into CA CSM to maintain all your installed products in a unified way from a single web-based interface.

You can use CA CSM to maintain a CA Technologies product.

You perform the following high-level tasks to maintain a product using CA CSM:

1. Verify that CA CSM recognizes the SMP/E environment where your product is installed. If not, migrate the SMP/E environment to CA CSM.

   During the migration, CA CSM stores information about the SMP/E environment in the database.

2. From the Product tab, download the latest maintenance for the installed product releases.

   If you cannot find the required release, perform the following steps to download the maintenance:

   a. Add the release to the catalog manually.

   b. Update the added release.

3. Apply the maintenance.

   CA CSM applies the maintenance to your product.

After the maintenance process completes, the product is ready for you to deploy to systems that are defined in the system registry.

Deploy the Product to the Destination System

Deployment is a process of copying SMP/E target libraries to a destination system. The destination system could be the local z/OS system, a remote z/OS system, or a sysplex. You identify the destination system, deployed data set names, and the transport mechanism as part of the deployment process. Deploying a product makes it available for configuration.

Important! Before you deploy a product, set up the destination systems and remote credentials in the system registry.

You perform the following high-level tasks to deploy your products using CA CSM:

1. On the Deployments tab, set up methodologies.

   Note: You can also set up methodologies when creating a deployment, or use existing methodologies, if you have set up any previously. If you do so, you can skip this step.

2. Start the New Deployment wizard to create a deployment. Complete each of the steps in the wizard. The wizard guides you through choosing deployment settings for your site. At any point, you can save your work and come back to it later.

3. Deploy:
   a. Take a snapshot of the deployment.
   b. Transmit the deployment to a destination system.
   c. Deploy (unpack) to the mainframe environment.

   CA CSM deploys the product to the destination system.

After the deployment process completes, the product is ready for you to configure.

Configure the Deployed Product

Configuration is a process of copying the deployed libraries to run-time libraries and customizes the product for your site to bring it to an executable state. You can configure CA Technologies products that you have already acquired, installed, and deployed using CA CSM. You cannot use CA CSM to configure a product unless you have already used CA CSM to deploy the product.

You perform the following high-level tasks to configure your products using CA CSM:

1. Select a configurable deployment on the Deployments tab to view details and products for that deployment.
2. Select a product in the deployment and start the Configuration wizard to create a configuration. Complete each of the steps in the wizard. The wizard has multiple levels of detailed instructions and guides you through choosing configuration settings for your site. At any point, you can save your work and come back to it later. Configurations where you have partially completed the steps in the wizard are listed on the Configurations tab. The steps in the wizard include the following:
   a. Define a configuration name and select a system for the configuration.
   b. Select configuration functions and options.
   c. Define system preferences.
   d. Create target settings.
   e. Select and edit resources.
3. Build the configuration. The last step of the Configuration wizard lets you build the configuration. If needed, you can edit the configuration and can build the configuration again. Building the configuration closes the wizard and creates a configuration with all your settings.
4. (Optional) Validate the configuration. Validation verifies access to resources that are going to be used when you implement the configuration.

5. Implement the configuration. You implement a configuration to make your deployed software fully functional. Implementation executes on the destination system, applying the variables, resources, and operations that are defined in the configuration.

   CA CSM configures the product.

After the configuration process completes, the product is ready for you to use.

Chapter 4: Installing Your Product Using Pax ESD or DVD

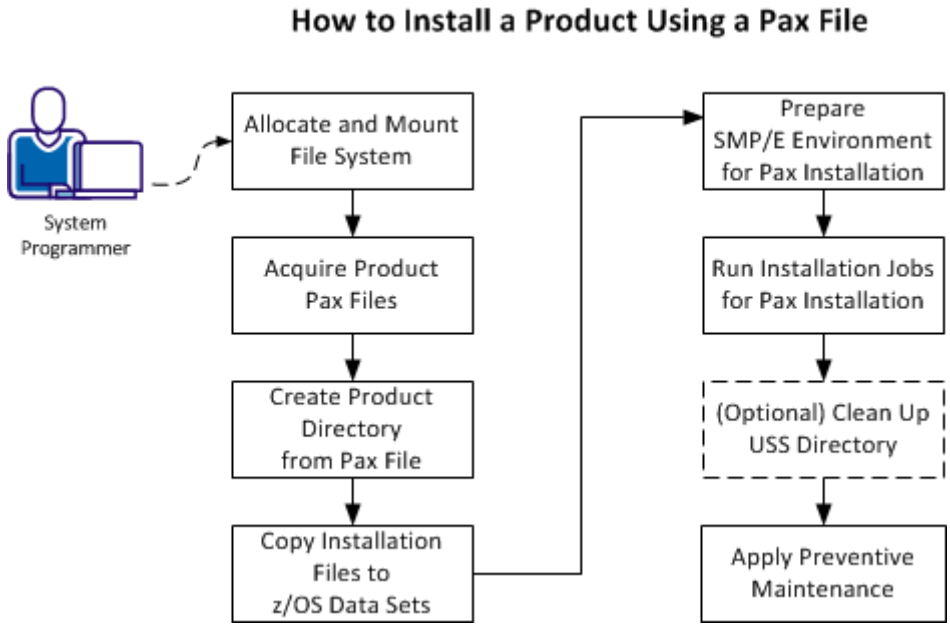
This section contains the following topics:

How to Install Your Product Using a Pax File

As a system programmer, your responsibilities include installing products on your mainframe system. With this option, you acquire a product pax file from http://ca.com/support or from a product DVD.

The DVD contains a folder that includes the pax file for the product. Product updates may have occurred after you acquired the product DVD. The files on the online site always have the most current product updates. To determine if you have the latest updates, go to http://ca.com/support and click Download Center.

You perform the following tasks to install a product with a pax file:



1. Allocate and mount the file system (see page 35).
2. Acquire the product pax files (see page 37).
3. Create a product directory from the pax file (see page 43).
4. Copy the installation files to z/OS data sets (see page 44).
5. Prepare the SMP/E environment for a pax installation.
6. Run the installation jobs for a pax installation.
7. (Optional) Clean up the USS directory (see page 49).
8. Apply preventive maintenance (see page 50).

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 http://ca.com/support.
- Perform utility functions to unpack the pax file into MVS data sets that you can use to complete the product installation.

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

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

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

Important! Downloading pax files for the SMP/E installation as part of the Pax ESD process requires write authority to the UNIX System Services (USS) directories that are used for the Pax ESD process. In the file system that contains the Pax 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 Pax ESD directory.

Allocate and Mount a File System

The product installation process requires a USS directory to receive the pax file and to perform the unpack steps. We recommend that you allocate and mount a file system that is dedicated to the product acquisition and create the directory in this file system.

You can use the zSeries File System (zFS) or hierarchical file system (HFS) for product downloads.

This procedure describes how to perform the following tasks:

- Allocate a zFS or an HFS.
- Create a mount point in an existing maintenance USS directory of your choice.
- Mount the file system on the newly created mount point.

  Note: You must have either SUPERUSER authority, or the required SAF profile setting to allow you to issue the USS mount command for the file system.
- Optionally, permit write access to anyone in the same group as the person who created the directory.

  Important! USS commands are case-sensitive.

Follow these steps:

1. Allocate the file system by customizing one of the following samples to your site requirements:

   - On a zFS, use the following sample:

```
//DEFINE   EXEC PGM=IDCAMS
//SYSPRINT DD   SYSOUT=*
//SYSUDUMP DD   SYSOUT=*
//AMSDUMP  DD   SYSOUT=*
//SYSIN    DD *
  DEFINE CLUSTER ( +
  NAME(your_zFS_data_set_name) +
  STORAGECLASS(class) +
  LINEAR +
  CYL(primary secondary) +
  SHAREOPTIONS(3,3) +
  )
/*
//FORMAT   EXEC PGM=IOEAGFMT,REGION=0M,
// PARM=('-aggregate your_zFS_data_set_name -compat')
//SYSPRINT DD   SYSOUT=*
//SYSUDUMP DD   SYSOUT=*
//STDOUT   DD   SYSOUT=*
//STDERR   DD   SYSOUT=*
//CEEDUMP  DD   SYSOUT=*
//*
```

   - On an HFS, use the following sample:

```
//ALCHFS EXEC PGM=IEFBR14
//CAPAX  DD   DSN=yourHFS_data_set_name,
//            DISP=(NEW,CATLG,DELETE),UNIT=3390,
//            DSNTYPE=HFS,SPACE=(CYL,(primary,secondary,1))
```

   The file system is allocated.

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

2. Create a mount point for the file system. This example shows how to create a /CA/CAPAX directory in an existing directory, /u/maint. From the TSO OMVS shell, enter the following commands:

   ```
   cd /u/maint/
   mkdir CA
   cd CA
   mkdir CAPAX
   ```

   Note: This document refers to this structure as *yourUSSpaxdirectory*.

   The mount point is created.

3. Mount the file system by customizing one of the following samples to your site requirements:

   - On a zFS, use the following sample:

     ```
     MOUNT FILESYSTEM('your_zFS_data_set_name')
           MOUNTPOINT('yourUSSpaxdirectory')
           TYPE(ZFS)  MODE(RDWR)
           PARM(AGGRGROW)
     ```

   - On an HFS, use the following sample:

     ```
     MOUNT FILESYSTEM('your_HFS_data_set_name')
           MOUNTPOINT('yourUSSpaxdirectory')
           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 Pax ESD directory and its files. For example, to allow write access to the Pax ESD directory for other users in your USS group, from the TSO OMVS shell, enter the following command:

   ```
   chmod -R 775 /yourUSSpaxdirectory/
   ```

   Write access is granted.

   Note: For more information about the chmod command, see the IBM *z/OS UNIX System Services User Guide* (SA22-7802).

Acquire the Product Pax Files

To begin the CA Technologies product installation procedure, copy the product pax file into the USS directory that you set up.

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

Use one of the following methods:

- Download the product pax file from http://ca.com/support to your PC (see page 38), and then upload it to your USS file system.

  If you download a zip file, you must unzip it before uploading to your USS file system.

- Download the pax files from http://ca.com/support directly to your USS file system (see page 39).

- Download the pax file from the product DVD to your PC, and then upload the pax files to your USS file system. (see page 42)

This section includes the following information:

- 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
- 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 that you are using 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.

Download Files to a PC Using Pax ESD

You can download product installation files from http://ca.com/support to your PC.

Follow these steps:

1. Log in to http://ca.com/support, and click Download Center.

   The Download Center web page appears.

2. Under Download Center, select Products from the first drop-down list, and specify the product, release, and gen level (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. If you download a zip file, you must unzip it before continuing.

   Note: For traditional installation downloads, see the *Traditional ESD User Guide*. For information about download methods, see the Download Methods and Locations article. Go to http://ca.com/support, log in, and click Download Center. Links to the guide and the article appear under the Download Help heading.

Download Using Batch JCL

You download a pax file from http://ca.com/support by running batch JCL on the mainframe. Use the sample JCL attached to the PDF file as CAtoMainframe.txt (see page 41) to perform the download.

Important! The PDF version of this guide includes sample JCL jobs that you can copy directly to the mainframe. To access these jobs, click the paper clip icon at the left of the PDF reader. A window displaying attachments opens. Double-click a file to view a sample JCL. We recommend that you use the latest version of Adobe Reader for viewing PDF files.

Note: We recommend that you follow the preferred download method as described on http://ca.com/support. This JCL procedure is our preferred download method for users who do not use CA CSM. We also include the procedure to download to the mainframe through a PC in the next section.

Follow these steps:

1. Replace *ACCOUNTNO* with 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 *yourUSSpaxdirectory* with the name of the USS directory that you use for Pax 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 PAX ESD PACKAGE',
//          MSGCLASS=X,CLASS=A,NOTIFY=&SYSUID
//*********************************************************************
//* This sample job can be used to download a pax file directly from  *
//* CA Support Online to a USS directory on your z/OS system.         *
//*                                                                   *
//* When editing the JCL ensure that you do not have sequence numbers *
//* turned on.                                                        *
//*                                                                   *
//* This job must be customized as follows:                           *
//* 1. Supply a valid JOB statement.                                  *
//* 2. The SYSTCPD and SYSFTPD JCL DD statements in this JCL may be   *
//*    optional at your site. Remove the statements that are not      *
//*    required. For the required statements, update the data set     *
//*    names with the correct site-specific data set names.           *
//* 3. Replace "Host" based on the type of download method.           *
//* 4. Replace "YourEmailAddress" with your email address.            *
//* 5. Replace "yourUSSpaxdirectory" with the name of the USS         *
//*    directory used on your system for Pax 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 TIMEOUT 120',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 yourUSSpaxdirectory
binary
get FTP_location
quit
/*
```

Download Files to Mainframe through a PC

You download the product installation files to your PC and transfer them to your USS system.

Follow these steps:

1. Download the product file to your PC using one of the following methods:

   - Pax ESD (see page 38). If you downloaded a zip file, first unzip the file to use the product pax files.
   - DVD. Copy the entire product software package (or individual pax files) to your PC.

   The pax file resides on your PC.

   Note: Do *not* change the format of the pax.Z.

2. Open a Windows command prompt.

   The command prompt appears.

3. Customize and enter the following FTP commands:

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

   mainframe

   Specifies the z/OS system IP address or DNS name.

   userid

   Specifies your z/OS user ID.

   password

   Specifies your z/OS password.

   C:*PC\folder\for\thePAXfile*

   Specifies the location of the pax file on your PC.

   Note: If you specify a location that has blanks or special characters in the path name, enclose that value in double quotation marks.

yourUSSpaxdirectory

Specifies the name of the USS directory that you use for Pax ESD downloads.

***paxfile*.pax.Z**

Specifies the name of the pax file to upload.

The pax file is transferred to the mainframe.

Create a Product Directory from the Pax File

The pax command performs the following actions:

- Extracts the files and directories that are packaged within the pax file.
- Creates a USS directory in the same directory structure where the pax file resides.
- Automatically generates a product and level-specific directory name.

Set the current working directory to the directory containing the pax file, and create a directory in your USS directory by entering the following command:

```
pax -rvf pax-filename
```

Use the sample JCL that is attached to the PDF file as Unpackage.txt (see page 44) to extract the product pax file into a product installation directory.

Important! The PDF version of this guide includes sample JCL jobs that you can copy directly to the mainframe. To access these jobs, click the paper clip icon at the left of the PDF reader. A window displaying attachments opens. Double-click a file to view a sample JCL. We recommend that you use the latest version of Adobe Reader for viewing PDF files.

Follow these steps:

1. Replace *ACCOUNTNO* with a valid JOB statement.
2. Replace *yourUSSpaxdirectory* with the name of the USS directory that you use for product 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 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.

Example: JCL File, Unpackage.txt, to Customize

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

```
//ESDUNPAX JOB (ACCOUNTNO),'UNPAX PAX 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 "yourUSSpaxdirectory" with the name of the USS         *
//*    directory used on your system for Pax 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,       *
//*       start entering characters in column 16 and make sure        *
//*       the 'X' continuation character is in column 72.             *
//*********************************************************************
//UNPAXDIR EXEC PGM=BPXBATCH,
// PARM='sh cd /yourUSSpaxdirectory/; pax -rvf paxfile.pax.Z'
//*UNPAXDIR EXEC PGM=BPXBATCH,
//* PARM='sh cd /yourUSSpaxdirectory/; 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.

The file UNZIPJCL in the product directory contains a sample job to GIMUNZIP the installation package. You edit and submit the UNZIPJCL job to create z/OS data sets.

Follow these steps:

1. Locate and read the product readme file or installation notes, if applicable, which resides in the product-specific directory that the pax command created. This file contains the product-specific details that you require to complete the installation procedure.

   You have identified the product-specific installation details.

2. Use ISPF EDIT or TSO ISHELL to edit the UNZIPJCL sample job. You can perform this step in one of the following ways:

   - Use ISPF EDIT. Specify the full path name of the UNZIPJCL file.
   - Use TSO ISHELL. Navigate to the UNZIPJCL file and use the E line command to edit the file.

   The job is edited.

3. Change the SMPDIR DD PATH to the product-specific directory created by the pax command.

   Your view is of the product-specific directory.

4. If ICSF is not active, perform the following steps:

   a. Change the SMPJHOME DD PATH to your Java runtime directory. This directory varies from system to system.

   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 that the installation process uses. We suggest that you use a unique HLQ for each expanded pax file to identify uniquely the package. Do *not* remove CAI after *yourHLQ*. 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 that you specified in the UNZIPJCL job. You use these data sets to perform the product installation. The pax file and product-specific directory are no longer needed.

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

Prepare the SMP/E Environment for a Pax Installation

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

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

The members that are used in this procedure prepare the data sets, initialize the zones, and create the DDDEFs for your product.

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.

Follow these steps:

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

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

   Note: Set the DASD HLQ to the same value specified for *yourHLQ* within the JCL that is used to unzip the pax file.

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

2. Open the SAMPJCL member BRN1HOLD in an edit session and execute the BRNSEDIT macro from the command line.

   BRN1HOLD is customized.

3. Submit BRN1HOLD.

   This job downloads the error and FIXCAT HOLDDATA from http://ca.com/support.

4. Open the SAMPJCL member BRN2ALL in an edit session and execute the BRNSEDIT macro from the command line.

   BRN2ALL is customized.

   Note: When upgrading into an existing CSI, comment out any allocation DD statements for existing files.

5. Submit BRN2ALL.

   This job produces the following results:

   - The target and distribution data sets for your product are created.
   - Unique SMPLTS, SMPMTS, SMPSCDS, and SMPSTS data sets for this target zone are created.

6. Open the SAMPJCL member BRN3CSI in an edit session and execute the BRNSEDIT macro from the command line.

   BRN3CSI is customized.

   Note: When upgrading into an existing CSI, comment out any allocation DD statements for existing files and delete the CREATCSI step. Change all ADD's to REP's.

7. Submit BRN3CSI.

   This job produces the following results:

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

Run the Installation Jobs for a Pax Installation

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

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

Comment out any unwanted FMIDs.

Follow these steps:

1. Open the SAMPJCL member BRN4RECD in an edit session, and execute the BRNSEDIT macro from the command line.

   BRN4RECD is customized.

2. Submit BRN4RECD to receive SMP/E base functions.

   Your product is received and now resides in the global zone.

3. Open the SAMPJCL member BRN5APP in an edit session, and execute the BRNSEDIT macro from the command line.

   BRN5APP is customized.

4. Submit BRN5APP to apply SMP/E base functions.

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

5. Open the SAMPJCL member BRN6ACC in an edit session, and execute the BRNSEDIT macro from the command line.

   BRN6ACC is customized.

6. Submit BRN6ACC to accept SMP/E base functions.

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

Clean Up the USS Directory

This procedure is optional. If you decide to perform the procedure, do so after you complete the installation process and when you do not need the installation files anymore.

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

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

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

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

Follow these steps:

1. Navigate to your Pax ESD USS directory.

   Your view is of the applicable USS directory.
2. Delete the pax file by entering the following command:

   `rm paxfile`

   paxfile

   Specifies the name of the CA Technologies pax file that you downloaded.

   The pax file is deleted.
3. Delete the product-specific directory by entering the following command:

   `rm -r product-specific_directory`

   product-specific_directory

   Specifies the product-specific directory that the pax command created.

   The product-specific directory is deleted.

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

Apply Preventive Maintenance

Important! We strongly recommend that you use CA CSM to maintain your CA Technologies z/OS-based products. The procedure that is discussed in this section is fully automated when you use CA CSM.

CA Support Online at http://ca.com/support has maintenance and HOLDDATA published since the installation data was created. After the maintenance process completes, the product is ready to deploy.

Use this procedure during product installation and for ongoing preventive maintenance in non-installation use cases according to your maintenance strategy.

Note: To review the CA Technologies mainframe maintenance philosophy, see your *Best Practices Guide* or visit the CA Next-Generation Mainframe Management page.

This procedure directs you to use the CAUNZIP utility. The CAUNZIP utility processes ZIP packages directly on z/OS without the need for an intermediate platform, such as a Microsoft Windows workstation. If you are not familiar with this utility, see the *CA Common Services for z/OS Administration Guide*. This guide includes an overview and sample batch jobs. To use this utility, you must be running CA Common Services for z/OS Version 14.0 with PTF RO54887 or CA Common Services for z/OS Release 14.1 with PTF RO54635 and RO58216. These PTFs are included in CA Common Services for z/OS Release 14.1 at the S1401 Service Update level.

Follow these steps:

1. Check the Download Center at http://ca.com/support for PTFs that have been published since this release was created. If the base release was created recently, no PTFs will have been published yet. If PTFs exist, add published solutions for your product to your Download Cart, and click Checkout.
2. Specify that you want a complete package.

   When processing completes, a link appears on the Review Download Requests page. You also receive an email notification.
3. Click the Alternate FTP link for your order to obtain FTP login information and the ZIP file location. Download the ZIP file into a USS directory on your z/OS system.

4. Run the CAUNZIP utility.

   CAUNZIP unzips the package of published solutions and creates a SMPNTS file structure that the SMP/E RECEIVE FROMNTS command can process. For sample JCL to run the utility that is located in *yourHLQ*.CAW0JCL(CAUNZIP), see the *CA Common Services for z/OS CAUNZIP Administration Guide*. After execution completes, the ZIPRPT data set contains the summary report. The summary report does the following:

   - Summarizes the content of the product order ZIP file.
   - Details the content of each data set and the z/OS UNIX files produced.
   - Provides a sample job to receive the PTFs in your order.

5. Review the sample job that is provided in the CAUNZIP output ZIPRPT file. Cut and paste the JCL into a data set, specify your SMP/E CSI on the SMPCSI DD statement and submit the job to receive the PTFs in your order.

6. Verify that you have the values from the base installation in the BRNSEDIT macro that was customized in the installation steps.

7. Open the SAMPJCL member BRN1HOLD in an edit session and execute the BRNSEDIT macro from the command line.

   Note: Update BRN1HOLD SAMPJCL to download the HOLDDATA file.

   BRN1HOLD is customized.

8. Submit BRN1HOLD.

   The job downloads the external HOLDDATA file.

9. Open the SAMPJCL member BRN7RECH in an edit session and execute the BRNSEDIT macro from the command line.

   BRN7RECH is customized.

10. Submit BRN7RECH.

    The job receives the external HOLDDATA file.

11. (CA Recommended Service (CA RS)) installation only) Do the following:

    a. Determine which ASSIGN statements to download.

       - The yearly CA RS ASSIGN statements are stored in the following file:

         `ftp.ca.com/pub/ASSIGN/YEARLY/CAR`*`yyyy`*`.TXT`

       - The quarterly CA RS ASSIGN statements are stored in the following file:

         `ftp.ca.com/pub/ASSIGN/CAR`*`yymm`*`.TXT`

    b. Open the SAMPJCL member BRN7CARS in an edit session, update BRN7CARS SAMPJCL to download ASSIGN statements from http://ca.com/support, and execute the BRNSEDIT macro from the command line.

    BRN7CARS is customized.

12. (CA RS installation only) Submit BRN7CARS.

    The job downloads the CA RS ASSIGN statements.

13. (CA RS installation only) Open the SAMPJCL member BRN7RECP in an edit session, manually add the data set that contains the ASSIGN statements to the SMPPTFIN DD, and execute the BRNSEDIT macro from the command line.

    BRN7RECP is customized.

14. (CA RS installation only) Submit BRN7RECP.

    The job receives the external HOLDDATA file and CA RS ASSIGN statements.

15. Open the SAMPJCL member BRN8APYP in an edit session and execute the BRNSEDIT macro from the command line.

    BRN8APYP is customized.

16. Submit BRN8APYP.

    The PTFs are applied.

17. (Optional) Open the SAMPJCL member BRN9ACCP in an edit session and execute the BRNSEDIT macro from the command line.

    BRN9ACCP is customized.

18. (Optional) Submit BRN9ACCP.

    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.

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.

System HOLDDATA

System HOLDDATA indicates data that is an in-stream part of the SYSMOD, informing you of special conditions. The following reasons are used with SYSTEM HOLDDATA for your product:

ACTION

Indicates that you must perform special processing before or after you apply this SYSMOD.

AO

Affects automated operations. It changes either the message identifier or the displacement of a field inside the message.

DB2BIND

Indicates that DBRMs have changed and packages need to be rebound.

DDDEF

Indicates that data sets and DDDEFs are being added or modified.

DELETE

Deletes the SYSMOD load module. You cannot reverse this type of SYSMOD with the SMP/E RESTORE command.

DEP

Indicates a dependency for this SYSMOD that you must externally verify.

DOC

Indicates a documentation change with this SYSMOD.

DYNACT

Describes the steps to dynamically activate this fix without performing an IPL.

EC

Indicates that this SYSMOD requires a hardware engineering change. An EC hold SYSMOD usually does not affect the product unless the EC is present on the hardware device.

ENH

Introduces a small programming enhancement. The hold contains the instructions to implement the enhancement. If no action is needed to implement the enhancement, give a summary of the enhancement.

EXIT

Indicates that changes delivered by this SYSMOD require reassembly of user exits.

EXRF

Indicates that the SYSMOD must be installed in both the Active and Alternate Extended Recovery Facility Systems.

IPL

Indicates that an IPL is required for this SYSMOD to take effect. This is used only when there is no alternative for dynamic activation.

MSGSKEL

Indicates that the SYSMOD contains internationalized message versions that must be run through the message compiler for each language.

MULTSYS

Apply this SYSMOD to multiple systems for either pre-conditioning, coexistence, or exploitation.

RESTART

Indicates that after applying this SYSMOD, the site must perform a special restart as opposed to a routine restart.

SQLBIND

Indicates that a bind is required for a database system other than DB2.

DOWNLD

Indicates that some or all of the elements that this SYSMOD delivers are to be downloaded to a workstation.

Code a BYPASS(HOLDSYS) operand on your APPLY command to install SYSMODs that have internal holds. Code the BYPASS(HOLDSYS) operand only after you have performed the required action, or if you are performing the action after the APPLY, if that is appropriate.

External HOLDDATA

External HOLDDATA is not part of the PTF. The HOLDDATA resides in a separate file and contains both error and FIXCAT HOLDDATA. The error HOLDDATA is used for SYSMODs that have been distributed and later are discovered to cause problems. The FIXCAT HOLDDATA helps identify maintenance that is required to support a particular hardware device, software, or function.

Download the external HOLDDATA from http://ca.com/support to a DASD file, and allocate the file to the SMPHOLD DD statement. To take care of the external HOLDDATA, receive it into your SMP/E environment. SMP/E receives the HOLDDATA from CA-supplied jobs.

You can find JCL to download the external HOLDDATA in your SAMPJCL member. Open BRN1HOLD in an edit session and execute the BRNSEDIT macro on the command line. Then, submit the JCL.

Error HOLDDATA

If a SYSMOD has unresolved error HOLDDATA, SMP/E does not install it unless you add a bypass to your APPLY command. You can bypass error HOLDDATA in situations that are not applicable to you. Error HOLDDATA that is not applicable to you can include a problem that happens only with a hardware device that you do not have or in a product feature that you do not use.

When CA Technologies publishes a SYSMOD that resolves the error HOLDDATA, the resolving SYSMOD supersedes the error HOLDDATA. This action lets you apply the original SYSMOD in conjunction with the fixing SYSMOD.

The only manual task is running a REPORT ERRSYSMODS. This report identifies the following:

- Any held SYSMODs already applied to your system
- Any resolving SYSMODs that are in RECEIVE status

SMP/E identifies the SYSMOD to apply to correct the situation.

FIXCAT HOLDDATA

CA Technologies provides FIXCAT HOLDDATA to help identify maintenance that is required to support a particular hardware device, software, or function. Fix categories are supplied as SMP/E FIXCAT HOLDDATA statements. Each FIXCAT HOLDDATA statement associates an APAR and its related fixing PTF to one or more fix categories.

Chapter 5: Starting Your Product

This section contains the following topics:

How to Complete Deployment With CA CSM

The topics in this section describe the manual tasks that you perform when deploying your product using CA CSM (see page 29).

How to Complete Configuration With CA CSM

The topics in this section describe the manual tasks that you perform when configuring your product using CA CSM (see page 30).

Authorize Program Load Libraries

All users must perform this step.

To either authorize the program load library or copy the modules to a system-authorized library, do *one* of the following:

- If you want CA Deliver to execute from its own load library, APF-authorize the load library by adding an entry for CAI.CVDELOAD to member PROG*xx* of SYS1.PARMLIB.

  Note: Use MVS system command SET PROG=xx to activate update to PROGxx.

- If you do *not* want to APF-authorize the CA Deliver target library, copy the load modules in CAI.CVDELOAD to an existing authorized library such as SYS1.LINKLIB or any other library in the linklist.

  Use *one* of the following methods to copy the load modules:

  - ISPF option 3.3
  - Member HBRNCAPF of CAI.CVDEJCL

    Run this batch job to copy the load modules from CAI.CVDELOAD to USER.APFLIB.

Important: We recommend that you authorize CVDELOAD rather than copying the modules. The load modules must reside in an authorized library.

Enter the LMP Code

All users must perform this step.

CA Deliver requires CA LMP (License Management Program), one of the CA Common Services, to initialize correctly. CA LMP provides a standardized and automated approach to the tracking of licensed software. Examine the CA LMP Key certificate you received with your product installation or maintenance cartridge.

The LMP Key Certificate

Your LMP Key certificate contains the following information:

Product Name

Signifies the trademarked or registered name of the copy of CA Deliver licensed for your designated site and CPUs.

Supplement

Signifies the reference number of your license for the particular CA Deliver, in the format nnnnnn nnn.

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

Expiration Date

Signifies the date (MONTH dd, yyyy as in OCTOBER 21, 2009) when your license expires for the installation and maintenance of the designated CA Deliver.

Technical Contact

Signifies the name of the technical contact at your site who is responsible for the installation and maintenance of CA Deliver.

This is the person to whom CA addresses all CA LMP correspondence.

MIS Director

Signifies the name of the Director of MIS, or the person who performs that function at your 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.

CPU Location

Signifies the address of the building where the CPU is installed.

Execution Key

Signifies the encrypted code required by CA LMP for CA Deliver initialization.

During installation, this code is referred to as the LMP Code.

Product Code

Signifies the two-character code that corresponds to CA Deliver.

CPU ID

Signifies a code that identifies the specific CPU for which installation of your CA Deliver is valid.

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.

Defining the CA LMP Execution Key

To define a CA LMP execution key to the CAIRIM parameters, modify member KEYS in OPTLIB data set.

Syntax is as follows:

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

where:

pp

Signifies the two-character product code (required).

For any given CA LMP software solution, this code agrees with the product code already in use by the CAIRIM initialization parameters for earlier service packs of the product.

ddmmmyy

Signifies the CA LMP licensing agreement expiration date (required).

tttt-mmmm

Signifies the CPU type and model (for example, 3090-600) on which the CA LMP software solution will run (required).

If the CPU type and/or model requires less than four characters, blank spaces are inserted for the unused characters.

ssssss

Signifies the serial number of the CPU on which the CA LMP software solution will run (required).

kkkkkkkkkkkk

Signifies the execution key needed to run the CA LMP software solution (required).

This CA LMP execution key is provided on the key certificate shipped with each CA LMP software solution.

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

Note: The CA LMP execution key is *invalid* and is provided as an example only.

```
PROD(HV) DATE(21OCT09) CPU(3090-600 /370623)
LMPCODE(52H2K06130Z7RZD6)
```

For a full description of the procedure for defining the CA LMP execution key to the CAIRIM parameters, see the installation tasks in the *CA Common Services Getting Started.*

Multiple LMP Codes

CA Deliver consists of the base product and several components (options) that are purchased separately. Because each component has its own LMP code, you must supply an LMP code for each component you purchased.

This table lists the component product codes:

pp	Component Description
HV	CA Deliver base product
HW	CICS online interface
HX	IMS/DC online interface
HZ	Native TSO online interface
IF	CA Roscoe online interface
IJ	VTAM online interface

Note: For more information about the components, see Software Requirements in the chapter "System Requirements."

Define Security Rules

All users must perform this step.

Upgrade Considerations

If you are upgrading, see the chapter "Upgrading from a Previous Release" for information that applies to this step.

CA Deliver has full external security support that uses security classes. CA Deliver interfaces with CA Top Secret, CA ACF2, and IBM's RACF and it gives you the ability to define a security table and use security exits.

Note: For more information about security, see the chapter "Security" in the *CA Deliver Reference Guide*.

Install the ISPF Online Retrieval Option

The ISPF online retrieval option runs under the IBM Interactive System Productivity Facility (ISPF).

This list summarizes the steps required to install the ISPF online retrieval option. Detailed instructions are in the sections that follow.

1. (Optional) Add STEPLIB Statements

   If the load modules were *not* copied to a linklist library, add STEPLIB DD statements to the TSO LOGON procedures.

2. Add the Panel and Command Libraries

   Add the panel and command table libraries to the TSO LOGON procedures.

3. (Optional) Modify an ISPF Selection Menu to Select Online Retrieval.

(Optional) Step 1: Add STEPLIB Statements

The action you take in this step depends on what you did during the base product installation—specifically, did you:

- Authorize the program load library or
- Copy the modules to a system-authorized library

If the CA Deliver load modules were *not* copied to one of the libraries in the linklist, proceed with this step; otherwise go directly to the next step.

Follow these steps:

1. Add STEPLIB DD statements to the TSO LOGON procedures if the load modules are not in a linklist library.
2. Add a STEPLIB DD statement for the library containing the product's load modules to the LOGON procedures for those TSO users who are going to be using the ISPF online retrieval option.

Note: If you have CA View, the CA View load modules must also be either in the linklist or in a STEPLIB statement with this step.

Step 2: Add the Panel and Command Libraries (ISPF only)

Note: If you are running under SPF, go to Step 3.

If you run CA Deliver under ISPF, proceed with this step.

To add the panel and command libraries to the TSO LOGON procedure:

1. Concatenate the command table library CAI.CVDETBL0 to DD statement ISPTLIB.
2. Concatenate the panel library CAI.CVDEPNL0 to DD statement ISPPLIB.

Note: If you also plan to use RMOSPF (the ISPF interface), and multiple versions of CA Deliver, concatenate CAI.CVDETBL0 first. Use the CAI.CVDETBL0 from the most current release.

Step 3: (Optional) Modify an ISPF Selection Menu to Select Online Retrieval

If you want to add a selection code for the online retrieval feature to one of the ISPF selection menus, proceed with this step; otherwise, your detailed instructions for ISPF are complete.

To define your selection code, use the following command:

```
PGM(RMOSPF) PARM(high-level-database-name) NEWAPPL(RMO)
```

Use the value next to the NAME parameter on your Initialization Parameter Worksheet for PARM (high-level-database-name).

Note: Adding a selection code allows you to select the online retrieval feature in the same way you would select other ISPF options.

Panel Libraries

The names of the panel libraries vary from site to site and for the different releases of ISPF. These panel libraries are allocated to the ISPPLIB DD statement under TSO.

Be aware that some installations do not allow direct modifications of IBM panels and libraries. In this case, you can place the modified panels in user or site-specific libraries and concatenate them ahead of the IBM libraries.

Ask your system administrator for the specific ISPF panel library that applies to your site and contains the panel ISR@PRIM.

Note: The selection menus shown in the following examples are part of the program product ISPF and are copyrighted by IBM.

Example 1

This example shows you how to add selection code R to the primary option menu ISR@PRIM for ISPF.

The offset lines are the inserted lines.

```
%----------------------- ISPF/PDF PRIMARY OPTION MENU ------------------------
%OPTION ===>_ZCMD                                                            +
%                                                        +USERID    - &ZUSER
%   0 +ISPF PARMS -   SPECIFY TERMINAL AND USER PARAMETERS   +TIME  -
%   1 +BROWSE      -  DISPLAY SOURCE DATA OR OUTPUT LISTINGS +TERMINAL -
%   2 +EDIT        -  CREATE OR CHANGE SOURCE DATA        +PF KEYS - &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, CLIST, OR REXX EXEC
%   7 +DIALOG TEST -  PERFORM DIALOG TESTING
%   8 +LM UTILITIES - PERFORM LIBRARY ADMINISTRATOR UTILITY FUNCTIONS
%   C +CHANGES     -  DISPLAY SUMMARY OF CHANGES FOR THIS RELEASE
%   R +RMOSPF      -  DELIVER ADMINISTRATION
%   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 /* TUTORIAL INDEX - 1ST PAGE         */
)PROC
 &ZSEL = TRANS( TRUNC (&ZCMD,'.')
                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(ISPYXDR) PARM(ISR) NOCHECK'
                8,'PANEL(ISRLPRIM)'
                C,'PGM(ISPTUTOR) PARM(ISR00005)'
           R,'PGM(RMOSPF) PARM(RMO.SYSTEM1) NEWAPPL(RMO)'
                T,'PGM(ISPTUTOR) PARM(ISR00000)'
               ' ',' '
                 X,'EXIT'
                 *,'?' )
   &ZTRAIL = .TRAIL
 )END
```

Note:

- NEWAPPL(RMO) is required and must be specified as shown previously in this section.

  This parameter is used with the command table library concatenation from Step 3 of the ISPF Installation Instructions.

- NEWAPPL(RMO) allows CA Deliver to correctly interpret commands and program function key invocation.

  If this parameter is not specified, certain PF keys such as the scroll keys may not function.

Example 2

This example shows you how to add selection code 3.R as a sub-option to the utilities menu ISPUTIL for ISPF.

The offset lines are the inserted lines.

```
%-----------------------  UTILITY SELECTION MENU  --------- -----------
%OPTION  ===>_OPT         +
%                                                                      +
%   1 +LIBRARY     - LIBRARY UTILITY:
+                    PRINT INDEX LISTING OR ENTIRE DATASET
+                    PRINT, RENAME, DELETE, OR BROWSE MEMBERS
+                    COMPRESS DATASET
%   2 +DATASET     - DATASET UTILITY:
+                    DISPLAY DATASET INFORMATION
+                    ALLOCATE, RENAME, OR DELETE ENTIRE DATASET
+                    CATALOG OR UNCATALOG DATASET
%   3 +MOVE/COPY   - MOVE OR COPY MEMBERS OR DATASETS
%   4 +CATALOG     - CATALOG MANAGEMENT:
+                    DISPLAY OR PRINT CATALOG ENTRIES
+                    INITIALIZE OR DELETE USER CATALOG ALIAS
%   5 +RESET       - RESET STATISTICS FOR MEMBERS OF ISPF LIBRARY
%   6 +HARDCOPY    - INITIATE HARDCOPY OUTPUT
%   7 +VTOC        - DISPLAY OR PRINT VTOC ENTRIES FOR A DASD VOLUME
%   8 +OUTLIST     - DISPLAY, DELETE, OR PRINT HELD JOB OUTPUT
%   9 +SCRIPT/VS   - FORMAT,DISPLAY, AND OPTIONALLY PRINT SCRIPT TEXT
%   R +RMOSPF      - DELIVER ADMINISTRATION

)INIT
  .HELP = TU
)PROC
  &SEL = TRANS( TRUNC (&OPT,'.')
                1,'PGM(ISPUDA) PARM(UDA1)'
                2,'PGM(ISPUDA) PARM(UDA1)'
                3,'PGM(ISPUMC)'
                4,'PGM(ISPUCA)'
                5,'PGM(ISPURS)'
                6,'PGM(ISPUHC)'
                7,'PGM(ISPUVT)'
                8,'PGM(ISPUOL) PARM(UOL01)'
                9,'PGM(ISPUSC) PARM(SCRPTA)'
             R,'PGM(RMOSPF) PARM(RMO.SYSTEM1) NEWAPPL(RMO)'
               ' ',' '
                *,'?' )
 )END
```

Install the TSO Online Retrieval Option

The following step is required to install the TSO online retrieval option and is explained in detail in the next topic.

(Optional) Add STEPLIB DD statements to the TSO LOGON procedures if the load modules are not in a linklist library.

Step 1: (Optional) Add STEPLIB DD Statements

The action you take in this step depends on what you did during the base-product installation—specifically, did you:

- Authorize the program load library or
- Copy the modules to a system authorized library

If the load modules were *not* copied to one of the libraries in the linklist:

- Add a STEPLIB DD statement (for the library containing the load modules) to the TSO LOGON procedures for those TSO users who are to use the native TSO online retrieval option.

If the load modules were copied to one of the libraries in the linklist, no STEPLIB DD statements are required.

Note: If you have CA View, the CA View load modules either must also be in the linklist, or placed in a STEPLIB statement with this step.

Step 2: (Optional) Add Mount Attributes

Assign the mount attribute to all TSO user IDs authorized to browse SYSOUT directly from an archival tape. Use the TSO ACCOUNT command to assign the mount attribute as follows:

```
ACCOUNT
C (userid) MOUNT
END
```

Install the CA Roscoe Online Retrieval Option

The CA Roscoe online retrieval option runs as a command processor under ETSO/Roscoe.

The following steps are required to install the CA Roscoe/Cross-Memory Online Retrieval Option. Each step is explained in detail in the sections that follow.

1. (Optional) Concatenate the Load Module Library to the ETSOLIB DD statement, if the load modules were not copied to a linklist library.
2. Add the control statement for the RMOROS command processor to the Eligible Program List (EPL).
3. Invoke the RMOROS command processor.

Step 1: (Optional) Concatenate the Load Module Library

If the load modules were *not* copied to a linklist library, concatenate the library that contains the load modules to the ETSOLIB DD statement in the CA Roscoe startup JCL.

Note: If you have CA View, the CA View load modules must also be either in the linklist or in an ETSOLIB statement with this step.

Step 2: Add RMOROS Command Process

Add this Eligible Program List control statement to member ETSOPGMS for the CA Roscoe user with the RO prefix:

Column	Contents
1–8	RMOROS
9	Blank
10–12	Number of users allowed to access CA Deliver at one time
13	Blank
14–17	CPU time slice; use 9999 to prevent premature termination
18	Blank
19–24	Maximum memory (in KB) below the 16 MB line This value can vary depending on size of database and other factors (0001000 should be adequate).
25	Blank
26–31	Maximum memory (in KB) below the line that CA Deliver can acquire at one time Use 999999 so that GETMAINs are not limited.

Column	Contents
32	Blank
33–38	Maximum memory (in KB) above the 16 MB line This value can vary depending on the features used (000512 should be adequate).
39	Blank
40–45	Maximum memory (in KB) above the line that CA Deliver can acquire at one time Use 999999 so that GETMAINs are not limited.
46	Blank
47–48	CP to call RMOROS as a TSO command processor
49	Y – Application authorized to issue MODESET SVC
50	Blank
51-52	CP to call EC2XMROS as a TSO command processor
53-255	Ignored

Install the XMS Online Interfaces (Optional)

If you want to install the XMS Online Interfaces to complete configuration with CSM see the topic *How to Complete Configuration of the XMS Online Interfaces with CA CSM* in the chapter *Installing the Online Interfaces*.

How to Configure Without CA CSM

The topics in this section describe the manual tasks you perform if you are not configuring your product using CA CSM.

Step 1: Authorize Program Load Libraries

All users should perform this step.

Do *one* of the following to either authorize the program load library or copy the modules to a system-authorized library:

- If you want CA Deliver to execute from its own load library, APF-authorize the load library by adding an entry for CAI.CVDELOAD to member PROG*xx* of SYS1.PARMLIB.

  Note: Use MVS system command SET PROG=xx to activate update to PROGxx.

- If you do *not* want to APF-authorize the CA Deliver target library, copy the load modules in CAI.CVDELOAD to an existing authorized library such as SYS1.LINKLIB or any other library in the linklist.

  Use *one* of the following methods to copy the load modules:

  - ISPF option 3.3
  - Member HBRNCAPF of CAI.CVDEJCL

    This batch job can be run to copy the load modules from CAI.CVDELOAD to USER.APFLIB.

Important: We recommend that you authorize CVDELOAD rather than copying the modules. The load modules must reside in an authorized library.

Step 2: Enter the LMP Code

All users must perform this step.

CA Deliver requires CA LMP (License Management Program), one of the CA Common Services, to initialize correctly. CA LMP provides a standardized and automated approach to the tracking of licensed software.

Examine the CA LMP Key certificate you received with your product installation or maintenance cartridge.

The LMP Key Certificate

Your LMP Key certificate contains the following information:

Product Name

Signifies the trademarked or registered name of the copy of CA Deliver licensed for your designated site and CPUs.

Supplement

Signifies the reference number of your license for the particular CA Deliver, in the format nnnnnn nnn.

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

Expiration Date

Signifies the date (MONTH dd, yyyy as in OCTOBER 21, 2009) when your license expires for the installation and maintenance of the designated CA Deliver.

Technical Contact

Signifies the name of the technical contact at your site who is responsible for the installation and maintenance of CA Deliver.

This is the person to whom CA addresses all CA LMP correspondence.

MIS Director

Signifies the name of the Director of MIS, or the person who performs that function at your 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.

CPU Location

Signifies the address of the building where the CPU is installed.

Execution Key

Signifies the encrypted code required by CA LMP for CA Deliver initialization.

During installation, this code is referred to as the LMP Code.

Product Code

Signifies the two-character code that corresponds to CA Deliver.

CPU ID

Signifies a code that identifies the specific CPU for which installation of your CA Deliver is valid.

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.

Defining the CA LMP Execution Key

To define a CA LMP execution key to the CAIRIM parameters, modify member KEYS in OPTLIB data set.

Syntax is as follows:

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

where:

pp

Signifies the two-character product code (required).

For any given CA LMP software solution, this code agrees with the product code already in use by the CAIRIM initialization parameters for earlier service packs of the product.

ddmmmyy

Signifies the CA LMP licensing agreement expiration date (required).

tttt-mmmm

Signifies the CPU type and model (for example, 3090-600) on which the CA LMP software solution will run (required).

If the CPU type and/or model requires less than four characters, blank spaces are inserted for the unused characters.

ssssss

Signifies the serial number of the CPU on which the CA LMP software solution will run (required).

kkkkkkkkkkkk

Signifies the execution key needed to run the CA LMP software solution (required).

This CA LMP execution key is provided on the key certificate shipped with each CA LMP software solution.

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

Note: The CA LMP execution key is *invalid* and is provided as an example only.

```
PROD(HV) DATE(21OCT09) CPU(3090-600 /370623)
LMPCODE(52H2K06130Z7RZD6)
```

For a full description of the procedure for defining the CA LMP execution key to the CAIRIM parameters, see the installation tasks in the *CA Common Services Getting Started.*

Multiple LMP Codes

CA Deliver consists of the base product and several components (options) that are purchased separately. Because each component has its own LMP code, you must supply an LMP code for each component you purchased.

This table lists the component product codes:

pp	Component Description
HV	CA Deliver base product
HW	CICS online interface
HX	IMS/DC online interface
HZ	Native TSO online interface
IF	CA Roscoe online interface
IJ	VTAM online interface

Note: For more information about the components, see Software Requirements in the chapter "System Requirements."

Step 3: Define Security Rules

All users must perform this step.

Upgrade Considerations

If you are upgrading, see the chapter "Upgrading from a Previous Release" for information that applies to this step.

CA Deliver has full external security support that uses security classes. CA Deliver interfaces with CA Top Secret, CA ACF2, and IBM's RACF and it gives you the ability to define a security table and use security exits.

Note: For more information about security, see the chapter "Security" in the *CA Deliver Reference Guide*.

Step 4: Create/Update the Database

All new users must perform this step.

Upgrade Considerations

If you are upgrading, see the chapter "Upgrading from a Previous Release" for more information about how to perform this step.

For new installations, to create the database use the ADDDS and MAKECKPT control statements in the RMODBASE utility program. Member HBRNADDS of CAI.CVDEJCL provides a sample set of parameters for this job.

Note: For more information about the RMODBASE utility, see the chapter "Utilities" in the *CA Deliver Reference Guide*.

Step 5: Create the Initialization Parameter Statements

All users must perform this step.

Upgrade Considerations

If you are upgrading, see the chapter "Upgrading from a Previous Release" for information that applies to this step.

For new installations, create the initialization parameter statements for the started task which can be a member within a PDS. This member is referenced by the RMOPARMS DD statement of the started task. Member RMOPARMS in CAI.CVDEOPTN provides a sample initialization parameter member.

Note: For more information about the descriptions of these parameters, see the chapter "Initialization Parameters" in the *Reference Guide.*

The data sets for the initialization parameter statements must:

- Be members in a partitioned data set
- Have a logical record length of 80 (LRECL=80)
- Have a block size of any multiple of 80 (for example, BLKSIZE=3200)
- Have record format FB (RECFM=FB)

Step 6: Modify the Skeleton JCL

All users must perform this step.

Examine the skeleton JCL and make any necessary changes by editing member RMOJCLB in the CAI.CVDEPENU data set. The following sections explain how to do this editing.

The online task uses the skeleton JCL to submit background bundle jobs.

Bundle Output Carriage Control

By default, machine carriage control produces batch bundle output for all banner pages and reports within the bundle.

If changes are required, the RMOJCLB skeleton JCL can be modified to instruct the batch bundle program to create batch bundle output with ASA carriage control. You can specify this option by adding ",ASA" after the database index name variable &IDX on the PARM field of the EXEC statement for RMOBBP in the skeleton JCL as follows:

```
//STEP1    EXEC PGM=RMOBBP,
//         PARM='&IDX,ASA'
```

Notes:

- By default, the beginning of each individual SYSOUT data set within the bundle contains a no skip ("+") ASA carriage control character. If you want the individual SYSOUT data sets to start with a skip to top of form ("1") ASA carriage control character, change the model bundle banner page members to use a "J" carriage control character instead of a "1" carriage control character.
- For more details on how to customize model banner pages, see the chapter Model Banner Pages in the *Reference Guide*.

Define STEPLIBs

The only change to make to the skeleton JCL is to the STEPLIB DD statement. If you are running CA View out of a separate CVDELOAD, the STEPLIB statement has to concatenate both the CA Deliver and CA View CVDELOADs.

Remove the STEPLIB DD statement if the CVDELOAD (or CVDELOADs) are in your linklist.

Be aware that you must concatenate the CA View load library after the CA Deliver load library in the STEPLIB statement.

Step 7: Load the Online Panels and JCL Library

All users must perform this step.

Upgrade Considerations

If you are upgrading, see the chapter "Upgrading from a Previous Release" for more information about this step.

Load the online panel and JCL library members to the database from the CAI.CVDEPENU data set.

The RMODBASE OLOAD control statement is used to load the panel, message, and skeleton JCL members in the online library to the database. The online library is defined with the DD statement RMOOLIB.

Note: The *high-level* name of the database must have been defined with the NAME control statement (or the PARM parameter of the EXEC JCL statement).

Syntax:

```
OLOAD
```

Member HBRNOLOD of CAI.CVDEJCL provides sample JCL for this job.

Customizing BROWSE and HELP Panels

The CAI.CVDEPENU data set contains the BROWSE and HELP panels; you can modify them with the following limitations:

Constants:

Constants can be modified and their length can be increased or decreased. The new text displays as coded.

Variables:

- Most variables can be moved around the screen as long as the original variable names are retained

  Be aware that the relative position of some variables is critical.
- The length of a variable can be changed, but be aware that the product pads the value with blanks (or truncates it) to conform to its internal length.
- Any variable can be deleted from a panel.
- An attempt to add a new variable to a screen results in the variable name itself appearing on the screen, without interpretation.

Customizing Panels for Color and Highlight

CA Deliver supports the display of the following colors:

- Blue
- Red
- Pink
- Green
- Turquoise
- Yellow
- White

CA Deliver supports the following highlight attributes:

- Blink
- Reverse video
- Underscore

Note: For these attributes, the colors used must be red, white, blue, or green.

Define color and highlight attributes on the CA Deliver panels according to the rules listed in the IBM manual *ISPF Dialog Developer's Guide and Reference.*

The following hexadecimal characters are reserved and cannot be defined as attribute statements on a panel:

00

Represents Null character.

0E

Represents Shift out.

0F

Represents Shift in.

40

Represents Blank.

50

Represents Ampersand (&).

Step 8: Load the Model Banner Pages and Email Format (EFORMAT) members

All users must perform this step.

Upgrade Considerations

If you are upgrading, see the chapter "Upgrading from a Previous Release" for more information about this step.

Review, change, or add model banner page and/or email format members in the model banner page library.

Note: For more information about model banner page and email format members, see the chapter "Model Banner Page and Email Format Members" in the *Reference Guide*.

Load the model banner page and email format members to the database from the CAI.CVDE133 data set.

The RMODBASE BLOAD control statement is used to load the model banner page and email format members in the model banner page library to the database. The model banner page library is defined with the DD statement RMOBLIB.

Note: The *high-level* name of the database must have been defined with the NAME control statement (or the PARM parameter of the EXEC JCL statement).

Syntax:

```
BLOAD
```

Member HBRNBLOD of CAI.CVDEJCL provides sample JCL for this job.

Step 9: Add the Start Procedure to PROCLIB

All users must perform this step.

Upgrade Considerations

If you are upgrading, see the chapter "Upgrading from a Previous Release" for more information about this step.

Add the Start Procedure

To add the start procedure to the PROCLIB for the started task:

1. Add the start procedure JCL, located in CBRNSSTC in CAI.CVDEPROC, as member RMOSTC of SYS1.PROCLIB:

   ```
   //RMOSTC    EXEC PGM=RMOSTC,TIME=NOLIMIT,REGION=0M
   //STEPLIB   DD  DSN=CAI.CVDELOAD,DISP=SHR
   //SYSUDUMP  DD  SYSOUT=A
   //RMOPARMS  DD  DSN=CAI.CVDEOPTN(RMOPARMS),DISP=SHR
   //*RMOJTAB  DD  DSN=your.rmojtab,DISP=SHR
   ```

2. Set the recommended CA Deliver REGION size.

   We recommend that you run CA Deliver with a REGION=128M. This covers the current storage requirements for a daily cycle and can be useful and still provide a reserve that might be needed when extra storage is required.

Alternately, you can leave the REGION size 0M from the sample procedure, start RMOSTC with a 0M region and continue with the same value for at least two days to monitor the processing for two daily cycles. This allows all available private storage above and below the 16 MB line to be used for RMOSTC.

Bring RMOSTC down and review the *IEF374I* message in the JOBLOG; this log provides a high-water mark of the storage use.

The REGION value is in K not M, so divide the value *nnn*K by 1024 to get the value in M. Round the result up and add at least 5 to the result. This gives you the minimum region size to use.

For example:

```
VIRT   540K SYS   296K EXT   40998K SYS   10124K
```

The storage usage value in this example is 40998K. If you divide this by 1024 you get a value over 40 (round up the result to 41 and add 5).

The required region in this case is 46M.

3. Do one of the following:

   - If the load modules were copied to an authorized library other than a linklist library, change the data set name on the STEPLIB DD statements.
   - If the load modules were copied to a linklist library, remove the STEPLIB DD statements.

4. If you use direct-to-VIEW, and the CA VIEW load library is separate, add it to the STEPLIB concatenation.

   Load module SARPAM in the CA View load library is required for direct-to-VIEW archival.

5. Change the data set name on the RMOPARMS DD statement to the name of the card image data set that contains the initialization parameter statements.

   RMOPARMS can be a member of a PDS:

   ```
   //RMOPARMS DD  DSN=CAI.CVDEOPTN(RMOPARMS),DISP=SHR
   ```

6. The RMOJTAB DD statement is optional; include it when job name translation control statements are to be input to the started task.

   The DD statement that is commented out in the procedure is an example only and must be changed to point to your *rmojtab*.

   Note: For more information about how to code this table, see the chapter "The Database" in the *Reference Guide*.

Step 10: (Optional) Maintain Detail History with JES2

This step is for JES2 sites only. JES3 users should go to the (Optional) Maintain Detail History with JES3 step.

Detail History is an optional feature of CA Deliver that is activated by setting HDETAIL=YES in your initialization parameters. More DASD space is required for storing this historical data than is required for running without it.

If you decide that you would like to maintain detailed historical data with the actual date and time that reports and bundles are printed, continue with the next section, Capturing Detailed Historical Data. Otherwise, go to the Set Up for Multiple CPUs step.

Note: Detailed history can consume a considerable amount of DASD space. For more information, see the description of the basic and detailed history panels in Appendix A of the *Administration Guide*.

Capture Detailed Historical Data

Do the following to capture detailed historical data:

1. Determine the following:
   - Do you want to capture detailed historical data?

     and:

     Do you use impact printers or IBM 3800 printers that are operating in compatibility mode?
   - Is your printer a local, channel-attached printer?

     or:

     Do you use APF printers that are driven by IBM's PSF?
2. Do *one* of the following:
   - If you answered No to both of the conditions in Step 1, go to the Set Up for Multiple CPUs step.
   - If you answered Yes to either of the conditions in Step 1, assemble and link edit RMOJ2XIT.

     RMOJ2XIT contains the source for EXIT1 and EXIT15, as a member of your JES2 load library (SYS1.LINKLIB).

Note: Apply USERMOD RMOJ2XIT. This USERMOD is located in dataset CAI.CVDEJCL as member BRNSJ2X.

Add the following JES2 initialization parameters to the JES2 startup initialization stream:

```
EXIT1    ROUTINE=RMOJ2X1
EXIT15   ROUTINE=RMOJ2X15
LOAD     RMOJ2XIT
```

- If you answered Yes to the AFP condition in Step 1, you have to install exit RMOFSSUX. For more information, see the chapter User Exits in the *Programming Guide*.

Step 11: (Optional) Maintain Detail History with JES3

This step is for JES3 sites only.

Detail History is an optional feature of CA Deliver; to activate it set HDETAIL=YES in your initialization parameters.

Note: Storing this historical data requires considerably more DASD space than running without it does.

If you decide that you want maintain detailed historical data with the actual date and time that reports and bundles are printed:

- Assemble the front-end control sections
- Link edit the sections with the JES3 load modules as shown in the following table:

CA Deliver JES3 User Exit Front-End Control Sections	JES3 User Exit Load Modules	USERMOD to Install
RMOJ3X21	IATUX21	BRNSJ321
RMOJ3X23	IATUX23	BRNSJ323

Your JES3 load module library is to appear as the data set name of the L.SYSLMOD DD statements.

To install these exits, use the USERMODs located in CAI.CVDEJCL. Note that the source for these exits is located within the USERMOD.

Note: Bring JES3 down then bring it up to turn on the user exits.

If you are driving APF printers with IBM's PSF, install the exit RMOFSSUX. For more information, see the chapter User Exits in the *Programming Guide.*

Note: Detailed history can consume a considerable amount of DASD space. For more information, see the description of the basic and detailed history panels in Appendix A of the *Administration Guide*.

Step 12: Set Up for Multiple CPUs

All users must perform this step.

Upgrade Considerations

If you are upgrading, see the chapter "Upgrading from a Previous Release" for information that applies to this step.

Define ENQs to the System Integrity Product

The product issues ENQs and RESERVEs as necessary to maintain the integrity of its data sets. CA Deliver uses the primary ENQ (QNAME=RMOSTC) during startup and shutdown to serialize control block updates.

- This enqueue is defined as SYSTEM to prevent a second CA Deliver from starting on this LPAR with the same characteristics. This ENQ does not have to be defined to a system integrity product.
- A second ENQ (QNAME=RMOCKPT) is used during the OPEN and CLOSE of the checkpoint file. This ENQ does not need to be defined to a system integrity product.
- The RESERVE issued by CA Deliver is normally short-lived but will cause deadlock conditions unless it is properly defined. The RESERVEs should be converted to global enqueues; however, if your environment dictates, the reserves do not have to be converted.

If the CA Deliver database and the checkpoint file are on dedicated volumes with no other datasets, you do not have to convert RESERVES to global enqueues.

Using RESERVE and ENQ

This table shows how CA Deliver uses ENQ and RESERVE.

QNAME	Type	Description	Integrity Product Control
RMOSTC	ENQ	Serializes control block updates during startup and shutdown	NO

QNAME	Type	Description	Integrity Product Control
RMOCKPT	ENQ	Serializes the CA Deliver checkpoint during open and close	NO
RMOUPD	RESERVE	Serializes the updating of the CA Deliver database	YES/NO (if environment dictates)

Database Extent Considerations

In a multiple CPU environment, it is possible that processes in each system image are accessing a database extent. To minimize contention, we recommend:

- Place each database extent on a dedicated volume.
- Where it is possible, match the size of the volume and the size of the database extent.

  This matching allows each extent to be accessed by its own server (device address). I/Os for multiple extents are prevented from queuing on the same device address, which can happen if multiple database extents are allocated on the same device.

Step 13: (Optional) Construct the Initial Report and Job Data

Perform this step if you want to construct initial report and job data in the database from an existing JCL library. Otherwise, skip this step.

Two utilities, RMOJCL and RMOJCS are supplied with CA Deliver to create report and job definitions in the database from the job's JCL.

Note: For more information about utilities, see these topics in the chapter "Utilities" in the *Reference Guide*:

- RMOJCL – Automatic Database Construction from JCL
- RMOJCS – Enhanced Database Construction from JCL

Note: The JCLCheck Common Component is no longer distributed as part of the CA Deliver Distribution Libraries. We recommend that clients who use the RMOJCS utility refer to the CA JCLCheck Common Component Installation documentation.

Step 14: Set Up the Viewing Interface

All CA View users must perform this step.

Upgrade Considerations

If you are upgrading, see the chapter "Upgrading from a Previous Release" for information that applies to this step.

To set up an interface between CA Deliver and CA View, run the SARINIT initialization utility to add this initialization option to CA View:

```
EXPRESS=DB.HLQ
```

Note: For more information about how to execute SARINIT, see the *CA View Reference Guide* and the *CA View Installation Guide*.

Step 15: (Optional) Install User Exits and Authorization Tables

If this is a new installation, skip this step until you have thoroughly tested CA Deliver and are familiar with the product.

Upgrade Considerations

For each user exit that you have tailored you must update the new CA Deliver skeleton version and assemble it using the macros in CAI.CVDEMAC.

Note: For more information about how to upgrade, see the chapter "Upgrading from a Previous Release".

User Exits

CA Deliver contains several optional user exits, most of which can be modified. For more information about these exits, see the *Programming Guide*.

CAI.CVDEJCL contains USERMODs that are used to modify and install these exits.

Exits can also be installed outside of SMP using the NON-SMP JCL contained in CAI.CVDEJCL.

The exits and their USERMODs are as follows:

Exit Name	USERMOD	NON-SMP
RMOATHUX	BRNSATHX	BRNJATHX
RMOBPCUX	BRNSBPCX	BRNJBPCX
RMOBPTUX	BRNSBPTX	BRNJBPTX
RMODSCUX	BRNSDSCX	BRNJDSCX

Exit Name	USERMOD	NON-SMP
RMOFSSUX	BRNSFSSX	BRNJFSSX
RMOJ2XIT	BRNSJ2X	BRNJJ2X
RMOJCLUX	BRNSJCLX	BRNJJCLX
RMOOMSUX	BRNSOMSX	BRNJOMSX
RMOPRBUX	BRNSPRBX	BRNJPRBX
RMORECUX	BRNSRECX	BRNJRECX
RMORPTUX	BRNSRPTX	BRNJRPTX
RMORPUX	BRNSRPX	BRNJRPUX
RMORRQUX	BRNSRRQX	BRNJRRQX
RMOSMFUX	BRNSSMFX	BRNJSMFX
RMOSUBUX	BRNSSUBX	BRNJSUBX
RMOUSRUX	BRNSUSRX	BRNJUSRX
RMOUSTUX	BRNSUSTX	BRNJUSTX
RMOUSXUX	BRNSUSXX	BRNJUSXX

Use USERMOD BRNSFSSX in CAI.CVDEJCL to modify user exit RMOFSSUX. However, RMOFSSUX must be assembled and linked outside of SMP.

Note: For more information about the JCL needed to install this exit, see the *Programming Guide*.

Authorization Tables

You can define a separate authorization table for each CA Deliver database.

Note: For more information about how to define and install the authorization tables, see the *Reference Guide.*

Step 16: (Optional) Install Optional Online Interfaces

Perform this step if you want to install any of the optional online interfaces; otherwise go to the next step.

Note: For more information about how to install optional online interfaces, see the chapter "Installing Online Interfaces."

Step 17: (Optional) Install Optional Features

Perform this step if you want to install any of the optional features; otherwise go to the next step.

Note: For more information about how to install optional features, see the chapter "Installing Features."

Upgrade Considerations

If you are upgrading, see the "Upgrading from a Previous Release" chapter for information about this step.

Chapter 6: Migration Information

This section contains the following topics:

Migration Considerations

This section contains the information that is required to upgrade to CA Deliver Release 12.2 from CA Deliver Release 12.1, Version 12.0, and Release 11.7.

For an overview of the changes in this release, see the *Release Notes*.

Upgrading from Previous Releases

Use these instructions to upgrade to CA Deliver Release 12.2 from CA Deliver Release 11.7, Version 12.0, or Release 12.1. The instructions consist of the original steps and a series of modifications.

To upgrade to Release 12.2, use the steps in these chapters:

- "Installing Your Product Using CA CSM", "Installing Your Product From Pax-Enhanced Electronic Software Delivery", or "Installing Your Product From DVD"
- "Configuring Your Product"
- "Installing Online Interfaces,"
- "Installing Features"

The steps must be modified according to the supplementary instructions in the tables in the following sections:

- Installation Steps to Upgrade to Release 12.2
- Configuration Steps to Upgrade to Release 12.2

Be aware that existing users are going to install the product using almost the same methods, as new users, with one exception—instead of creating a database you are going to version your existing database. This process updates several records in the database and is expected to execute in a few minutes.

Before upgrading your CA Deliver database, be certain that:

- The started task from the previous release has been withdrawn from the system by one of these methods:
  - The F RMOSTC,OFF operator command has been entered
  - An initial program load of the system was performed
- All application jobs containing reports that are distributed by CA Deliver are completed before CA Deliver Release 12.2 is started.
- All bundles have been completed.

Important! Failure to follow these procedures can result in lost bundles and abends in your application jobs.

Note: To revert to Release 12.1, Version 12.0, or Release 11.7, see the chapter *Reverting to a Previous Installation*.

Installation Steps for Upgrading to Release 12.2

To upgrade to Release 12.2, you must perform each installation step exactly as it is presented in the appropriate Installation chapter, unless the step has upgrade instructions in the table that follows.

The Step column lists the installation step in the chapter "Installation" and the Upgrade Instructions column explains what you must do to modify or replace the step.

Installation Step	Supplementary Upgrade Instructions
Step BRN1HOLD	No supplementary instructions.
Step BRN2ALL	Comment out or delete the allocations for any existing libraries. If you are upgrading from Release 11.7 Version 12.0, or Release 12.1, and the panel libraries are sufficiently allocated, skip this step.

Installation Step	Supplementary Upgrade Instructions
Step BRN3CSI	Comment out or delete the allocations for any libraries that already exist. Comment out or delete the step that creates the CSI. If you are upgrading from Release 11.7, Version 12.0, or Release 12.1, comment out or delete the DDDEF statements for SYSPUNCH (three occurrences). Change all ADD statements to REP statements. Condition code 04 is acceptable. **Note:** The default middle level qualifier name of the SMP/E CSI was removed beginning with Release 11.6. If you are upgrading from a previous release, ensure that the correct, complete name of your CSI is specified in the PARM= on the execute card.
Step BRN4RECD, BRN5APP, BRN6ACC	No supplementary instructions. **Note:** The default middle level qualifier name of the SMP/E CSI has been removed beginning with Release 11.6. If you are upgrading from a previous release, be sure that the correct, complete name of your CSI is specified in the PARM= value on the execute card.

Configuration Steps to Upgrade to CA Deliver Release 12.2 without CA CSM

To upgrade to Release 12.2, you must perform each installation step exactly as it is presented in the "Configuring Your Product" chapter unless the step has upgrade instructions in the table that follows.

The Step column lists the installation step in the "Installation" chapter and the Upgrade Instructions column explains what you must do to modify or replace the step.

Step	Upgrade Instructions
Steps 1-2	No supplementary instructions
Step 3	Define Security Rules If you modified the RMOATHUX authorization user exit or installed authorization tables, copy your changes into to the new CA Deliver skeleton version and assemble them in Step 15. If you have external security rules, review the "Security" chapter in the *Reference* Guide to determine if new security rules are necessary.

Step 4	Optionally, set the version of your database up to Release 12.2. Release 12.2 provides full compatibility with Release 11.7, Version 12.0, and Release 12.1 databases. If you want to utilize specific Release 12.2 features the database must be upgraded to Release 12.2. **Note:** If you do not want to upgrade your Release 11.7, Version 12.0, or Release 12.1 database, skip this step. This step replaces the Create the Database step in the chapter "Installation." Be aware of the following: ■ Instead of creating a CA Deliver database, you use the VERSION control statement of the RMODBASE utility to version your database to Release 12.2. You can tailor and submit CAI.CVDEJCL(HBRNVERS). ■ The high-level name of the database must have been previously defined with the NAME control statement (or the PARM parameter of the EXEC JCL statement) for the RMODBASE utility. The format of the VERSION control statement is: Release 12.2 For more information, see the RMODBASE Utility section in the chapter "Database Utilities" in the *Reference Guide*. **Note:** Save your initialization parameter settings; some parameter settings have been added or eliminated in Release 12.2, and you may need the original settings if you have to revert to a previous release.
Step 5	Create the Initialization Parameter Statements Follow the instructions in the "Installation" chapter. Some initialization parameters have been added, changed, or eliminated in Release 12.2. Be sure to review the initialization parameters presented in the chapter "Initialization Parameters" in the *CA Deliver Reference Guide.* For information about all initialization parameter changes, see the *CA Deliver Release Notes*. Save a copy of your initialization parameters in case you have to revert to a previous release.
Step 6	No supplementary instructions

Step 7	Load Online Panels and the JCL Library ■ If online panel members are customized in previous releases, copy those members to the appropriate Release 12.2 online library. ■ If the customized panels are maintained in a separate library, load those online panel members after loading the Release 12.2 panel members to the database. Follow the instructions in the "Installation" chapter and load the online panels to the database. Because some online panels have changed, you must OLOAD the new panels. **Important!** Only perform the OLOAD of the new panels if the database has been versioned to Release 12.2.
Step 8	Load the Model Banner Pages ■ If model banner page members were customized or added in previous releases, copy those members to the Release 12.2 model banner page library. ■ If the customized banner pages are maintained in a separate library, load those banner page members after loading the Release 12.2 banner page members to the database. Follow the instructions in the "Installation" chapter and load the model banner panels to the database.
Step 9	Add the Start Procedure to PROCLIB Follow the instructions in the "Installation" chapter and add or adjust the start procedure in the PROCLIB. Be sure that STEPLIB points to the new CAI.CVDELOAD.
Steps 10-11	No supplementary instructions
Step 12	Set Up for Multiple CPUs Follow the instructions in the chapter "Installation." If you use a system integrity product, make the changes needed to accommodate the new CA Deliver database. **Note:** There have been no changes to the way previous releases interact with products of this type, so changes must be minimal. Be aware of the following: ■ No active tasks can be running that point to the CVDELOAD and database that are being upgraded. ■ If multiple versions of CA Deliver are running on multiple CPUs and share the same database, all PROCs, JCL, CLISTS, and so forth, that access a given CA Deliver database must also be upgraded.
Step 13	No supplementary instructions

Step 14	Set up the Viewing Interface Skip this step if the Deliver databases have already been defined to CA View.
Step 15	Replace or Modify User Exits (Optional) If you modified any of the CA Deliver user exits perform this step; otherwise, go to the next step. Note the following: ■ For each user exit that you tailored in previous releases, copy your changes to the new CA Deliver skeleton version and assemble it. ■ All modifications to these exits must be done as an SMP/E USERMOD with the load module installed into CVDELOAD. ■ For your convenience, CVDEOPTN members are provided for all of the user exits. Save a copy of your user exits in case you need to revert to a previous release. For more information about user exits, see the chapter "User Exits" in the *Programming Guide*.
Step 16	No supplementary instructions
Step 17	Install Optional Features (Optional) Review the chapter "Installing Features". Verify that the LMP key has been supplied for each feature that you want to install (see the Enter the LMP Code step in the "Installation" chapter), then follow the installation instructions in the chapter "Installing Features." Be sure that all STEPLIB statements in your JCL reference the new CAI.CVDELOAD. There has been a minor change to cross-memory (one of the CA Deliver optional features):The cross-memory task program name has been changed to EC2DRV. Any JCL that contains the earlier release names, must be changed to EC2DRV. For more information about installing cross-memory services, see the "Installing Online Interfaces" chapter.

Chapter 7: Reverting to a Previous Installation

This section provides the instructions to use to revert to Release 12.1, Version 12.0, or Release 11.7

This section contains the following topics:

Revert Considerations

Versioning of the CA Deliver database from release level 12.2 to a previous release will convert dynamic report definitions to basic reports. The dynamic report variable and distribution specifications will also be removed from the report definition. After the versioning process, these report definitions must be reviewed and new distribution requirements must be added to the report definition.

To identify the dynamic report definitions that will be affected, run RMOGRW release 12.2 with the following control statements before versioning the database.

```
/CONTROL DATABASE=DELIVER.SYSTEM1
/SELECT RTYPE = 'D'
/PRINT RID 'DYNAMIC REPORTS' COL(1)
```

The RMOGRW report will identify all dynamic report definitions, if any, that need to be reviewed and changed after versioning.

Another consideration with versioning from release level 12.2 to a previous release is the use of generic bundle distribution identifiers in bundle definitions. The versioning process does not remove generic bundle distribution identifiers from the bundle definitions. These generic bundle distribution identifiers specifications must be changed to properly bundle reports with a previous release level.

To identify bundle definitions with contain generic distribution identifiers, run RMOGRW release 12.2 with the following control statements before versioning the database.

```
/CONTROL DATABASE=DELIVER.SYSTEM1
/DEFINE I BIN
/DO I = 1 TO 32 BY 1
/   IF SUBSTR(DISTID,I,1) = '*' THEN
/      PRINT BID 'BUNDLE IDENTIFIER' COL(1)
/      PRINT DISTID 'GENERIC DISTID'
/      BREAK
/   END
/END
```

The RMOGRW report identifies all bundle definitions, if any, that contain a generic bundle distribution identifier. These bundle definitions can be changed under release 12.2 before versioning the database or with the previous release after versioning.

The size of the checkpoint must be considered when versioning from CA Deliver r12.2 to a previous release, including the following:

- In prior releases, the maximum usable checkpoint size is 42 cylinders. In CA Deliver r12.2, the maximum checkpoint size is 200 cylinders.
- When determining whether to version to a previous release, the checkpoint will not be compatible if it was allocated using CA Deliver r12.2 and greater than 42 cylinders.
- If you decide to version to a previous release, and if the checkpoint is less than or equal to 42 cylinders, apply the released compatibility PTFs for prior versions of CA Deliver before restarting CA Deliver.
- To continue the versioning process with a checkpoint larger than 42 cylinders, the checkpoint must be resized using RMODBASE MAKECKPT to less than or equal to 42 cylinders.
- If the reversion is done with a checkpoint larger than 42 cylinders, the checkpoint dataset must be deleted and reallocated using the prior release.
- All the prior data from the larger 12.2 checkpoint will be lost.

Revert to Release 12.1

Follow these steps:

1. Use the CA Deliver Release 12.2 RMODBASE utility to set the version of your CA Deliver database back to a CA Deliver Release 12.1 database.

   The format of the VERSION control statement is:

   VERSION 12.1

2. Use the CA Deliver Release 12.2 RMODBASE utility to OLOAD the Release 12.1 online panel library into your database.
3. Use the CA Deliver Release 12.2 RMODBASE utility to BLOAD the Release 12.1 banner page library to your database.
4. If you modified any of the CA Deliver user exits, revert to your Release 12.1 versions of the exits.
5. Change your JCL, Procs, and started task JCL to point to the Release 12.1 libraries.
6. If the Release 12.2 load library was link listed, revert to the Release 12.1 link listed library.

Revert to Version 12.0

Follow these steps:

1. Use the CA Deliver Release 12.2 RMODBASE utility to set the version of your CA Deliver database back to a CA Deliver Version 12.0 database.

   The format of the VERSION control statement is:

   VERSION 12.0
2. Use the CA Deliver Version 12.0 RMODBASE utility to OLOAD the Version 12.0 online panel library into your database.
3. Use the CA Deliver Version 12.0 RMODBASE utility to BLOAD the Version 12.0 banner page library to your database.
4. If you modified any of the CA Deliver user exits, revert to your Version 12.0 versions of the exits.
5. Change your JCL, Procs, and started task JCL to point to the Version 12.0 libraries.
6. If the Release 12.2 load library was link listed, revert to the Version 12.0 link listed library.

Revert to Release 11.7

Follow these steps:

1. Use the CA Deliver Release 12.2 RMODBASE utility to set the version of your CA Deliver database back to a CA Deliver Release 11.7 database.

   The format of the VERSION control statement is:

   VERSION 11.7

2. Use the CA Deliver Release 11.7 RMODBASE utility to OLOAD the Release 11.7 online panel library into your database.
3. Use the CA Deliver Release 11.7 RMODBASE utility to BLOAD the Release 11.7 banner page library to your database.
4. If you modified any of the CA Deliver user exits, revert to your Release 11.7 versions of the exits.
5. Change your JCL, Procs, and started task JCL to point to the Release 11.7 libraries.
6. If the Release 12.2 load library was link listed, revert to the Release 11.7 link listed library.

Chapter 8: Installing Online Interfaces

This section contains the following topics:

How to Complete Configuration of the XMS Online Interfaces With CA CSM

These steps are configured automatically by the EBC Common Component Configuration Option:

- XMS Startup PROC
- Initialization Parameter Statements
- Modify, Assemble and Link of the EC2XMCTR Module
- Definition of Transactions and Programs to CICS

The EBC Common Component Configuration Option also includes several other external tasks that are required to complete the configuration.

Define Security Requirements

Follow these steps to define security requirements for CA Top Secret Security (eTrust CA Top Secret) security:

1. Rename the existing facility in the facility matrix table if you do not have a facility defined for RMOXMS:

   ```
   TSS MODIFY FACILITY(USERnn=NAME=RMOXMS)
   ```

   Note: The TSS MODIFY command is only valid until the next recycle of CA Top Secret. To make the change permanent, add the following to the CA Top Secret parameter file after the FACILITY(USERnn=NAME=RMOXMS) statement :

   ```
   FACILITY(USERnn=NAME=RMOXMS)
   ```

2. Verify that the correct PGMname is defined for the new facility, where PGMname is either the first three characters or all the eight characters of the program name that is going to make security calls (EC2 or EC2DRV).

   ```
   TSS MODIFY FACILITY(RMOXMS=PGM=EC2)
   ```

   Note: The TSS MODIFY command is only valid until the next recycle of CA Top Secret. To make the change permanent, add the following to the CA Top Secret parameter file:

   ```
   FACILITY(RMOXMS==PGM=EC2)
   ```

3. Create region ACID for the facility and add a master facility of the facility defined in Step 1:

   ```
   TSS CREATE(RMOXMS) PASSWORD(xxxx,0) TYPE(USER) DEPT(dept)
   ```

   ```
   TSS ADDTO(RMOXMS) MASTFAC(RMOXMS)
   ```

   We recommend that all started task (STC) acids be given a password and OPTIONS(4) be set in the CA Top Secret parameter file. OPTIONS(4) eliminates the prompt for a password when the STC starts, but if someone tries to signon with the STC acid, he will need to know the password.

   The region acid needs access to all resources accessed at startup.

   This access can be given by adding bypass attributes:

   TSS ADD(RMOXMS) NODSNCHK NOVOLCHK) or by permitting the specific resources

   TSS PERMIT(RMOXMS) DATASET(xxxx) ACCESS(access)).

   These resources include:

   - READ access to the XMS load library if pointing to this library in a STEPLIB concatenation.
   - READ access to any other libraries specified in the STEPLIB concatenation.
   - READ access to the SYSIN DD statement if it points to a dataset.
   - UPDATE access to the Deliver database.

   If any other DD statements (that is, SYSPRINT, RMOLOG, EBCUDUMP, SYSUDUMP, etc) in the XMS startup procs point to datasets instead of SYSOUT, READ access to these datasets is required.

4. Define the RMOXMS STC to the TSS STC record:

   ```
   TSS ADDTO(STC) PROCNAME(RMOXMS) ACID(RMOXMS)
   ```

5. Give access to the ACIDs required to sign on to this facility (from Step 1):

   ```
   TSS ADDTO(acid) FACILITY(RMOXMS)
   ```

   Where 'acid' is the user acid that needs access, an attached profile, or the ALL record if all users must have access.

Install the ISPF/Cross-Memory Online Retrieval Option

The ISPF/Cross-Memory Online Retrieval Option runs under IBM's ISPF for z/OS Version 3.0 and higher.

Important! This interface requires Cross-memory services to be already installed. For more information, see Install Cross-Memory Services in this chapter.

Note: In the JCL for the cross-memory services task, the parameter XMSSUB must be set to YES.

Installation Steps

The following steps are required to install the ISPF/cross-memory online retrieval option. Each step is explained in detail later in the sections that follow.

1. (Optional) Add STEPLIB DD statements to the TSO LOGON procedures if the load modules were not copied to a linklist library.
2. Add the panel and command table libraries to the TSO LOGON procedures.
3. (Optional) Modify an ISPF Selection Menu to Select Online Retrieval feature.

Step 1: (Optional) Add STEPLIB DD Statements to the TSO LOGON Procedures

The action you take in this step depends on what you did during the base-product installation—specifically, did you:

- Authorize the program load library, or
- Copy the modules to a system authorized library.

If the CA Deliver load modules were *not* copied to one of the libraries in the linklist, proceed with this step; otherwise go to the next step.

For this interface, the libraries do not have to be APF authorized. Authorization is provided in the cross-memory installation. Multiple versions of this online interface can coexist in one TSO library concatenation.

Do *one* of the following:

- Add a STEPLIB DD statement for the library that contains the load modules to the LOGON procedures for those TSO users who are going to use the ISPF/cross-memory online retrieval option.
- Provide the load library using the ISPF LIBDEF facility.

Note: If multiple versions of CA Deliver are going to be running simultaneously, or you want to also run a previous version of RMOSPF or RMOTSO, concatenate the load library you want RMOSPF or RMOTSO to use first.

More information:

Step 6: Modify the Skeleton JCL (see page 74)

Step 2: Add Panel and Command Table Libraries to TSO LOGON

If you are going to run CA Deliver under ISPF, proceed with this step. For Version 3 or higher, both the command table library and the panel library are used.

To add panel and command table libraries to the TSO LOGON procedure:

1. Concatenate the command table library CAI.CVDETBL0 to DD statement ISPTLIB.
2. Concatenate the panel library CAI.CVDEPNL0 to DD statement ISPPLIB.

Note: If you also plan to use RMOSPF (the ISPF interface), and multiple versions of CA Deliver, concatenate CAI.CVDETBL0 first. Use the CAI.CVDETBL0 from the most current release.

Step 3: (Optional) Modify an ISPF Selection Menu to Select Online Retrieval

If you want to add a selection code to one of the ISPF selection menus for the online retrieval feature, proceed with this step; otherwise, your ISPF detailed instructions are complete.

Note: If you add a selection code, you are able to select the online retrieval feature in the same way you select other ISPF options.

Use the value next to the NAME parameter on your Initialization Parameter Worksheet for PARM (high-level database name).

Use the values in this table for either SPF or ISPF.

Type	Selection Code is Defined As
ISPF (all versions)	'PGM(EC2XMSPF) PARM(high-level-database-name) NEWAPPL(RMO)'
SPF	'PGM(EC2XMSPF) PARM(high-level-database-name)'

Panel Libraries

The names of the panel libraries vary from site to site and for the different releases of ISPF. These panel libraries are allocated to the ISPPLIB DD statement under TSO.

Be aware that some installations do not allow direct modifications of IBM panels and libraries. In this case, you can place the modified panels in user or site-specific libraries and concatenate them ahead of the IBM libraries.

Ask your system administrator for the specific ISPF panel library that applies to your site and contains the panel ISR@PRIM.

Note: The selection menus shown in these examples are part of the program product ISPF and are copyrighted by IBM.

Example 1

This example shows you how to add selection code R to the primary option menu ISR@PRIM for ISPF. The bright, offset text identifies the inserted lines.

```
----------------------  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           +PF KEYS  - &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, CLIST, OR REXX EXEC
%   7 +DIALOG TEST - PERFORM DIALOG TESTING
%   8 +LM UTILITIES- PERFORM LIBRARY ADMINISTRATOR UTILITY FUNCTIONS
%   C +CHANGES     - DISPLAY SUMMARY OF CHANGES FOR THIS RELEASE
%   R +RMOSPF      - DELIVER ADMINISTRATION
%   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 /* TUTORIAL INDEX - 1ST PAGE         */
)PROC
  &ZSEL = TRANS( TRUNC (&ZCMD,'.')
               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(ISPYXDR) PARM(ISR) NOCHECK'
               8,'PANEL(ISRLPRIM)'
               C,'PGM(ISPTUTOR) PARM(ISR00005)'
               R,'PGM(EC2XMSPF) PARM(RMO.SYSTEM1) NEWAPPL(RMO)'
               T,'PGM(ISPTUTOR) PARM(ISR00000)'
              ' ',' '
                X,'EXIT'
                *,'?' )
   &ZTRAIL = .TRAIL
 )END
```

Note:

- NEWAPPL(RMO) is required and must be specified as shown previously in this section.

  This parameter is used with the command table library concatenation from Step 3 of the ISPF Installation Instructions.

- NEWAPPL(RMO) allows CA Deliver to correctly interpret commands and program function key invocation.

  If this parameter is not specified, certain PF keys such as the scroll keys may not function.

Example 3

This example shows you how to add selection code R to the primary option menu ISP@PRIM for SPF. Shading identifies the inserted lines.

```
%----------------------  SPF—MVS PRIMARY OPTION MENU  ---------------
%OPTION  ===>_OPT
%                                                              +USERID   -
%   0 +ISPF PARMS  -     SPECIFY TERMINAL AND USER PARAMETERS   +TIME     -
%   1 +BROWSE      -     DISPLAY SOURCE DATA OR OUTPUT LISTINGS +TERMINAL —
%   2 +EDIT        -     CREATE OR CHANGE SOURCE DATA           +PF KEYS  -
%   3 +UTILITIES   -     PERFORM SPF UTILITY FUNCTIONS
%   4 +FOREGROUND  -     COMPILE, ASSEMBLE, OR DEBUG
%   5 +BACKGROUND  -     COMPILE, ASSEMBLE, OR LINK EDIT
%   6 +COMMAND     -     ENTER TSO COMMAND OR CLIST
%   7 +SUPPORT     -     TEST DIALOG OR CONVERT MENU/MESSAGE FORMATS
%   8 +LM UTILITIES-     PERFORM LIBRARY ADMINISTRATOR UTILITY FUNCTIONS
%   R +RMOSPF      -     DELIVER ADMINISTRATION
%   T +TUTORIAL    -     DISPLAY INFORMATION ABOUT SPF
%   X +EXIT        -     TERMINATE SPF USING LIST/LOG DEFAULTS
%
+PRESS%END KEY TO TERMINATE SPF+
%
)INIT
  .HELP = TTUTOR
  &ZHTOP = TTUTOR   /* TUTORIAL TABLE OF CONTENTS        */
  &ZHINDEX = TINDEX /* TUTORIAL INDEX - 1ST PAGE         */
)PROC
  &ZSEL = TRANS( TRUNC (&OPT,'.')
               0,'PANEL(ISPOPT)'
               1,'PGM(ISRBRO)'
               2,'PGM(ISPEDIT)'
               3,'PANEL(ISPUTIL)'
               4,'PANEL(ISPFORA)'
               5,'PANEL(ISRJOB)'
               6,'PGM(ISPTSO)'
               7,'PANEL(ISPOTAC)'
               R,'PGM(EC2XMSPF) PARM(RMO.SYSTEM1)'
               T,'PGM(ISPTUTOR) PARM(T)'
               ' ',' '
                X,'EXIT'
                *,'?' )
 )END
```

Example 3

This example shows you how to add selection code 3.R as a sub-option to the utilities menu ISPUTIL for ISPF.

The bright, offset text identifies the inserted lines.

```
     %-----------------------  UTILITY SELECTION MENU  -----------------
%OPTION  ===>_OPT         +
%                                                                      +
%   1 +LIBRARY        LIBRARY UTILITY:
+                     PRINT INDEX LISTING OR ENTIRE DATASET
+                     PRINT, RENAME, DELETE, OR BROWSE MEMBERS
+                     COMPRESS DATASET
%   2 +DATASET        DATASET UTILITY:
+                     DISPLAY DATASET INFORMATION
+                     ALLOCATE, RENAME, OR DELETE ENTIRE DATASET
+                     CATALOG OR UNCATALOG DATASET
%   3 +MOVE/COPY      MOVE OR COPY MEMBERS OR DATASETS
%   4 +CATALOG        CATALOG MANAGEMENT:
+                     DISPLAY OR PRINT CATALOG ENTRIES
+                     INITIALIZE OR DELETE USER CATALOG ALIAS
%   5 +RESET          RESET STATISTICS FOR MEMBERS OF ISPF LIBRARY
%   6 +HARDCOPY       INITIATE HARDCOPY OUTPUT
%   7 +VTOC           DISPLAY OR PRINT VTOC ENTRIES FOR A DASD VOLUME
%   8 +OUTLIST        DISPLAY, DELETE, OR PRINT HELD JOB OUTPUT
%   9 +SCRIPT/VS      FORMAT, DISPLAY, AND OPTIONALLY PRINT SCRIPT TEXT
%   R +RMOSPF         DELIVER ADMINISTRATION
)INIT
  .HELP = TU
)PROC
  &SEL = TRANS( TRUNC (&OPT,'.')
                1,'PGM(ISPUDA) PARM(UDA1)'
                2,'PGM(ISPUDA) PARM(UDA1)'
                3,'PGM(ISPUMC)'
                4,'PGM(ISPUCA)'
                5,'PGM(ISPURS)'
                6,'PGM(ISPUHC)'
                7,'PGM(ISPUVT)'
                8,'PGM(ISPUOL) PARM(UOL01)'
                9,'PGM(ISPUSC) PARM(SCRPTA)'
                R,'PGM(EC2XMSPF) PARM(RMO.SYSTEM1) NEWAPPL(RMO)'
               ' ',' '
                 *,'?' )
 )END
```

ISPF Cross-Memory Notes

Be aware of the following:

- The primary RMOXMS region must be started with the XMSSUB=YES parameter.
- The XMSSUB=YES parameter must only be used in an XMS address space with a default subsystem ID (SUBSYS=XMC2 or not specified).
- If multiple RMOXMS regions are started, they must be started with XMSSUB=NO parameter.

  Only the primary XMS region can have XMSSUB=YES specified.
- The XMS regions must have the XMS=YES parameter to make it accessible.
- The EBCXMCTR table must be assembled during installation to define the relationship between CA Deliver and CA View database high-level qualifiers. The table contains an EBCXMOPT macro to define initialization options and the EBCXMTRN macro for each CICS user transaction.

The EBCXMTRN macro also contains options for the specific database as follows:

- SUBSYS= parameter of the cross-memory task must match the SUBSYS= parameter specified in the EBCXMCTR table entry.
- RECON=YES can be used to allow reconnection (after an ISPF terminal error) at the point of exit.
- TIMEOUT= specifies how long ISPF will wait for the XMS session to respond after the user enters input, in seconds.

  We recommend as high a value as possible but not less than 240 (4 minutes).

To abort the XMS session and return the user to ISPF or the TSO command prompt, press the ATTN key.

Note: The SUBMAX= parameter controls the number of user connections, not the USERMAX= parameter. USERMAX= only applies when you are using the subtask with the CICS interface.

Install the TSO/Cross-Memory Online Retrieval Option

Important! This interface requires cross-memory services to be installed. For more information, see the topic Installing Cross-Memory Services in this chapter.

Note: The parameter XMSSUB must be set to YES in the JCL for the cross-memory services task.

Installation Steps

The following steps are required to install the TSO/Cross-Memory Online Retrieval Option. Each step is explained in detail in the sections that follow.

1. (Optional) Add STEPLIB DD Statements to the TSO LOGON procedures if the load modules were not copied to a linklist library.
2. (Optional) Create user CLISTs to execute the CA Deliver TSO/XMS driver program.

Step 1: (Optional) Add STEPLIB DD Statements

The action you take in this step depends on what you did during the base-product installation—specifically, did you:

- Authorize the program load library or
- Copy the modules to a system authorized library

If the CA Deliver load modules were *not* copied to one of the libraries in the linklist, proceed with this step; otherwise go to the next step.

To add STEPLIB DD statements (for the library containing the CA Deliver load modules) to the TSO LOGON procedures, do the following:

- Add a STEPLIB DD statement for the library that contains the CA Deliver load modules to the LOGON procedures for those TSO users who are to use the ISPF/Cross-Memory Online Retrieval Option.

Note: For this interface, the libraries do not have to be APF authorized—authorization is provided in the cross-memory installation. Multiple releases of this online interface can coexist in one TSO library concatenation.

Step 2: (Optional) Set up the TSOXMS Driver Program

To create user CLISTs to execute the CA Deliver TSOXMS driver program, issue:

```
EC2XMTSO highlevel.databasename
```

TSO Cross-Memory Notes

Be aware of the following:

- The primary RMOXMS region should be started with the XMSSUB=YES parameter.
- The XMSSUB=YES parameter must only be used in an XMS address space with a default subsystem ID (SUBSYS=XMC2 or not specified).
- If multiple RMOXMS regions are started, they must be started with XMSSUB=NO parameter.

  Only the primary XMS region can have XMSSUB=YES specified.
- The XMS regions must have the XMS=YES parameter to make it accessible.
- The EBCXMCTR table must be assembled during installation to define the relationship between CA View and CA Deliver database high-level qualifiers. The table contains an EBCXMOPT macro to define initialization options and the EBCXMTRN macro for each CICS user transaction.

The EBCXMTRN macro also contains options for the specific database as follows:

- SUBSYS= parameter of the cross-memory task.

  This parameter must match the SUBSYS= parameter specified in the EBCXMCTR table entry.
- RECON=YES can be used to allow reconnection (after a TSO terminal error) at the point of exit.
- TIMEOUT= specifies how long TSO will wait for the XMS session to respond after the user enters input, in seconds.

  We recommend as high a value as possible but not less than 240 (4 minutes).

To abort the XMS session and return the user to ISPF or the TSO command prompt, press the ATTN key.

Note: The SUBMAX= parameter controls the number of user connections, not the USERMAX= parameter. USERMAX=only applies when you are using the subtask with the CICS interface.

Install the VTAM Online Retrieval Option

Important! This facility uses the cross-memory feature distributed with CA Deliver and must be installed with that feature. For more information about cross-memory feature, see the Install Cross-Memory Services section in this chapter.

Installation Steps

The following steps are required to install the VTAM online retrieval option. Each step is explained in detail in the sections that follow.

1. Define the APPL definition statement to VTAM.
2. (Optional) Create a USS Table Definition.

Step 1: Define the Application Program to VTAM

Add this application program definition to SYS1.VTAMLST:

```
* SYS1.VTAMLST(rmomajor)
rmomajor VBUILD TYPE=APPL
rmovtam  APPL  ACBNAME=rmovtam,AUTH=(PASS,ACQ),EAS=nn
```

where:

rmomajor

Specifies the application program major node name.

Use the SYS1.VTAMLST member name. The member name must be unique and must not be the same as the names on the APPL statement.

AUTH=(PASS,ACQ)

Is required when the cross-memory parameter VTAMPASS=YES is used to support multiple cross-memory regions.

If VTAMPASS=NO, you can specify AUTH=(ACQ). For more information about the VTAMPASS parameter, see the Add the Start Procedure for the Cross-Memory Online Task step in this chapter.

EAS=nn

Specifies the approximate number of concurrent sessions.

rmovtam

Specifies the minor node name of the application program.

- This name must be unique within the network domain; it is the APPLID referenced in the USS definition table or LOGON command.
- This name is also specified on the cross-memory RMOAPPL parameter.
- If not specified, the network-unique name (the name of the APPL definition statement) is used.

Step 2: (Optional) Create a USS Table Definition

To simplify the manner in which a user logs on to VTAM online retrieval, you can create a USS definition table for CA Deliver.

Example

Assume that two CA Deliver systems have been created. The databases for the two systems have high-level names of RMO.SYSTEM1 and RMO.SYSTEM2, and you want a user to simply enter one of the commands to log on to VTAM online retrieval for the respective systems:

```
RMO1
RMO2
```

Create a USS definition table as follows:

```
USSTAB
*
*    ENTRY FOR RMO1
*
USSCMD  CMD=RMO1,REP=LOGON,FORMAT=PL1
USSPARM PARM=APPLID,DEFAULT=RMOVTAM
USSPARM PARM=LOGMODE
USSPARM PARM=DATA,DEFAULT=RMO.SYSTEM1
*
*    ENTRY FOR RMO2
*
USSCMD  CMD=RMO2,REP=LOGON,FORMAT=PL1
USSPARM PARM=APPLID,DEFAULT=RMOVTAM
USSPARM PARM=LOGMODE
USSPARM PARM=DATA,DEFAULT=RMO.SYSTEM2
USSEND
```

VTAM Cross-Memory Notes

Be aware of the following:

- For VTAM only regions, you can start the primary RMOXMS task with the XMSSUB=NO parameter. However if this is not a VTAM only region, we recommend that you start the primary RMOXMS region with the XMSSUB=YES parameter.
- If multiple RMOXMS regions are started, they must be started with XMSSUB=NO parameter.

  Only the primary XMS region can have XMSSUB=YES specified.
- VTAM only XMS regions can have the XMS=NO parameter to make it accessible.
- All XMS interfaces require the EC2XMCTR table. You must assemble the table during installation to:
  - Define the relationship between CA Deliver and CA View database high-level qualifiers and the session options to be used
  - Provide information used to build the XMS database table. Only the database high-level qualifier is used for VTAM XMS users.
- Specify the RMOAPPL=*applid* parameter. This parameter provides VTAM user signon capability.

  Note: When you are using multiple VTAM XMS regions, each region must have a unique *applid*.
- To pass VTAM signon requests to other XMS regions, specify the VTAMPASS=YES parameter.
- When you are using multiple VTAM XMS regions, the values for LGNFMT=, RMOVDTB=, VTMQUERY=, and VTMSAA= must be the same in each region. Otherwise, the XMS interface may react in unpredictable ways.
- To activate the VTAM generic resource support for your cross memory regions, specify the VGRAPPL= parameter.

  Note: For more information about VTAM generic resources, see the following topic.

VTAM Generic Resource Name

If the VGRAPPL parameter is specified in an EMAS complex, this parameter specifies a common VTAM generic resource name for the entire EMAS complex.

Specifying the common VTAM generic resource name in the session request can initiate VTAM cross memory sessions to any of the EMAS members.

When you are using the VTAM generic resource name, by default VTAM tries to request a session with an EMAS member in the same MVS image.

If it is not possible to get the session that was requested, VTAM uses normal load balancing when passing the session request to one of the active EMAS members.

Install the CA Roscoe/Cross-Memory Online Retrieval Option

The CA Roscoe/cross-memory online retrieval option runs as a command processor under ETSO/Roscoe.

Important! This interface requires cross-memory services to be installed. For more information about cross-memory services, see the Install Cross-Memory Services section in this chapter. Be sure to set the parameter XMSSUB to YES in the JCL for the cross-memory services task.

Installation Steps

The following steps are required to install the CA Roscoe/Cross-Memory Online Retrieval Option. Each step is explained in detail in the sections that follow.

1. (Optional) Concatenate the Load Module Library to the ETSOLIB DD statement, if the load modules were not copied to a linklist library.
2. Add the control statement for the RMOROS command processor to the Eligible Program List (EPL).
3. Invoke CA Roscoe/Cross-Memory Online Retrieval.

Step 1: (Optional) Concatenate the Load Module Library

If the load modules were *not* copied to a linklist library, concatenate the library that contains the load modules to the ETSOLIB DD statement in the CA Roscoe startup JCL, .

Note: If you have CA View, the CA View load modules must also be either in the linklist or in a ETSOLIB statement with this step.

Step 2: Add RMOROS Command Processor Statements

Important! This step is for CA Roscoe 6.0 and Higher.

Add these EPL control statements to member ETSOPGMS for the CA Roscoe user with the RO prefix:

Column	Contents
1–8	EC2XMROS
9	Blank
10–12	Number of users allowed to access CA Deliver at one time
13	Blank
14–17	CPU time slice (use 9999 to prevent premature termination)
18	Blank

Column	Contents
19–24	Maximum memory (in KB) below the 16 MB line This memory is only for the cross-memory driver program (50 KB is ample)
25	Blank
26–31	Maximum memory (in KB) below the line that CA Deliver can acquire at one time Use 999999 so that GETMAINs are not limited
32	Blank
33–38	Maximum memory (in KB) above the 16 MB line This memory is only for the cross-memory driver program (50 KB is ample)
39	Blank
40–45	Maximum memory (in KB) above the line that CA Deliver can acquire at one time Use 999999 so that GETMAINs are not limited
46	Blank
47–48	CP to call EC2XMROS as a TSO command processor
49	Y – Application authorized to issue MODESET SVC
50	Blank
51-52	CP to call EC2XMROS as a TSO command processor
53-255	Ignored

CA Roscoe Cross-Memory Notes

Be aware of the following:

- Start the primary RMOXMS region with the XMSSUB=YES parameter.

  The XMSSUB=YES parameter must only be used in an XMS address space with a default subsystem ID (SUBSYS=XMC2 or not specified).

- If multiple RMOXMS regions are started, they must be started with XMSSUB=NO parameter.

  Only the primary XMS region can have XMSSUB=YES specified.

- The XMS regions must have the XMS=YES parameter to make it accessible.

- The EBCXMCTR table must be assembled during installation to define the relationship between CA View and CA Deliver database high-level qualifiers.

  The table contains an EBCXMOPT macro to define initialization options and the EBCXMTRN macro for each CICS user transaction.

The EBCXMTRN macro also contains options for the specific database as follows:

- SUBSYS= parameter of the cross-memory task.

  This parameter must match the SUBSYS= parameter specified in the EBCXMCTR table entry.

- RECON=YES can be used to allow reconnection (after a TSO terminal error) at the point of exit.

- TIMEOUT= specifies how long TSO is to wait for the XMS session to respond after the user enters input, in seconds.

  We recommend as high a value as possible but not less than 240 (4 minutes).

Note: The SUBMAX= parameter controls the number of user connections, not the USERMAX= parameter. USERMAX=only applies when using the subtask with the CICS interface.

Install the CICS Pseudo-Conversational Option

Important! This option uses the cross-memory feature distributed with CA Deliver and must be installed with that feature. For more information about cross-memory, see Install Cross-Memory Services.

Installation Steps

The following steps are required to install the CICS Pseudo-Conversational Option. Each step is explained in detail in the sections that follow.

1. Place the CA Deliver load libraries into DFHRPL and STEPLIB.
2. Code the PCT and PPT Table Entries to CICS.
3. (Optional) Prepare the interface to a user-written CICS menu system.

Step 1: Add Modules to DFHRPL and STEPLIB

The CA Deliver load library is required in the CICS DFHRPL and in the STEPLIB in the CICS region.

Note: If the CAI.CVDELOAD load library is in the linklist, it does not have to be included as a STEPLIB in the CICS region

Be sure that these modules are available in the DFHRPL concatenation of libraries.

1. EC2CICUX
2. EC2CIEND
3. EC2CINIT
4. EC2CISRV
5. EC2XMCIC
6. EC2C*version-number*

   Where:

   release-number represents the CICS release number.

   - CTS 3.1 release number: 0640
   - CTS 3.2 release number: 0650
   - CTS 4.1 release number: 0660
   - CTS 4.2 release number: 0670
   - CTS 5.1 release number: 0680
   - CTS 5.2 release number: 0690

You can copy the six modules to the DD statement DFHRPL in your CICS task. However, we strongly recommend that you concatenate CAI.CVDELOAD to the DD statement DFHRPL.

Note: Several CA Deliver modules are loaded (MVS load) from the CICS STEPLIB or LINKLIST. Verify that the entire CA Deliver load library is defined in the CICS STEPLIB or is included in the linklist.

Step 2: Code the PCT and PPT Table Entries to CICS

The CICS transactions and programs were previously defined in the CSM configuration step. Review the following points to determine if they are applicable to your installation.

CICS Resource Definition Online Storage Protection

If you have CICS storage protection activated, resource definition online settings are required, as follows:

- For all transactions:

  ```
  TASKDATALOC=ANY
  TASKDATAKEY=CICS
  ```

- For all programs:

  ```
  DATALOCATION=ANY
  EXECKEY=CICS
  ```

PLT Start-up List

Add these table entries to the last phase of the PLT startup list to initialize the subtask that is used for cross-memory access:

```
DFHPLT TYPE=ENTRY,PROGRAM=DFHDELIM
DFHPLT TYPE=ENTRY,PROGRAM=EC2CINIT
```

PLT Shutdown List

Add these table entries to the first phase of the PLT shutdown list to ensure that the subtask that executes as part of the CA Deliver online facility correctly shuts down when CICS shuts down:

```
DFHPLT TYPE=ENTRY,PROGRAM=EC2CIEND
DFHPLT TYPE=ENTRY,PROGRAM=DFHDELIM
```

Optional DCT Entries

Specify a value for the DESTID parameter in the EBCXMOPT macro in the EC2XMCTR module and corresponding DCT entries. This value defines a transient data destination for messages issued by the subtask.

Note: Specify a blank for DESTID to suppress the generation of informational messages from the subtask.

The DCT entries for a DESTID of XMC2 are:

```
RMOLOG   DFHDCT TYPE=SDSCI,   FOR CICS MESSAGES AND SHUTDOWN
               BLKSIZE=250,   STATISTICS
               BUFNO=1,
               DSCNAME=RMOLOG,
               RECFORM=VARUNBM,
               RECSIZE=242,
               TYPEFLE=OUTPUT
XMC2G    DFHDCT TYPE=EXTRA,
               DESTID=XMC2,
               DSCNAME=RMOLOG
```

Step 3: (Optional) Invoke the System from a CICS Menu System

If you want to invoke CA Deliver from a user-written CICS menu system, then return to that menu system when you exit from CA Deliver, do the following:

Invoke CA Deliver from the menu system by using this CICS command:

```
EXEC CICS START TRANSID(DELIVER transaction-id)
     TERMID(EIBTRMID)
     FROM(data-area)
     LENGTH(4)
```

where:

TRANSID(DELIVER transaction-id)

Specifies the CA Deliver transaction ID.

TERMID(EIBTRMID)

Specifies the terminal that a CA Deliver transaction will communicate with.

FROM (data-area)

Specifies the optional variable length character string.

The format of the data-area parameter is:

tran,

where:

tran

Specifies the return menu CICS transaction to be started when CA Deliver finishes.

Note: None of the data-area parameters is required.

LENGTH (4)

Specifies the number of bytes in the data field being passed.

Note:

When CA Deliver receives control, it retrieves the four-byte return transaction ID and saves it from iteration to iteration.

If the retrieve fails, CA Deliver retains the information that it was started directly from a terminal, not a menu system.

When CA Deliver finishes processing, it determines whether it should return to a menu system by starting the return transaction.

If there is a saved transaction ID, CA Deliver starts the return transaction before it exits to CICS by issuing:

```
EXEC CICS START TRANSID(RETURN transaction-id)
     TERMID(EIBTRMID)
     NOCHECK
```

CICS Notes

The cross memory CICS access involves two different address spaces: the CICS address spaces and the XMS address spaces.

CICS Address Spaces

The user's CICS transactions and the cross memory support subtask reside in the address spaces.

- If multiple CICS regions are used to access CA Deliver, each CICS region will have an XMS support subtask.
- If you are using CICS/MRO, CA Deliver normally runs in an AOR (application region).

XMS Address Spaces

Be aware of the following:

- The primary RMOXMS region can be started with the XMSSUB=YES or XMSSUB=NO parameter.
- CICS has a router subtask in its region and does not require the XMSSUB=YES function. However, we recommend that you start the primary XMS region with XMSSUB=YES.
- If multiple RMOXMS regions are started, they must be started with XMSSUB=NO parameter.

  Only the primary XMS region can have XMSSUB=YES specified.
- The XMS regions must have the XMS=YES parameter to be accessible.
- The SUBSYS= parameter must match the EC2XMCTR table entry for the CICS transaction.

- The EBCXMCTR table must be assembled during installation to define the relationship between CA View and CA Deliver database high-level qualifiers.

  The table contains an EBCXMOPT macro to define initialization options and the EBCXMTRN macro for each CICS user transaction.

The EBCXMTRN macro also contains options for the specific database as follows:

- SUBSYS= parameter can be used to route the CA Deliver transaction to an alternate XMS subsystem ID. The SUBSYS= of the cross memory task must match the SUBSYS= parameter specified in the EBCXMCTR table entry.
- TRANID=parameter specifies the CA Deliver transaction identifier for CICS.
- RECON=YES can be used to allow reconnection (after a CICS terminal error) at the point of exit.

  Note: Do not specify RECON=YES if you use a multi-session manager that assigns LU names from a pool of names. Coding RECON=YES under these conditions could allow a user to be connected to another user's session. For more information, see Multi-Session Managers later in this chapter.
- TIMEOUT= specifies how long CICS is to wait for the XMS session to respond after the user enters input, in seconds.

  We recommend as high a value as possible but not less than 240 (4 minutes).

CICS XMS Subtask Startup

Use *one* of these methods to start the XMS subtask automatically:

1. When the CICS region is started, use the DFHPLTPI definition to automatically start the XMS subtask.
2. Define a transaction for the EC2CINIT program to allow for manual startup.
3. Write a CICS program to transfer control (XCTL) to EC2CINIT when you want to start the XMS subtask.

Until the XMS subtask is started, expect the transactions referencing EC2XMCIC to terminate with an error message that indicates that the XMS subtask is not active.

Note:

- When the CICS region is terminated, the DFHPLTSD definition is to be used to terminate the XMS subtask.

  You can manually terminate the XMS subtask through a user application program that LINKs the EC2CIEND or you can use the optional transaction defined for EC2CIEND for manual termination.

- If you want to terminate the XMS subtask manually, we recommend that you use the DFHPLTSD entry to terminate the XMS subtask. This definition is needed to clean up linkages to the XMS address spaces.
- To prevent users from shutting down the XMS subtask, secure the optional transaction for program EC2CIEND.

Multi-Session Managers Using Virtual LU Names

Multi session manager products, for example CA TPX Session Management (CA TPX), can be configured to assign an LU name to a user's terminal at the time the user selects the CICS application.

Important! This assignment means that a user can enter CICS each time with a different terminal ID which can cause problems for CA Deliver application.

For example: If a user uses a multi-session manager to end a session, or shuts the PC down, CA Deliver does not know that the user has left. Another user might select CICS, be assigned to the same LU name as the previous user, and enter CA Deliver with the same terminal ID as the previous user. CA Deliver believes that there are two active users on the same terminal.

To prevent this situation, you can add a small amount of code to the CICS Autoinstall Control Program.

Note: The default name of this program is DFHZATDX and its source is located in SDFHSAMP.

If you are not a CICS systems programmer, discuss this situation with the person in your company who is responsible for CICS support and maintenance.

The sample code that follows shows how to clear an active user from the CA Deliver application at terminal deletion time. Insert this code in your Autoinstall Control Program.

The source that is shipped with CICS contains this line:

* ==> *PUT DELETE CODE HERE*

Insert the code after that line.

```
          LOAD  EP=EC2XSLOC,ERRET=RETURN
          LR    R6,R0                  GET EBCXSLOC ADDRESS
          ICM   R8,B'1111',0(R6)       ADDR OF MAIN CONTROL BLOCK
          BZ    RETURN                 GET OUT IF NONE
          LA    R7,4(,R8)              LOOK LIKE FIRST USER BLOCK
XSU_LOOP DS    0H
          ICM   R7,B'1111',8(R7)       USER BLOCK ADDR
          BZ    RETURN                 GET OUT IF DONE
          CLC   DELETE_TERM_ID,104(R7) FOR THIS TERMINAL?
          BNE   XSU_LOOP               NO
          TM    120(R7),X'01'          ACTIVE ENTRY?
          BZ    XSU_LOOP               NO
          OI    120(R7),X'02'          SHOW SESSION DONE
          B     RETURN                 EXIT PROGRAM
```

This code does the following:

1. Attempts to load program EC2XSLOC
   - If the load fails, this is not the region containing CA Deliver and it exits.
   - If CA Deliver is active in this region, the first word of EC2XSLOC contains the address of the main control block.

     If this word is zero, CA Deliver is not active and the program exits.
2. Scans the chain of CA Deliver user control blocks to find the terminal to be deleted
   - If the program finds the terminal ID, it makes sure that the user block is in use and is active, and then it clears the appropriate fields.
   - If the block does not represent an active user, the program continues to search the chain to the end.
   - If the program gets to the end of the chain without finding the terminal ID, the program exits.
   - If you implement this change to the terminal deletion section of the Autoinstall Control Program, you can prevent the problems caused by the methods that were used to leave the CA Deliver application.

Install the IMS Online Retrieval Option

Use these steps to install the IMS online retrieval option.

Important! This facility uses the cross-memory feature distributed with CA Deliver and must be installed with that feature. For more information about cross-memory, see Installing Cross-Memory Services.

Installation Steps

This list summarizes the steps required to install the IMS Online Retrieval Option. Detailed instructions are in the sections that follow.

1. Code the IMS TRANSACT, PSB and APPLCTN macros.
2. Run the PSB, ACB, and SYSGEN Procedures.
3. Load EC2IMSUX Modules.
4. Move load modules to IMSVS.PGMLIB.

Important! All JCL and macros provided in this section are provided as general examples only and must be modified for your site's systems and standards.

Step 1: Code the Macros

Use the examples in this section as a guide as you code these macros, and implement them in your IMS system.

- (IMS) TRANSACT macro
- PSB macros
- APPLCTN macro

TRANSACT Macro

One or more transactions must be defined for the IMS online retrieval program RMOXMIMS. Normally, only one transaction identifier is defined, although you can define multiple transactions.

This TRANSACT macro identifies the RMOXMIMS transaction to IMS:

```
TRANSACT NAME=EC2XMIMS,SPA=(18)
```

PSB Macros

This PSB must be generated for the EC2XMIMS transaction:

```
PCB       TYPE=TP,ALTRESP=YES,MODIFY=YES
PSBGEN    PSBNAME=EC2XMIMS,LANG=ASSEM,COMPAT=YES
```

APPLCTN Macro

This APPLCTN must be generated for the RMOXMIMS transaction:

```
APPLCTN    PSB=EC2XMIMS
```

Step 2: Run the PSB, ACB, and SYSGEN Procedures

Use the macros created in Step 1. Code the Macros as input for these procedures:

```
PSBGEN
ACBGEN
IMS SYSGEN
```

Step 3: Load EC1IMSUX Modules

Move load modules EC2IMSUX to IMSVS.PGMLIB.

Note: EC2IMSUX is in CAI.CVDELOAD and must be copied to IMSVS.PGMLIB.

IMS Notes (New Version)

Be aware of the following:

- The new IMS/DC Transaction Program (EC2XMIMS) is a replacement for the older RMOXMIMS program.
- The EC2XMIMS does not need to be linkedited to the ASMTDLI interface program. The transaction is now conversational with a SPASIZE=18 (this can be adjusted).
- If you use extended color, the SEGSIZE= may need to be increased, because extended color data streams can be a 50% increase over the monochrome data stream size.

  To determine the SEGSIZE= value, take the terminal that will use the interface with the largest screen size, in bytes, and apply this formula:

  ```
  ROWS * COLS * 1.5 = SEGSIZE
  ```

  For example, a 3278-5 with a 27 x 132 screen size would be (27 * 132 * 1.5) = 5346. If the SEGSIZE= is too small, the terminal user will get an RC= "A6" message indicating that a message insert failed.

IMS/DC Parameter Relationships

The cross-memory IMS/DC access involves up to three different address spaces as follows:

- IMS/DC message processing region address spaces

  The user's IMS/DC transaction resides here. If multiple IMS/DC users are processing concurrently (input being processed by the XMS system), a separate IMS/DC message region is used for each user.

  IMS/DC can control the maximum number of IMS/DC transactions executing at one time.

- The XMS support subtask
  - The subtask is started when the XMSSUB=YES input parameter is used when an XMS address space is started.
  - The subtask can be in a separate XMS address space or share the address space with XMS or VTAM sessions.
  - The XMSSUB=YES must only be used in an XMS address space with a default subsystem ID (SUBSYS=XMC2 or not specified).
  - If multiple XMS address spaces are started, only one can have the XMSSUB=YES specified.

  Note: All IMS/DC, TSO/XMS, ISPF/XMS and CA Roscoe/XMS sessions share the same XMS subtask.

- XMS address spaces

  See the topic that follows.

IMS/DC Cross-Memory Notes

Be aware of the following:

- The primary RMOXMS region is to be started with the XMSSUB=YES parameter.

  This region can be in a separate XMS address space or share the address space with XMS or VTAM sessions.

- The XMSSUB=YES parameter must only be used in an XMS address space with a default subsystem ID (SUBSYS=XMC2 or not specified).

- If multiple RMOXMS regions are started, they must be started with XMSSUB=NO parameter.

  Only the primary XMS region can have XMSSUB=YES specified.

- The XMS regions must have the XMS=YES parameter to make it accessible.

- The EBCXMCTR table must be assembled during installation to define the relationship between CA View and CA Deliver database high-level qualifiers. The table contains an EBCXMOPT macro to define initialization options and the EBCXMTRN macro for each CICS user transaction.

The EBCXMTRN macro also contains options for the specific database:

- SUBSYS= parameter of the cross-memory task.

  The parameter must match the SUBSYS= parameter specified in the EBCXMCTR table entry.

- RECON=YES can be used to allow reconnection (after an ISPF terminal error) at the point of exit.

- TIMEOUT= specifies how long ISPF is to wait for the XMS session to respond after the user enters input, in seconds.

  We recommend a value as high as possible but not less than 240 (4 minutes).

To abort the XMS session and return the user to ISPF or the TSO command prompt, press the ATTN key.

Note: The SUBMAX= parameter controls the number of user connections, not the USERMAX= parameter. USERMAX=only applies when you are using the subtask with the CICS interface.

To control screen size manually, use these operands. The SNA query command can also be used to determine the device characteristics.

Enter	For Terminal Type
M2	3278-2 24 x 80 default screen size
M2H	3278-2 24 x 80 highlighting

Enter	For Terminal Type
M2X	3279-2 24 x 80 color highlighting
M2C	3279-2 24 x 80 color
M3	3278-3 32 x 80
M3H	3278-3 32 x 80 highlighting
M3X	3279-3 32 x 80 color highlighting
M3C	3279-3 32 x 80 color
M4	3278-4 43 x 80 highlighting
M4H	3278-4 43 x 80 highlighting
M4X	3279-4 43 x 80 color highlighting
M4C	3279-4 43 x 80 color
M5	3278-5 27 x 132
M5H	3278-5 27 x 132 highlighting
M5X	3279-5 27 x 132 color highlighting
M5C	3279-5 27 x 132 color
M6	3290 62 x 80
M6H	3290 62 x 80 highlighting
M7	3290 31 x 160
M7H	3290 31 x 160 highlighting
M8	3290 62 x 160
M8	3290 62 x 160 highlighting

For other modifications to your system, see your VTAM programmer.

Optional Initialization Parameter Statements

The optional initialization parameter statements are delivered as comments in the initialization member RMOPARMS in the CVDEOPTN library.

Review these initialization parameters in the RMOPARMS member after configuration is completed.

Note: For more information about the descriptions of these parameters, see the chapter *Initialization Parameters* in the *Reference Guide*.

If any of the parameters are deemed necessary, remove the comment and supply the necessary parameter before you start CA Deliver.

How to Configure the Online Interfaces Without CA CSM

The topics in this section describe the manual tasks you must perform if you are not using CA CSM to configure your product.

This section also describes the online interface options, the cross-memory drivers, and how to install the online interfaces, including these topics:

- Online and cross-memory interfaces
- Cross-memory drivers for ISPF, TSO, and CA Roscoe interfaces
- Installation of these options:
  - ISPF online retrieval option
  - TSO online retrieval option
  - CA Roscoe online retrieval option
  - Cross-memory services
  - ISPF/cross-memory online retrieval option
  - TSO/cross-memory online retrieval option
  - VTAM online retrieval option
  - CA Roscoe/cross-memory online retrieval option
  - CICS pseudo-conversational option
  - IMS online retrieval option

Online Interfaces

The following table lists the online interfaces, whether cross-memory services (XMS) must be installed and any special advantages of using the interface.

Online Interface	XMS	Advantages
ISPF	NO	Provides full online access without the need for a cross-memory region
ISPF/XMS	YES	Does not require the STEPLIB to be APF authorized To simplify migration, you can run multiple versions of CA Deliver concurrently.
TSO	NO	Provides full online access without the need for a cross-memory region
TSO/XMS	YES	Does not require the STEPLIB to be APF authorized To simplify migration, you can run multiple versions of CA Deliver concurrently.
VTAM	YES	Supports extended data stream to queriable terminals
CICS	YES	To simplify migration, you can run multiple versions of CA Deliver concurrently
IMS/DC	YES	
CA Roscoe	NO	Provides full online access without the need for a cross-memory region
CA Roscoe/XMS	YES	Does not require the STEPLIB to be APF authorized To simplify migration, you can run multiple versions of CA Deliver concurrently.

Cross-Memory Services Interface (XMS)

The cross-memory services interface manages several interfaces; this allows you to control online access with a single operator interface. Advantages of the interfaces are discussed later in this chapter.

The parameters in the startup procedure for the cross-memory task allow you to control:

- The maximum number of users allowed on the system
- Whether to cancel users when they are inactive for a specified time (CANCEL and LONGWAIT)

Note: For information about startup parameters, see Installing Cross-Memory Services later in this chapter.

The operator commands available to modify the cross-memory task allow you to:

- Cancel users
- Suspend additional logons
- List online usage statistics
- Modify selected cross-memory startup JCL parameters

Note: For more information about operator commands, see the chapter "Operator Commands" in the *Reference Guide*.

Cross-Memory Drivers for Interfaces

You can use cross-memory services drivers to run the TSO, ISPF, and CA Roscoe online interfaces.

The advantages of using these drivers are:

- Users are authorized by cross-memory drivers.

  When you use the cross-memory services drivers for the ISPF, TSO, or CA Roscoe interfaces, users are authorized by cross-memory and do not also need authorization from the online interface (for example, TSO).

- Multiple versions of CA Deliver can run simultaneously.

  When you use the cross-memory services drivers for the ISPF, TSO, or CA Roscoe interfaces, you can run multiple versions of CA Deliver concurrently. This ability supports migration; it makes it easier to migrate when you are converting to a new version level of CA Deliver.

  You can also run multiple versions of the online interfaces simultaneously.

Restrictions

These restrictions apply when you execute the program using the cross-memory drivers for TSO, ISPF, and CA Roscoe:

- TSO SUBMIT is not used. The SUBMIT occurs from the connected cross-memory region.

- Direct reprints from the user have the JES banner pages of the cross-memory region. The internal system banner page can be used to check the user requesting the reprint.

User Exits

User exits run in the cross-memory region and do not have access to TSO or CA Roscoe allocations.

Install the ISPF Online Retrieval Option

The ISPF online retrieval option runs under the IBM Interactive System Productivity Facility (ISPF) for z/OS Version 3.0 and higher.

Installation Steps

The following steps are required to install the ISPF/cross-memory online retrieval option. Each step is explained in detail later in the sections that follow.

1. (Optional) Add STEPLIB DD statements to the TSO LOGON procedures if the load modules were not copied to a linklist library.
2. Add the panel and command table libraries to the TSO LOGON procedures.
3. (Optional) Modify an ISPF Selection Menu to Select Online Retrieval feature.

(Optional) Step 1: Add STEPLIB Statements

The action you take in this step depends on what you did during the base product installation—specifically, did you:

- Authorize the program load library or
- Copy the modules to a system-authorized library

If the CA Deliver load modules were *not* copied to one of the libraries in the linklist, proceed with this step; otherwise go directly to the next step.

Follow these steps:

1. Add STEPLIB DD statements to the TSO LOGON procedures if the load modules are not in a linklist library.
2. Add a STEPLIB DD statement for the library containing the product's load modules to the LOGON procedures for those TSO users who are going to be using the ISPF online retrieval option.

Note: If you have CA View, the CA View load modules must also be either in the linklist or in a STEPLIB statement with this step.

Step 2: Add the Panel and Command Libraries (ISPF only)

Note: If you are running under SPF, go to Step 3.

If you run CA Deliver under ISPF, proceed with this step.

To add the panel and command libraries to the TSO LOGON procedure:

1. Concatenate the command table library CAI.CVDETBL0 to DD statement ISPTLIB.
2. Concatenate the panel library CAI.CVDEPNL0 to DD statement ISPPLIB.

Note: If you also plan to use RMOSPF (the ISPF interface), and multiple versions of CA Deliver, concatenate CAI.CVDETBL0 first. Use the CAI.CVDETBL0 from the most current release.

Step 3: (Optional) Modify an ISPF Selection Menu to Select Online Retrieval

If you want to add a selection code for the online retrieval feature to one of the ISPF selection menus, proceed with this step; otherwise, your detailed instructions for ISPF are complete.

To define your selection code, use the following command:

```
PGM(RMOSPF) PARM(high-level-database-name) NEWAPPL(RMO)
```

Use the value next to the NAME parameter on your Initialization Parameter Worksheet for PARM (high-level-database-name).

Note: Adding a selection code allows you to select the online retrieval feature in the same way you would select other ISPF options.

Panel Libraries

The names of the panel libraries vary from site to site and for the different releases of ISPF. These panel libraries are allocated to the ISPPLIB DD statement under TSO.

Be aware that some installations do not allow direct modifications of IBM panels and libraries. In this case, you can place the modified panels in user or site-specific libraries and concatenate them ahead of the IBM libraries.

Ask your system administrator for the specific ISPF panel library that applies to your site and contains the panel ISR@PRIM.

Note: The selection menus shown in the following examples are part of the program product ISPF and are copyrighted by IBM.

Example 1

This example shows you how to add selection code R to the primary option menu ISR@PRIM for ISPF.

The offset lines are the inserted lines.

```
%----------------------- ISPF/PDF PRIMARY OPTION MENU -----------------------
%OPTION ===>_ZCMD                                                            +
%                                                          +USERID    - &ZUSER
%   0 +ISPF PARMS -   SPECIFY TERMINAL AND USER PARAMETERS   +TIME   -
%   1 +BROWSE      -  DISPLAY SOURCE DATA OR OUTPUT LISTINGS +TERMINAL -
%   2 +EDIT        -  CREATE OR CHANGE SOURCE DATA        +PF KEYS - &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, CLIST, OR REXX EXEC
%   7 +DIALOG TEST -  PERFORM DIALOG TESTING
%   8 +LM UTILITIES - PERFORM LIBRARY ADMINISTRATOR UTILITY FUNCTIONS
%   C +CHANGES     -  DISPLAY SUMMARY OF CHANGES FOR THIS RELEASE
%   R +RMOSPF      -  DELIVER ADMINISTRATION
%   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 /* TUTORIAL INDEX - 1ST PAGE         */
)PROC
 &ZSEL = TRANS( TRUNC (&ZCMD,'.')
                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(ISPYXDR) PARM(ISR) NOCHECK'
                8,'PANEL(ISRLPRIM)'
                C,'PGM(ISPTUTOR) PARM(ISR00005)'
            R,'PGM(RMOSPF) PARM(RMO.SYSTEM1) NEWAPPL(RMO)'
                T,'PGM(ISPTUTOR) PARM(ISR00000)'
               ' ',' '
                 X,'EXIT'
                 *,'?' )
   &ZTRAIL = .TRAIL
 )END
```

Note:

- NEWAPPL(RMO) is required and must be specified as shown previously in this section.

  This parameter is used with the command table library concatenation from Step 3 of the ISPF Installation Instructions.

- NEWAPPL(RMO) allows CA Deliver to correctly interpret commands and program function key invocation.

  If this parameter is not specified, certain PF keys such as the scroll keys may not function.

Example 2

This example shows you how to add selection code 3.R as a sub-option to the utilities menu ISPUTIL for ISPF.

The offset lines are the inserted lines.

```
%-----------------------  UTILITY SELECTION MENU  --------- -----------
%OPTION  ===>_OPT         +
%                                                                      +
%   1 +LIBRARY     - LIBRARY UTILITY:
+                    PRINT INDEX LISTING OR ENTIRE DATASET
+                    PRINT, RENAME, DELETE, OR BROWSE MEMBERS
+                    COMPRESS DATASET
%   2 +DATASET     - DATASET UTILITY:
+                    DISPLAY DATASET INFORMATION
+                    ALLOCATE, RENAME, OR DELETE ENTIRE DATASET
+                    CATALOG OR UNCATALOG DATASET
%   3 +MOVE/COPY   - MOVE OR COPY MEMBERS OR DATASETS
%   4 +CATALOG     - CATALOG MANAGEMENT:
+                    DISPLAY OR PRINT CATALOG ENTRIES
+                    INITIALIZE OR DELETE USER CATALOG ALIAS
%   5 +RESET       - RESET STATISTICS FOR MEMBERS OF ISPF LIBRARY
%   6 +HARDCOPY    - INITIATE HARDCOPY OUTPUT
%   7 +VTOC        - DISPLAY OR PRINT VTOC ENTRIES FOR A DASD VOLUME
%   8 +OUTLIST     - DISPLAY, DELETE, OR PRINT HELD JOB OUTPUT
%   9 +SCRIPT/VS   - FORMAT,DISPLAY, AND OPTIONALLY PRINT SCRIPT TEXT
%   R +RMOSPF      - DELIVER ADMINISTRATION

)INIT
  .HELP = TU
)PROC
  &SEL = TRANS( TRUNC (&OPT,'.')
                1,'PGM(ISPUDA) PARM(UDA1)'
                2,'PGM(ISPUDA) PARM(UDA1)'
                3,'PGM(ISPUMC)'
                4,'PGM(ISPUCA)'
                5,'PGM(ISPURS)'
                6,'PGM(ISPUHC)'
                7,'PGM(ISPUVT)'
                8,'PGM(ISPUOL) PARM(UOL01)'
                9,'PGM(ISPUSC) PARM(SCRPTA)'
             R,'PGM(RMOSPF) PARM(RMO.SYSTEM1) NEWAPPL(RMO)'
               ' ','  '
                *,'?' )
 )END
```

Example 3

This example shows you how to add selection code R to the primary option menu ISP@PRIM for SPF. Shading identifies the inserted lines.

```
%----------------------  SPF—MVS PRIMARY OPTION MENU  ---------------
%OPTION  ===>_OPT
%                                                              +USERID   -
%   0 +ISPF PARMS  -     SPECIFY TERMINAL AND USER PARAMETERS   +TIME     -
%   1 +BROWSE      -     DISPLAY SOURCE DATA OR OUTPUT LISTINGS +TERMINAL —
%   2 +EDIT        -     CREATE OR CHANGE SOURCE DATA           +PF KEYS  -
%   3 +UTILITIES   -     PERFORM SPF UTILITY FUNCTIONS
%   4 +FOREGROUND  -     COMPILE, ASSEMBLE, OR DEBUG
%   5 +BACKGROUND  -     COMPILE, ASSEMBLE, OR LINK EDIT
%   6 +COMMAND     -     ENTER TSO COMMAND OR CLIST
%   7 +SUPPORT     -     TEST DIALOG OR CONVERT MENU/MESSAGE FORMATS
%   8 +LM UTILITIES-     PERFORM LIBRARY ADMINISTRATOR UTILITY FUNCTIONS
%   R +RMOSPF      -     DELIVER ADMINISTRATION
%   T +TUTORIAL    -     DISPLAY INFORMATION ABOUT SPF
%   X +EXIT        -     TERMINATE SPF USING LIST/LOG DEFAULTS
%
+PRESS%END KEY TO TERMINATE SPF+
%
)INIT
  .HELP = TTUTOR
  &ZHTOP = TTUTOR   /* TUTORIAL TABLE OF CONTENTS        */
  &ZHINDEX = TINDEX /* TUTORIAL INDEX - 1ST PAGE         */
)PROC
  &ZSEL = TRANS( TRUNC (&OPT,'.')
                0,'PANEL(ISPOPT)'
                1,'PGM(ISRBRO)'
                2,'PGM(ISPEDIT)'
                3,'PANEL(ISPUTIL)'
                4,'PANEL(ISPFORA)'
                5,'PANEL(ISRJOB)'
                6,'PGM(ISPTSO)'
                7,'PANEL(ISPOTAC)'
                R,'PGM(EC2XMSPF) PARM(RMO.SYSTEM1)'
                T,'PGM(ISPTUTOR) PARM(T)'
                ' ',' '
                 X,'EXIT'
                 *,'?' )
 )END
```

Install the TSO Online Retrieval Option

The following step is required to install the TSO online retrieval option and is explained in detail in the next topic.

(Optional) Add STEPLIB DD statements to the TSO LOGON procedures if the load modules are not in a linklist library.

Step 1: (Optional) Add STEPLIB DD Statements

The action you take in this step depends on what you did during the base-product installation—specifically, did you:

- Authorize the program load library or
- Copy the modules to a system authorized library

If the load modules were *not* copied to one of the libraries in the linklist:

- Add a STEPLIB DD statement (for the library containing the load modules) to the TSO LOGON procedures for those TSO users who are to use the native TSO online retrieval option.

If the load modules were copied to one of the libraries in the linklist, no STEPLIB DD statements are required.

Note: If you have CA View, the CA View load modules either must also be in the linklist, or placed in a STEPLIB statement with this step.

Install the CA Roscoe Online Retrieval Option

The CA Roscoe online retrieval option runs as a command processor under ETSO/Roscoe.

The following steps are required to install the CA Roscoe/Cross-Memory Online Retrieval Option. Each step is explained in detail in the sections that follow.

1. (Optional) Concatenate the Load Module Library to the ETSOLIB DD statement, if the load modules were not copied to a linklist library.
2. Add the control statement for the RMOROS command processor to the Eligible Program List (EPL).
3. Invoke the RMOROS command processor.

Step 1: (Optional) Concatenate the Load Module Library

If the load modules were *not* copied to a linklist library, concatenate the library that contains the load modules to the ETSOLIB DD statement in the CA Roscoe startup JCL.

Note: If you have CA View, the CA View load modules must also be either in the linklist or in an ETSOLIB statement with this step.

Step 2: Add RMOROS Command Process

Add this Eligible Program List control statement to member ETSOPGMS for the CA Roscoe user with the RO prefix:

Column	Contents
1–8	RMOROS
9	Blank
10–12	Number of users allowed to access CA Deliver at one time
13	Blank
14–17	CPU time slice; use 9999 to prevent premature termination
18	Blank
19–24	Maximum memory (in KB) below the 16 MB line This value can vary depending on size of database and other factors (0001000 should be adequate).
25	Blank
26–31	Maximum memory (in KB) below the line that CA Deliver can acquire at one time Use 999999 so that GETMAINs are not limited.
32	Blank
33–38	Maximum memory (in KB) above the 16 MB line This value can vary depending on the features used (000512 should be adequate).
39	Blank
40–45	Maximum memory (in KB) above the line that CA Deliver can acquire at one time Use 999999 so that GETMAINs are not limited.
46	Blank
47–48	CP to call RMOROS as a TSO command processor

Column	Contents
49	Y – Application authorized to issue MODESET SVC
50	Blank
51-52	CP to call EC2XMROS as a TSO command processor
53-255	Ignored

Install Cross-Memory Services

The cross-memory services interface is required for these online interfaces:

- CICS pseudo-conversational
- IMS
- VTAM
- ISPF/cross-memory
- TSO/cross-memory
- CA Roscoe/cross-memory

This list summarizes the steps to install the cross-memory services. Detailed instructions are in the sections that follow.

1. (Optional) Add the Start Procedure to the PROCLIB for the Cross-Memory Online Task.
2. (Optional) Modify, Assemble, and Link the EC2XMCTR Module.
3. Define Security Requirements.

Cross-Memory Services Regions

The VTAM and XMS (cross-memory services) interfaces operate in one or more cross-memory online regions.

A cross-memory region can be configured as:

- An XMS only region
- A VTAM only region
- A combination of XMS and VTAM users

Be aware of the following:

- Each cross-memory region is configured with the start-up parameters provided on the PARM= of the execute statement, and with an optional SYSIN DD statement.

  The REGION= specification determines the maximum number of users supported.

- Allow 20 MB (megabytes) for the XMS region plus 1 MB of storage for every two users.

For example, if you specified a REGION of 120 MB, you could specify:

```
USERMAX=200
```

If more users are needed, multiple regions can be started under the same SUBSYS= value and will be chained together.

Note: The REGION ID specified in the parameters must be different for each region, and if VTAM interface is used, a different RMOAPPL= name will be needed for each region.

Interface Parameter Requirements

This table lists the optional and required parameters for each interface.

Note: The numbers next to the interface values refer to note references.

Parameter	VTAM	TSO	TSO/ISPF	CA Roscoe	CICS	IMS/DC
CANCEL	Opt. (1)	Opt. (1)	Opt. (1)	Opt. (1)	Opt. (1)	Opt. (1)
LGNFMT	Opt. (2)					
LGNSEC	Opt. (3)	Opt. (3)	Opt. (3)	Opt. (3)	Opt. (3)	Opt. (3)
LGNPROP	Opt. (3)	Opt. (3)	Opt. (3)	Opt. (3)	Opt. (3)	Opt. (3)
LONGWAIT	Opt. (1)	Opt. (1)	Opt. (1)	Opt. (1)	Opt. (1)	Opt. (1)
MSGLVL	Opt.	Opt.	Opt.	Opt.	Opt.	Opt.
RMOAPPL	Req.					
RMOVTDB	Opt. (4)					
SMFSESS	Opt. (5)	Opt. (5)	Opt. (5)	Opt. (5)	Opt. (5)	Opt. (5)
SUBSYS	Opt. (6)	Opt. (6)	Opt. (6)	Opt. (6)	Opt. (6)	Opt. (6)
USERMAX	Req.	Req.	Req.	Req.	Req.	Req.
VTAMPASS	Opt. (7)					
VTAMSAA	Opt. (8)					
VTMQUERY	Opt. (9)					

Parameter	VTAM	TSO	TSO/ISPF	CA Roscoe	CICS	IMS/DC
XMS	Opt. (10)	Opt. (10)	Opt. (10)	Opt. (10)	Opt. (10)	Opt. (10)
XMSSUB		Req. (11)	Req. (11)	Req. (11)		Req. (11)

Notes for the Interface Parameter Requirements Table

1. The CANCEL= and LONGWAIT= values work together.

   We recommend that you set CANCEL=YES and set LONGWAIT to a value appropriate for your site.

2. LGNFMT= should either not be specified, or it is to be specified as the default (LGNFMT=1), unless your session manager cannot provide logon data in the normal format.

   If RMOVTDB= is specified, LGNFMT=1 must be specified; any VTAM logon data will be ignored.

3. The LGNSEC= and LGNPROP= work together, and require the default RMOUSxUX exit.

   If LGNSEC=YES, LGNSEC=YESP, or LGNSEC=PPHRASE is used (to indicate external security signon), the LGNPROP=YES/NO will be used to control whether security violations, database opens and jobs submitted will use the user ID (LGNPROP=YES which is the default) or will use the XMS region's user ID.

   In the online region, the CA Deliver database is opened before logon, and uses the XMS region's user ID.

4. The RMOVTDB= only affects VTAM access, and is only to be used when the session manager cannot produce valid LOGON DATA.

   For the valid formats supported by CA Deliver, see the LGNFMT= parameter.

5. The SMFSESS= is to be specified when the user needs to collect user session statistics (CPU, logon/LOGOFF times, storage used, and so on).

6. The SUBSYS= is only to be specified when you are using a non-default subsystem ID under MVS.

   The default is release specific; it does not require JCL/PARM changes when you are converting to a new software release.

7. VTAMPASS= is only to be specified if you are going to be running a multi-region VTAM interface.

   The other VTAM regions must specify the same parameters (LGNFMT= RMOVDTB=, VTMQUERY=, VTAMSAA=), or the interface might react in unpredictable ways.

8. VTMQUERY= is to be specified either as NORM (normal) or allowed to default to that value.

   VTMQUERY=NONE works, but CA Deliver cannot detect color/high-light terminal attributes so color/high-light support will be shut off.

   VTAMSAA=NO is to be used if terminals cannot support the SNA QUERY LIST command, such as the older 3270/3290 devices and some older PC/3270 emulators.

9. XMS=NO is to be used when you are going to be using only the VTAM interface.

10. XMS=YES (the default) must be used to provide support for these interfaces.

11. XMSSUB=YES must be specified to provide support for these interfaces.

    The XMSSUB=YES must reside in an XMS region with a default SUBSYS= value. If multiple XMS regions are started, only one region can have XMSSUB=YES. The other regions will still be available for user sessions, but their traffic will be routed through the region specifying XMSSUB=YES.

    If you terminate the region with XMSSUB=YES, all sessions using the subtask are going to fail (that is, all TSO/XMS, ISPF/XMS, CA Roscoe/XMS, IMS/DC regions). CICS has router SUBTASK in its region, and does not use the XMSSUB=YES function.

12. The OVERRIDE parameter is valid for all interfaces and is optional. It might be specified only in the execute statement PARM field and it cannot be coded in the SYSIN data set.

    If the parameter is not coded, the default duplicate parameter substitution hierarchy is SYSIN then the EXEC PARM.

    - The OVERRIDE parameter determines whether parameters in the execute statement PARM field have precedence over parameters in the SYSIN data set.
    - If OVERRIDE is coded in the execute statement PARM field, parameters specified in the execute statement PARM field will override duplicate specifications in the SYSIN data set.
    - If OVERRIDE is not coded, parameters specified in the SYSIN data set are used and corresponding parameter specifications in the execute statement PARM field are ignored.
    - The OVERRIDE parameter does not have any sub-parameters and it is coded as is in the execute statement PARM field.
    - If this parameter is coded in the SYSIN data set, error message "EBCDRV99 OVERRIDE KEYWORD NOT ALLOWED IN SYSIN STATEMENTS - RUN ENDED U0016" is going to be displayed in the XMS job log and XMS will terminate with a return code of 16.

Step 1: Add the Start Procedure for the Cross-Memory Online Task

Add this start-procedure JCL for the cross-memory online retrieval task as member CBROSDRV to SYS1.PROCLIB. Sample JCL for this PROC is provided in member CBROSDRV of CAI.CVDEPROC.

```
//CBROSDRV   EXEC PGM=EC2DRV,REGION=1024K,TIME=1440,
//           PARM=('XMSSYS01,RMOAPPL=RMOVTAM,USERMAX=30,VTAMPASS=YES')
//*
//STEPLIB DD DSN=&CAI.CVDELOAD,DISP=SHR
//*
//SYSPRINT DD SYSOUT=A <--MESSAGE LOG (NEW, OUTPUT REQUIRED WHEN SUBMITTING
//*                       DUMP TO CA TECH SUPPORT)
//*
//RMOLOG   DD SYSOUT=A <--MESSAGE LOG (NEW, OUTPUT REQUIRED WHEN
//*                       SUBMITTING DUMP TO CA TECH
//*                       SUPPORT) ONLY USED WHEN XMSSUB=YES)
//*
//EBCUDUMP DD SYSOUT=A <--INTERNAL DUMP OUTPUT (NEW, OUTPUT REQUIRED WHEN
//*                       SUBMITTING DUMP TO CA TECH SUPPORT)
//*
//*
//SYSUDUMP DD SYSOUT=A <--MVS DUMP OUTPUT (OPTIONAL, MVS DUMP CAN BE ROUTED
//*                       WITH SYSMDUMP OR SYSABEND ALSO)
//*                       WARNING!!!! ABENDAID DUMPS ARE OF NO USE CORRECTING
//*                       PROBLEMS WITH RMOXMS. YOU MUST ALWAYS SUPPRESS
//*                       ABENDAID IF YOU HAVE IT INSTALLED FOR THIS REGION.
//*
//SYSIN    DD DSN=CAI.CVDEOPTN (PARMXMS),DISP=SHR
```

SYSIN Statements for Parameters

The REGIONID parameter is positional and must be specified in the PARM= statement of the cross-memory task JCL.

You can use SYSIN DD statements to specify the other cross-memory parameters.

If you are going to run multiple regions, specify these parameters in the PARM= statement:

```
SUBSYS=
RMOAPPL=
XMS=
```

You can specify the rest of the parameters with SYSIN DD statements. If you place the SYSIN statements in a PDS member, you can alter the parameters without shutting down the cross-memory region. Be aware that the parameters do not take effect until the next time the region is shut down and restarted.

Note:

- SYSIN parameters for cross-memory services must start in column #1. Any parameter that does not begin in column #1 is treated as a comment and is ignored.
- The OVERRIDE parameter cannot be coded in the SYSIN data set.
  - If the OVERRIDE parameter is coded in the execute statement PARM field, a duplicate parameter in the PARM field and the SYSIN data set will be set to the value specified in the PARM field parameter.
  - If the OVERRIDE parameter is not coded in the execute statement PARM field, a duplicate parameter in the PARM field and the SYSIN dataset will be set to the value specified in the SYSIN dataset parameter.

Start Procedure Parameters

XMSSYS01 (in the PARM statement) specifies the one- to eight-character REGIONID. The REGIONID is positional—it must be the first value of the PARM= statement.

This value is used to define separate cross-memory regions attached to one MVS subsystem (specified by the SUBSYS parameter).

Note: Each separate RMOXMS region has its own REGIONID. We suggest using the PROC name of the cross-memory-started task.

CANCEL=YES|NO

Indicates one of the following:

- CANCEL=YES

  Specifies that a user who is inactive (no commands entered) for the time specified by the LONGWAIT parameter will be canceled, and the session will be terminated. With CANCEL=YES, all users will be automatically canceled if the region is shut down by an operator command.

- CANCEL=NO specifies that the connection is not canceled, and the user status changes to LONGWAIT.

Default: NO

LGNFMT=*n*

Specifies the format of the data parameter when logging on to a VTAM region where n is a digit (1 through 3), as follows:

1 database//userid/password/newpass

2 userID/password/newpass/database/mode

3 database/mode

Note: LGNFMT does not support password phrases. If implementing password phrases, leave the password fields blank to prompt a logon screen.

Default: 1

LGNPROP=YES|NO

Indicates whether the CA Deliver user ID should be passed to MVS for propagation during submit processing.

This parameter is only valid if LGNSEC=YES is specified.

Default: YES

LGNSEC=YES|NO|PASSWORD|YESP|PPHRASE

Indicates whether there is to be RACROUTE security checking.

LGNSEC must be YES, YESP, or PPHRASE if you are accessing a database that has the CA Deliver initialization parameter SECURITY=EXTERNAL specified.

Modifications to default logon exit (RMOUSXUX) is not required to implement external security. This exit is only provided so that you can customize the exit to provide any necessary functionality.

For example, to access external security packages directly, without SAF, you must modify and install the RMOUSXUX user exit.

These values for LGNSEC are effective when the default exits are implemented:

Value

Result

YES

External security checking is performed using SAF calls.

External security verifies userid only for all cross-memory interfaces (with no interruption to the user).

A panel is presented to the user to verify userid and password.

Note: This panel is only presented when the user interface does not automatically send the userid to the XMS region.

The password is not forwarded; RACF or CA ACF2R Security (eTrust CA-ACF2) requires additional specifications. For RACF or CA ACF2, see Bypassing Password Verification in the chapter "Security" in the Reference Guide for implementation instructions.

NO

No SAF call to external security is performed.

The user ID is checked internally against CA Deliver definitions.

If no match is found, CA Deliver might or might not dynamically create a user ID depending on the value of your DEFMODE initialization parameter.

Review your DEFMODE values to be sure that they are appropriate.

PASSWORD

No call to external security is performed.

Internally, user ID and password are verified.

YESP

External security checking is performed using SAF calls.

External security verifies userid and password for all cross-memory interfaces (with no interruption to the user).

A panel is presented to the user to verify the userid and password. This panel is only presented when the user interface does not automatically send the userid and password to the XMS region.

PPHRASE

External security checking is performed using SAF calls.

External security verifies userid and password phrase for all cross-memory interfaces (with no interruption to the user).

A panel is presented to the user to verify the userid and password phrase. This panel is only presented when the user interface does not automatically send the userid and password to the XMS region.

Default: NO

LONGWAIT=nn

Specifies the number of minutes of inactivity (no commands entered) before a user's session is terminated.

The CANCEL parameter must be YES to terminate the session.

Default: 15

MSGLVL=CRIT|ACTN|NORM|INFO|TRCE

Indicates the level of message to be written to the started task job log.

Unless they are suppressed, the CRITICAL and ACTION messages are written to the console. These settings cause these types of messages to be displayed:

CRIT

Displays critical messages.

ACTN

Displays critical and action messages.

NORM

Displays critical, action, and normal messages.

Default: NORM

INFO

Displays all but trace messages.

TRCE

Displays all messages.

Note: This parameter does not suppress messages from the SYSPRINT log.

RMOAPPL=applname

Specifies the RMOVTAM APPLID which provides VTAM user signon capability.

Default: RMOVTAM

RMOVTDB=high-level.databasename

Specifies that this database high-level qualifier must be used by all RMOVTAM interface users.

Typically, you would not specify this value and allow the user to specify which database to access when the user logs on. When this parameter is specified, any database specified at logon time with the VTAM logon command is ignored.

SMFSESS=nnn

Specifies whether SMF records are to be collected for the cross-memory sessions.

The EBCSMFU1 macro documents the records available.

Default: zero—no record collection

SUBSYS=name

Specifies the four-character MVS subsystem.

This must match the value in the EC2XMCTR table.

Default: XMC2

Note: The SUBSYS parameter does not apply to VTAM or IMS interface users.

USERMAX=nn

The maximum number of sessions to be allowed.

Default: 10

VTAMPASS=YES|NO

Indicates whether signon requests can be passed to other regions in this subsystem when this region cannot accept the request

Possible reasons for not being able to accept a signon request are that the USERMAX parameter has been exceeded, or a SUSPEND operator command has been issued.

If VTAMPASS=YES is specified, include PASS in the AUTH value on the APPL statement in the VTAM definition. If you want to run multiple regions, VTAMPASS must be YES.

Default: NO

VTMQUERY=ALL|NORM|NONE

Indicates whether the VTAM interface will QUERY terminals with dynamic log modes to determine the alternate screen size.

Use this parameter only to query VTAM terminals that support SNA QUERY commands and do not have an alternate screen size defined in their logmode.

ALL

Queries all terminals.

NORM

Queries the terminal if the bind image indicates it is a VTAM QUERY terminal, and there is no alternate screen size defined.

NONE

Does not query any terminals (and color is not supported).

Default: NORM

VTAMSAA=YES|NO

Indicates whether all terminals are SAA compliant.

If you have the following:

- Older terminals that cannot support SAA (such as 3290 terminals)
- These older terminals are going to be connecting with log modes that indicate that CA View should query their alternate screen size

You must specify VTAMSAA=NO or these terminals are not able to log onto the SARVTAM interface.

VTAMSAA=NO causes more overhead in logging on terminals than can be queried, and is only to be used when required.

XMS=YES|NO

Indicates whether cross-memory users are to be allowed to sign on to the region.

Set XMS=NO if this is a VTAM only region, and cross-memory is not to be supported.

Note: If XMS=NO, there should be a VTAM ACB name coded in the SARAPPL= parameter.

Default: YES

XMSSUB=YES|NO

XMSSUB=YES is required for ISPF cross-memory, TSO cross-memory, and CA Roscoe cross-memory sessions.

All other interface users should set XMSSUB=NO.

Default: NO

RMOLOG DD Statement (Optional)

The optional RMOLOG DD statement is used to specify where to write the log of user subtask messages.

This output is critical to resolving user subtask ABENDs, and is to be submitted to CA Technical Support along with the region or task dump created with an ABEND.

SYSPRINT DD Statement (Optional)

The optional SYSPRINT DD statement is used to specify where to write the log of cross-memory (RMOXMS) messages.

This output is critical to resolving RMOXMS ABENDs, and is to be submitted to CA Technical Support along with the region or task dump created with an ABEND.

EBCUDUMP DD Statement

The EBCUDUMP DD statement is required, and is used to specify where to write a special dump of CA Deliver control blocks that do not appear in normal MVS dump output.

This output is critical to resolving RMOXMS ABENDs, and is to be submitted to CA Technical Support along with the region or task dump created with an ABEND.

Notes:

- On ABEND Output, only regular MVS dump output should be collected. Output from dump compression and analysis programs is not helpful to technical support—you might be required to recreate the dump.
- Acceptable types include SYSUDUMP, SYSMDUMP, or SYSABEND output, in print-record format. IPCS/SVC dumps and CICS transaction or region dumps are also acceptable, but must be formatted for printing before they are placed on the tape.
- The RMOXMS region uses the operator facility to abort a user's task for various problems. These problems might be a LONGWAIT time out, a VTAM I/O error, or a detected internal error, which appear in the log followed by a U0522 ABEND of the user subtask. No dump is generated.

STEPLIB for This Job

The action you take in this step depends on what you did during the base-product installation. Specifically, did you:

- Authorize the program load library or
- Copy the modules to a system authorized library.

Be aware of the following before you run this job:

- If the CA Deliver load modules were copied to an authorized library other than one of the linklist libraries, you must change the data set name on the STEPLIB DD statement.
- If the load modules were copied to a linklist library, you must remove the STEPLIB DD statement.
- If you have CA View installed, you must consider these possibilities before you run the job listed previously above: If the CA Deliver load modules were copied to an authorized library other than one of the linklist libraries, concatenate the CA Deliver load library as a second STEPLIB after the CA View load library in the STEPLIB DD statement.
- If the load modules were copied to a linklist library, do nothing.

Step 2: Modify, Assemble, and Link the EC2XMCTR Module

The EC2XMCTR module defines the relationship between a transaction identifier and the database, and session attributes. Also, the execution options for the cross-memory subtask system are also defined in this module. All interfaces except VTAM require the EC2XMCTR table.

Be aware of the following:

- You must assemble the EC2XMCTR table during installation to define the relationship between CA View and CA Deliver database qualifiers, and the session options to be used, and to provide information used to build the XMS database table.
- The table contains an EBCXMOPT macro to define initialization options and one EBCXMTRN, RMOXMTRN, or INBXMTRN macro for each TSO user session. For all users except VTAM, the transaction being used for each session must be defined in an EBCXMTRN statement. Only the database high-level qualifier is used for VTAM XMS users.
- The transaction definition macros are searched by database name, and the first match is used. If no entry is found in the EC2XMCTR table, the session is rejected.

A sample EBCXMCTR source program is in the CAI.CVDESRC library, which is unloaded as part of CA Deliver's installation. The source is comprised of one or more assembler macros.

Format of the Macros

The first statement defines the system options and has this format:

```
EBCXMOPT DESTID=dest,SRVTRAN=transaction,MSGLVL=level,          X
      DESTID=CICS-dest,LOGWAIT=timout-val,                      X
      USERMAX=user-number,WAITCNT=maxcount
```

The next group of statements is for each transaction, database, or both to be accessed; they have this format:

```
EBCXMTRN TRANID=tranid,INDEX=high-level-name,TIMEOUT=sec,       X
       SUBSYS=subsysid,RECON=yes|no,                            X
       MSGSUPP=yes|no
```

The last statement generates the transaction table:

```
EBCXMTRN TYPE=GEN
```

Finally, an assembler END statement is needed to end the table:

```
END
```

EBCXMOPT Statement Parameters

The following parameters are specified in the EBCXMOPT statement:

DESTID=dest

Specifies the transient data destination to which messages from the CICS subtask are sent.

- Supply a DESTID to indicate that a queue (typically an extra partitioned queue that points to a SYSOUT data definition name) is defined.
- Leave DESTID blank to specify that messages from the CICS subtask are not to be captured.

XMC11=transaction

Specifies a four character transaction that is to be added to the EBCXMC11 timeout message.

This transaction allows for site-specific tailoring of the timeout message.

Default: None

SRVTRAN=transaction

Specifies the transaction defined for EC2CISRV that is initiated as a service transaction when CA Deliver CICS is initialized.

Default: XMC2

MSGLVL=CRIT|ACTN|NORM|INFO|TRCE

Indicates the level of messages to display on the console.

These settings cause the following types of messages to be written:

CRIT

Displays only critical messages.

ACTN

Displays only critical and action messages.

NORM

Displays only critical, action, and normal messages.

INFO

Displays all but trace messages.

TRCE

Displays all messages.

Default: NORM

LOGWAIT=nnn

Indicates the amount of time a user is to wait to log on before the user's session times out.

Default: 200 seconds (2 minutes, 00 seconds)

SGNCNT=nn

Controls the number of logon control blocks allocated. These blocks are only used during the logon process. They are then reused and made available to other users attempting to log on.

When you increase the SGNCNT value, be aware that 256 bytes of ECSA are needed each time SGNCNT is increased by 1. Typically, 5 logon blocks are enough, but the value cannot exceed 50.

Default: 5

SUBMAX=nn

Indicates the total number of user control blocks that are allocated when a cross-memory subtask (other than CICS) is initialized.

Default: 500

USERMAX=nn

Indicates the number of user control blocks that are allocated when CICS is initialized.

Default: 500

WAITCNT=nnn

The number of sessions for which the subtask can wait.

Default: 256

IMSMENU

The IMS/DC conversational menu to transfer to when CA Deliver terminates.

If this value is not specified, the transaction in the SPA is set to blanks.

IMSSPA

The size of the IMS/DC SPA.

The SPA size must be at least 18, but cannot exceed 100.

Default: 18

EBCXMTRN Statement Parameters

The following parameters are specified in the EBCXMTRN statements:

TYPE=EXPRESS|GEN

Specifies whether this is a transaction/database entry or the table is to be generated.

GEN

Generates the table.

EXPRESS

Contains a transaction code and index entry for CA Deliver. SAR and INB are valid for CA View and CA Balancing Report Control (CA Balancing) if this is a combined table.

TRANID=tranid

Defines the transaction identifier for CICS.

For TSO, ISPF, and CA Roscoe (the cross-memory drivers), TRANID is ignored, and the first instance of the database high-level qualifier is used.

INDEX=high-level-name

Defines the high-level name of the database.

TIMEOUT=nnn

Defines the time out value, in seconds, to be used by this transaction.

- This value is used as the maximum wait time for a response from the RMOXMS started task.
- This value must be greater than zero and less than 9999 seconds (which is two hours, 40 minutes).
- If you do not want any timeout to occur, specify TIMEOUT=NO.

Default: 240 seconds (four minutes)

SUBSYS=subsys-id

Defines a four-character MVS subsystem name which must match the value specified for SUBSYS in the cross-memory started task JCL.

Each subsystem can support multiple databases and/or CICS/IMS regions.

Default: XMC2

Note:

- There is no need to change the default unless you wish to bring up multiple cross-memory regions and separate transactions for testing or performance reasons.
- This subsystem name is not defined in SYS1.PARMLIB.

RECON=YES|NO

Indicates whether a user can reconnect to a lost session.

Default: NO.

MSGSUPP=YES|NO

Indicates whether a termination message is displayed when a session is terminated by a user.

Default: NO. This does not suppress messages generated from abnormal termination.

Note: The statements follow standard assembler coding conventions.

Macro Coding Example

Assume that two CA Deliver systems have been created.

The databases for the two systems have high-level names of RMO.SYSTEM1 and RMO.SYSTEM2. A user must enter transaction identifier RM1 for the first system and RM2 for the second.

The source for program EC2XMCTR contains these control statements:

```
EBCXMOPT MSGLVL=CRIT,USERMAX=50
EBCXMTRN TRANID=RM1,INDEX=RMO.SYSTEM1
EBCXMTRN TRANID=RM2,INDEX=RMO.SYSTEM2
EBCXMTRN TYPE=GEN
END
```

EBCXMTRN TYPE=GEN must be the last statement before the END. This statement causes the EBCXMCTR CSECT to be generated.

Sample JCL

Sample JCL for this job is provided in member BROSXCTR of CAI.CVDEJCL.

This job provides an SMP/E USERMOD which assembles and links an installation-dependent version of EC2XMCTR.

Parameters for Online Interfaces

The EC2XMCTR table defines the way linkages between the online drivers and the XMS region are established. Some of the parameters are used only in specific environments and others are used in all environments.

This table indicates which parameter affects each online interface.

All XMS interfaces require the EC2XMCTR table.

You must:

- Assemble the table during installation to define the relationship between CA View and CA Deliver database high-level qualifiers and the session options that are to be used
- Provide the information that is used to build the XMS database table.

  Note: Be aware if both CA View and CA Deliver are installed and the CA View interface is doing any access to an associated DLVR database, the associated DLVR database needs to be added as an entry in the EC2XMCTR table.

Only the database high-level qualifier is used for VTAM XMS users.

The numbers in parentheses are explained in the notes section that follows the table.

Parameter	TSO	TSO/ISPF	CA Roscoe	CICS	IMS/DC
DESTID				Opt. (1)	
XMC11				Opt. (8)	
SRVTRAN				Opt. (2)	
MSGLVL	Opt.	Opt.	Opt.	Opt.	Opt.
LOGWAIT	Opt.	Opt.	Opt.	Opt.	Opt.
SUBMAX	Opt. (3)	Opt. (3)	Opt. (3)		Opt. (3)
USERMAX				Opt. (4)	
WAITCNT	Opt. (5)	Opt. (5)	Opt. (5)	Opt. (5)	Opt. (5)
IMSMENU					Opt. (6)
IMSSPA					Opt. (7)

Note: The numbers next to the table values refer to note references.

Notes for the Online Interface Parameters

Follow these steps:

1. DESTID= specifies an optional CICS destination to which message output is to be written.
2. SRVTRAN= specifies the service transaction ID.

   This transaction is required for CICS, but you can use the default service transaction name XMC2.
3. SUBMAX= controls the maximum connections that can be managed by the subtask program.

   The default is 500, which should be changed for most users. Each ISPF/XMS, TSO/XMS, CA Roscoe/XMS, or IMS/DC user connects through the XMS subtask and the value defines the total number of users that can be connected from these interfaces at one time.
4. USERMAX= controls the maximum connections that can be managed by the subtask program.

   The default is 500. Each CICS region can manage this number of sessions. To increase the value, you must restart the CICS or XMS region that owns the subtask.
5. WAITCNT= specifies a value that should remain at the default value at this time.

   Major performance problems occur if you set this to a lower value. Note that this value cannot be set above 255.
6. IMSMENU= specifies the IMS/DC conversational menu to transfer to when CA Deliver ends. If this value is not specified, the SPA TRAN is set to blank upon termination.
7. IMSSPA= specifies the length of the IMS/DC spa to be used (IMS/DC only).

   This parameter allows the spa size to be adjusted so that CA Deliver can transfer to user transactions.

   IMS/DC requires the spa size to remain the same. The spa size must be at least 18 bytes, and although you can specify a spa size of up to 100 bytes, only the first 18 bytes are used.
8. XMC11= specifies an optional 4-character CICS transaction ID that is displayed as part of message EBCXMC11 when a CICS user times out.

Step 3: Define Security Requirements

Follow these steps to define security requirements for CA Top Secret Security (eTrust CA Top Secret):

1. Rename the existing facility in the facility matrix table if you do not have a facility defined for RMOXMS:

   ```
   TSS MODIFY FACILITY(USERnn=NAME=RMOXMS)
   ```

   Note: The TSS MODIFY command is only valid until the next recycle of CA Top Secret. To make the change permanent, add the following to the CA Top Secret parameter file:

   ```
   FACILITY(USERnn=NAME=RMOXMS)
   ```

2. Verify that the correct PGMname is defined for the new facility, where PGMname is either the first three characters or all the eight characters of the program name that is to make security calls (EC2 or EC2DRV).

   ```
   TSS MODIFY FACILITY(RMOXMS=PGM=EC2)
   ```

   Note: The TSS MODIFY command is only valid until the next recycle of CA Top Secret. To make the change permanent, add the following to the CA Top Secret parameter file after the FACILITY(USERnn=NAME=RMOXMS) statement:

   ```
   FACILITY(RMOXMS=PGM=EC2)
   ```

3. Create region ACID for the facility and add a master facility of the facility defined in Step 1:

   ```
   TSS CREATE(RMOXMS) PASSWORD(xxxx,0) TYPE(USER) DEPT(dept) NAME('CA Deliver XMS
   REGION ACID')
   ```

   ```
   TSS ADDTO(RMOXMS) MASTFAC(RMOXMS)
   ```

   We recommend that all started task (STC) acids be given a password and OPTIONS(4) be set in the CA Top Secret parameter file. OPTIONS(4) eliminates the prompt for a password when the STC starts, but if someone tries to signon with the STC acid, he needs to know the password.

   The region acid needs access to all resources accessed at startup.

   This access can be given by adding bypass attributes:

   TSS ADD(RMOXMS) NODSNCHK NOVOLCHK) or by permitting the specific resources

   TSS PERMIT(RMOXMS) DATASET(xxxx) ACCESS(access)).

These resources include:

- READ access to the XMS load library if pointing to this library in a STEPLIB concatenation.
- READ access to any other libraries specified in the STEPLIB concatenation.
- READ access to the SYSIN DD statement if it points to a dataset.
- UPDATE access to the Deliver database.

If any other DD statements (that is, SYSPRINT, RMOLOG, EBCUDUMP, SYSUDUMP, etc) in the XMS startup procs point to datasets instead of SYSOUT, READ access to these datasets is required.

4. Define the RMOXMS STC to the TSS STC record:

```
TSS ADDTO(STC) PROCNAME(RMOXMS) ACID(RMOXMS)
```

5. Give access to the ACIDs required to sign on to this facility (from Step 1).

```
TSS ADDTO(acid) FACILITY(RMOXMS)
```

Where 'acid' is the user acid that needs access, an attached profile, or the ALL record if all users must have access.

Install the ISPF/Cross-Memory Online Retrieval Option

The ISPF/Cross-Memory Online Retrieval Option runs under IBM's ISPF for z/OS Version 3.0 and higher.

Important! This interface requires Cross-memory services to be already installed. For more information, see Install Cross-Memory Services in this chapter.

Note: In the JCL for the cross-memory services task, the parameter XMSSUB must be set to YES.

Installation Steps

The following steps are required to install the ISPF/cross-memory online retrieval option. Each step is explained in detail later in the sections that follow.

1. (Optional) Add STEPLIB DD Statements to the TSO LOGON procedures if the load modules were not copied to a linklist library.
2. Add the panel and command table libraries to the TSO logon procedures. (For ISPF only, not for SPF.)
3. (Optional) Modify an ISPF selection menu to select the online retrieval feature.

Step 1: (Optional) Add STEPLIB DD Statements to the TSO LOGON Procedures

The action you take in this step depends on what you did during the base-product installation—specifically, did you:

- Authorize the program load library, or
- Copy the modules to a system authorized library.

If the CA Deliver load modules were *not* copied to one of the libraries in the linklist, proceed with this step; otherwise go to the next step.

For this interface, the libraries do not have to be APF authorized. Authorization is provided in the cross-memory installation. Multiple versions of this online interface can coexist in one TSO library concatenation.

Do *one* of the following:

- Add a STEPLIB DD statement for the library that contains the load modules to the LOGON procedures for those TSO users who are going to use the ISPF/cross-memory online retrieval option.
- Provide the load library using the ISPF LIBDEF facility.

Note: If multiple versions of CA Deliver are going to be running simultaneously, or you want to also run a previous version of RMOSPF or RMOTSO, concatenate the load library you want RMOSPF or RMOTSO to use first.

More information:

Step 6: Modify the Skeleton JCL (see page 74)

Step 2: Add Panel and Command Table Libraries to TSO LOGON

If you are going to run CA Deliver under ISPF, proceed with this step. For Version 3 or higher, both the command table library and the panel library are used.

To add panel and command table libraries to the TSO LOGON procedure:

1. Concatenate the command table library CAI.CVDETBL0 to DD statement ISPTLIB.
2. Concatenate the panel library CAI.CVDEPNL0 to DD statement ISPPLIB.

Note: If you also plan to use RMOSPF (the ISPF interface), and multiple versions of CA Deliver, concatenate CAI.CVDETBL0 first. Use the CAI.CVDETBL0 from the most current release.

Step 3: (Optional) Modify an ISPF Selection Menu to Select Online Retrieval

If you want to add a selection code to one of the ISPF selection menus for the online retrieval feature, proceed with this step; otherwise, your ISPF detailed instructions are complete.

Note: If you add a selection code, you are able to select the online retrieval feature in the same way you select other ISPF options.

Use the value next to the NAME parameter on your Initialization Parameter Worksheet for PARM (high-level database name).

Use the values in this table for either SPF or ISPF.

Type	Selection Code is Defined As
ISPF (all versions)	'PGM(EC2XMSPF) PARM(high-level-database-name) NEWAPPL(RMO)'
SPF	'PGM(EC2XMSPF) PARM(high-level-database-name)'

Panel Libraries

The names of the panel libraries vary from site to site and for the different releases of ISPF. These panel libraries are allocated to the ISPPLIB DD statement under TSO.

Be aware that some installations do not allow direct modifications of IBM panels and libraries. In this case, you can place the modified panels in user or site-specific libraries and concatenate them ahead of the IBM libraries.

Ask your system administrator for the specific ISPF panel library that applies to your site and contains the panel ISR@PRIM.

Note: The selection menus shown in these examples are part of the program product ISPF and are copyrighted by IBM.

Example 1

This example shows you how to add selection code R to the primary option menu ISR@PRIM for ISPF. The bright, offset text identifies the inserted lines.

```
----------------------  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           +PF KEYS   - &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, CLIST, OR REXX EXEC
%   7 +DIALOG TEST - PERFORM DIALOG TESTING
%   8 +LM UTILITIES- PERFORM LIBRARY ADMINISTRATOR UTILITY FUNCTIONS
%   C +CHANGES     - DISPLAY SUMMARY OF CHANGES FOR THIS RELEASE
%   R +RMOSPF      - DELIVER ADMINISTRATION
%   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 /* TUTORIAL INDEX - 1ST PAGE         */
)PROC
  &ZSEL = TRANS( TRUNC (&ZCMD,'.')
               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(ISPYXDR) PARM(ISR) NOCHECK'
               8,'PANEL(ISRLPRIM)'
               C,'PGM(ISPTUTOR) PARM(ISR00005)'
               R,'PGM(EC2XMSPF) PARM(RMO.SYSTEM1) NEWAPPL(RMO)'
               T,'PGM(ISPTUTOR) PARM(ISR00000)'
              ' ',' '
                X,'EXIT'
                *,'?' )
   &ZTRAIL = .TRAIL
 )END
```

Note:

- NEWAPPL(RMO) is required and must be specified as shown previously in this section.

  This parameter is used with the command table library concatenation from Step 3 of the ISPF Installation Instructions.

- NEWAPPL(RMO) allows CA Deliver to correctly interpret commands and program function key invocation.

  If this parameter is not specified, certain PF keys such as the scroll keys may not function.

Example 2

This example shows you how to add selection code R to the primary option menu ISP@PRIM for SPF. Shading identifies the inserted lines.

```
%----------------------  SPF—MVS PRIMARY OPTION MENU  ---------------
%OPTION  ===>_OPT
%                                                              +USERID   -
%   0 +ISPF PARMS  -     SPECIFY TERMINAL AND USER PARAMETERS   +TIME     -
%   1 +BROWSE      -     DISPLAY SOURCE DATA OR OUTPUT LISTINGS +TERMINAL —
%   2 +EDIT        -     CREATE OR CHANGE SOURCE DATA           +PF KEYS  -
%   3 +UTILITIES   -     PERFORM SPF UTILITY FUNCTIONS
%   4 +FOREGROUND  -     COMPILE, ASSEMBLE, OR DEBUG
%   5 +BACKGROUND  -     COMPILE, ASSEMBLE, OR LINK EDIT
%   6 +COMMAND     -     ENTER TSO COMMAND OR CLIST
%   7 +SUPPORT     -     TEST DIALOG OR CONVERT MENU/MESSAGE FORMATS
%   8 +LM UTILITIES-     PERFORM LIBRARY ADMINISTRATOR UTILITY FUNCTIONS
%   R +RMOSPF      -     DELIVER ADMINISTRATION
%   T +TUTORIAL    -     DISPLAY INFORMATION ABOUT SPF
%   X +EXIT        -     TERMINATE SPF USING LIST/LOG DEFAULTS
%
+PRESS%END KEY TO TERMINATE SPF+
%
)INIT
  .HELP = TTUTOR
  &ZHTOP = TTUTOR   /* TUTORIAL TABLE OF CONTENTS        */
  &ZHINDEX = TINDEX /* TUTORIAL INDEX - 1ST PAGE         */
)PROC
  &ZSEL = TRANS( TRUNC (&OPT,'.')
                0,'PANEL(ISPOPT)'
                1,'PGM(ISRBRO)'
                2,'PGM(ISPEDIT)'
                3,'PANEL(ISPUTIL)'
                4,'PANEL(ISPFORA)'
                5,'PANEL(ISRJOB)'
                6,'PGM(ISPTSO)'
                7,'PANEL(ISPOTAC)'
                R,'PGM(EC2XMSPF) PARM(RMO.SYSTEM1)'
                T,'PGM(ISPTUTOR) PARM(T)'
                ' ',' '
                 X,'EXIT'
                 *,'?' )
 )END
```

Example 3

This example shows you how to add selection code 3.R as a sub-option to the utilities menu ISPUTIL for ISPF.

The bright, offset text identifies the inserted lines.

```
     %-----------------------  UTILITY SELECTION MENU  -----------------
%OPTION  ===>_OPT         +
%                                                                      +
%   1 +LIBRARY        LIBRARY UTILITY:
+                     PRINT INDEX LISTING OR ENTIRE DATASET
+                     PRINT, RENAME, DELETE, OR BROWSE MEMBERS
+                     COMPRESS DATASET
%   2 +DATASET        DATASET UTILITY:
+                     DISPLAY DATASET INFORMATION
+                     ALLOCATE, RENAME, OR DELETE ENTIRE DATASET
+                     CATALOG OR UNCATALOG DATASET
%   3 +MOVE/COPY      MOVE OR COPY MEMBERS OR DATASETS
%   4 +CATALOG        CATALOG MANAGEMENT:
+                     DISPLAY OR PRINT CATALOG ENTRIES
+                     INITIALIZE OR DELETE USER CATALOG ALIAS
%   5 +RESET          RESET STATISTICS FOR MEMBERS OF ISPF LIBRARY
%   6 +HARDCOPY       INITIATE HARDCOPY OUTPUT
%   7 +VTOC           DISPLAY OR PRINT VTOC ENTRIES FOR A DASD VOLUME
%   8 +OUTLIST        DISPLAY, DELETE, OR PRINT HELD JOB OUTPUT
%   9 +SCRIPT/VS      FORMAT, DISPLAY, AND OPTIONALLY PRINT SCRIPT TEXT
%   R +RMOSPF         DELIVER ADMINISTRATION
)INIT
  .HELP = TU
)PROC
  &SEL = TRANS( TRUNC (&OPT,'.')
                1,'PGM(ISPUDA) PARM(UDA1)'
                2,'PGM(ISPUDA) PARM(UDA1)'
                3,'PGM(ISPUMC)'
                4,'PGM(ISPUCA)'
                5,'PGM(ISPURS)'
                6,'PGM(ISPUHC)'
                7,'PGM(ISPUVT)'
                8,'PGM(ISPUOL) PARM(UOL01)'
                9,'PGM(ISPUSC) PARM(SCRPTA)'
                R,'PGM(EC2XMSPF) PARM(RMO.SYSTEM1) NEWAPPL(RMO)'
               ' ',' '
                 *,'?' )
 )END
```

ISPF Cross-Memory Notes

Be aware of the following:

- The primary RMOXMS region must be started with the XMSSUB=YES parameter.
- The XMSSUB=YES parameter must only be used in an XMS address space with a default subsystem ID (SUBSYS=XMC2 or not specified).
- If multiple RMOXMS regions are started, they must be started with XMSSUB=NO parameter.

  Only the primary XMS region can have XMSSUB=YES specified.
- The XMS regions must have the XMS=YES parameter to make it accessible.
- The EBCXMCTR table must be assembled during installation to define the relationship between CA Deliver and CA View database high-level qualifiers. The table contains an EBCXMOPT macro to define initialization options and the EBCXMTRN macro for each CICS user transaction.

The EBCXMTRN macro also contains options for the specific database as follows:

- SUBSYS= parameter of the cross-memory task must match the SUBSYS= parameter specified in the EBCXMCTR table entry.
- RECON=YES can be used to allow reconnection (after an ISPF terminal error) at the point of exit.
- TIMEOUT= specifies how long ISPF will wait for the XMS session to respond after the user enters input, in seconds.

  We recommend as high a value as possible but not less than 240 (4 minutes).

To abort the XMS session and return the user to ISPF or the TSO command prompt, press the ATTN key.

Note: The SUBMAX= parameter controls the number of user connections, not the USERMAX= parameter. USERMAX= only applies when you are using the subtask with the CICS interface.

Install the TSO/Cross-Memory Online Retrieval Option

Important! This interface requires cross-memory services to be installed. For more information, see the topic Installing Cross-Memory Services in this chapter.

Note: The parameter XMSSUB must be set to YES in the JCL for the cross-memory services task.

Installation Steps

The following steps are required to install the TSO/Cross-Memory Online Retrieval Option. Each step is explained in detail in the sections that follow.

1. (Optional) Add STEPLIB DD Statements to the TSO LOGON procedures if the load modules were not copied to a linklist library.
2. (Optional) Set Up the TSOXMS Driver Program.

Step 1: (Optional) Add STEPLIB DD Statements

The action you take in this step depends on what you did during the base-product installation—specifically, did you:

- Authorize the program load library or
- Copy the modules to a system authorized library

If the CA Deliver load modules were *not* copied to one of the libraries in the linklist, proceed with this step; otherwise go to the next step.

To add STEPLIB DD statements (for the library containing the CA Deliver load modules) to the TSO LOGON procedures, do the following:

- Add a STEPLIB DD statement for the library that contains the CA Deliver load modules to the LOGON procedures for those TSO users who are to use the ISPF/Cross-Memory Online Retrieval Option.

Note: For this interface, the libraries do not have to be APF authorized—authorization is provided in the cross-memory installation. Multiple releases of this online interface can coexist in one TSO library concatenation.

Step 2: (Optional) Set up the TSOXMS Driver Program

To create user CLISTs to execute the CA Deliver TSOXMS driver program, issue:

```
EC2XMTSO highlevel.databasename
```

TSO Cross-Memory Notes

Be aware of the following:

- The primary RMOXMS region should be started with the XMSSUB=YES parameter.
- The XMSSUB=YES parameter must only be used in an XMS address space with a default subsystem ID (SUBSYS=XMC2 or not specified).
- If multiple RMOXMS regions are started, they must be started with XMSSUB=NO parameter.

  Only the primary XMS region can have XMSSUB=YES specified.
- The XMS regions must have the XMS=YES parameter to make it accessible.
- The EBCXMCTR table must be assembled during installation to define the relationship between CA View and CA Deliver database high-level qualifiers. The table contains an EBCXMOPT macro to define initialization options and the EBCXMTRN macro for each CICS user transaction.

The EBCXMTRN macro also contains options for the specific database as follows:

- SUBSYS= parameter of the cross-memory task.

  This parameter must match the SUBSYS= parameter specified in the EBCXMCTR table entry.
- RECON=YES can be used to allow reconnection (after a TSO terminal error) at the point of exit.
- TIMEOUT= specifies how long TSO will wait for the XMS session to respond after the user enters input, in seconds.

  We recommend as high a value as possible but not less than 240 (4 minutes).

To abort the XMS session and return the user to ISPF or the TSO command prompt, press the ATTN key.

Note: The SUBMAX= parameter controls the number of user connections, not the USERMAX= parameter. USERMAX=only applies when you are using the subtask with the CICS interface.

Install the VTAM Online Retrieval Option

Important! This facility uses the cross-memory feature distributed with CA Deliver and must be installed with that feature. For more information about cross-memory feature, see the Install Cross-Memory Services section in this chapter.

Installation Steps

The following steps are required to install the VTAM online retrieval option. Each step is explained in detail in the sections that follow.

1. Define the Application Program to VTAM.
2. (Optional) Create a USS Table Definition.

Step 1: Define the Application Program to VTAM

Add this application program definition to SYS1.VTAMLST:

```
* SYS1.VTAMLST(rmomajor)
rmomajor VBUILD TYPE=APPL
rmovtam  APPL  ACBNAME=rmovtam,AUTH=(PASS,ACQ),EAS=nn
```

where:

rmomajor

Specifies the application program major node name.

Use the SYS1.VTAMLST member name. The member name must be unique and must not be the same as the names on the APPL statement.

AUTH=(PASS,ACQ)

Is required when the cross-memory parameter VTAMPASS=YES is used to support multiple cross-memory regions.

If VTAMPASS=NO, you can specify AUTH=(ACQ). For more information about the VTAMPASS parameter, see the Add the Start Procedure for the Cross-Memory Online Task step in this chapter.

EAS=nn

Specifies the approximate number of concurrent sessions.

rmovtam

Specifies the minor node name of the application program.

- This name must be unique within the network domain; it is the APPLID referenced in the USS definition table or LOGON command.
- This name is also specified on the cross-memory RMOAPPL parameter.
- If not specified, the network-unique name (the name of the APPL definition statement) is used.

Step 2: (Optional) Create a USS Table Definition

To simplify the manner in which a user logs on to VTAM online retrieval, you can create a USS definition table for CA Deliver.

Example

Assume that two CA Deliver systems have been created. The databases for the two systems have high-level names of RMO.SYSTEM1 and RMO.SYSTEM2, and you want a user to simply enter one of the commands to log on to VTAM online retrieval for the respective systems:

```
RMO1
RMO2
```

Create a USS definition table as follows:

```
USSTAB
*
*    ENTRY FOR RMO1
*
USSCMD  CMD=RMO1,REP=LOGON,FORMAT=PL1
USSPARM PARM=APPLID,DEFAULT=RMOVTAM
USSPARM PARM=LOGMODE
USSPARM PARM=DATA,DEFAULT=RMO.SYSTEM1
*
*    ENTRY FOR RMO2
*
USSCMD  CMD=RMO2,REP=LOGON,FORMAT=PL1
USSPARM PARM=APPLID,DEFAULT=RMOVTAM
USSPARM PARM=LOGMODE
USSPARM PARM=DATA,DEFAULT=RMO.SYSTEM2
USSEND
```

VTAM Cross-Memory Notes

Be aware of the following:

- For VTAM only regions, you can start the primary RMOXMS task with the XMSSUB=NO parameter. However if this is not a VTAM only region, we recommend that you start the primary RMOXMS region with the XMSSUB=YES parameter.
- If multiple RMOXMS regions are started, they must be started with XMSSUB=NO parameter.

  Only the primary XMS region can have XMSSUB=YES specified.
- VTAM only XMS regions can have the XMS=NO parameter to make it accessible.
- All XMS interfaces require the EC2XMCTR table. You must assemble the table during installation to:
  - Define the relationship between CA Deliver and CA View database high-level qualifiers and the session options to be used
  - Provide information used to build the XMS database table. Only the database high-level qualifier is used for VTAM XMS users.
- Specify the RMOAPPL=*applid* parameter. This parameter provides VTAM user signon capability.

  Note: When you are using multiple VTAM XMS regions, each region must have a unique *applid*.
- To pass VTAM signon requests to other XMS regions, specify the VTAMPASS=YES parameter.
- When you are using multiple VTAM XMS regions, the values for LGNFMT=, RMOVDTB=, VTMQUERY=, and VTMSAA= must be the same in each region. Otherwise, the XMS interface may react in unpredictable ways.
- To activate the VTAM generic resource support for your cross memory regions, specify the VGRAPPL= parameter.

  Note: For more information about VTAM generic resources, see the following topic.

VTAM Generic Resource Name

If the VGRAPPL parameter is specified in an EMAS complex, this parameter specifies a common VTAM generic resource name for the entire EMAS complex.

Specifying the common VTAM generic resource name in the session request can initiate VTAM cross memory sessions to any of the EMAS members.

When you are using the VTAM generic resource name, by default VTAM tries to request a session with an EMAS member in the same MVS image.

If it is not possible to get the session that was requested, VTAM uses normal load balancing when passing the session request to one of the active EMAS members.

Install the CA Roscoe/Cross-Memory Online Retrieval Option

The CA Roscoe/cross-memory online retrieval option runs as a command processor under ETSO/Roscoe.

Important! This interface requires cross-memory services to be installed. For more information about cross-memory services, see the Install Cross-Memory Services section in this chapter. Be sure to set the parameter XMSSUB to YES in the JCL for the cross-memory services task.

Installation Steps

The following steps are required to install the CA Roscoe/Cross-Memory Online Retrieval Option. Each step is explained in detail in the sections that follow.

1. (Optional) Concatenate the Load Module Library to the ETSOLIB DD statement, if the load modules were not copied to a linklist library.
2. Add the control statement for the RMOROS command processor to the Eligible Program List (EPL).
3. Invoke CA Roscoe/Cross-Memory Online Retrieval.

Step 1: (Optional) Concatenate the Load Module Library

If the load modules were *not* copied to a linklist library, concatenate the library that contains the load modules to the ETSOLIB DD statement in the CA Roscoe startup JCL, .

Note: If you have CA View, the CA View load modules must also be either in the linklist or in a ETSOLIB statement with this step.

Step 2: Add RMOROS Command Processor Statements

Important! This step is for CA Roscoe 6.0 and Higher.

Add these EPL control statements to member ETSOPGMS for the CA Roscoe user with the RO prefix:

Column	Contents
1–8	EC2XMROS
9	Blank
10–12	Number of users allowed to access CA Deliver at one time
13	Blank
14–17	CPU time slice (use 9999 to prevent premature termination)
18	Blank

Column	Contents
19–24	Maximum memory (in KB) below the 16 MB line This memory is only for the cross-memory driver program (50 KB is ample)
25	Blank
26–31	Maximum memory (in KB) below the line that CA Deliver can acquire at one time Use 999999 so that GETMAINs are not limited
32	Blank
33–38	Maximum memory (in KB) above the 16 MB line This memory is only for the cross-memory driver program (50 KB is ample)
39	Blank
40–45	Maximum memory (in KB) above the line that CA Deliver can acquire at one time Use 999999 so that GETMAINs are not limited
46	Blank
47–48	CP to call EC2XMROS as a TSO command processor
49	Y – Application authorized to issue MODESET SVC
50	Blank
51-52	CP to call EC2XMROS as a TSO command processor
53-255	Ignored

CA Roscoe Cross-Memory Notes

Be aware of the following:

- Start the primary RMOXMS region with the XMSSUB=YES parameter.

  The XMSSUB=YES parameter must only be used in an XMS address space with a default subsystem ID (SUBSYS=XMC2 or not specified).

- If multiple RMOXMS regions are started, they must be started with XMSSUB=NO parameter.

  Only the primary XMS region can have XMSSUB=YES specified.

- The XMS regions must have the XMS=YES parameter to make it accessible.
- The EBCXMCTR table must be assembled during installation to define the relationship between CA View and CA Deliver database high-level qualifiers.

  The table contains an EBCXMOPT macro to define initialization options and the EBCXMTRN macro for each CICS user transaction.

The EBCXMTRN macro also contains options for the specific database as follows:

- SUBSYS= parameter of the cross-memory task.

  This parameter must match the SUBSYS= parameter specified in the EBCXMCTR table entry.

- RECON=YES can be used to allow reconnection (after a TSO terminal error) at the point of exit.
- TIMEOUT= specifies how long TSO is to wait for the XMS session to respond after the user enters input, in seconds.

  We recommend as high a value as possible but not less than 240 (4 minutes).

Note: The SUBMAX= parameter controls the number of user connections, not the USERMAX= parameter. USERMAX=only applies when using the subtask with the CICS interface.

Install the CICS Pseudo-Conversational Option

Important! This option uses the cross-memory feature distributed with CA Deliver and must be installed with that feature. For more information about cross-memory, see Install Cross-Memory Services.

Installation Steps

The following steps are required to install the CICS Pseudo-Conversational Option. Each step is explained in detail in the sections that follow.

1. Place the CA Deliver load libraries into DFHRPL and STEPLIB.
2. Code the PCT and PPT Table Entries to CICS.
3. (Optional) Prepare the interface to a user-written CICS menu system.

Step 1: Add Modules to DFHRPL and STEPLIB

The CA Deliver load library is required in the CICS DFHRPL and in the STEPLIB in the CICS region.

Note: If the CAI.CVDELOAD load library is in the linklist, it does not have to be included as a STEPLIB in the CICS region

Be sure that these modules are available in the DFHRPL concatenation of libraries.

1. EC2CICUX
2. EC2CIEND
3. EC2CINIT
4. EC2CISRV
5. EC2XMCIC
6. EC2C*version-number*

   Where:

   release-number represents the CICS release number.

   - CTS 3.1 release number: 0640
   - CTS 3.2 release number: 0650
   - CTS 4.1 release number: 0660
   - CTS 4.2 release number: 0670
   - CTS 5.1 release number: 0680
   - CTS 5.2 release number: 0690

You can copy the six modules to the DD statement DFHRPL in your CICS task. However, we strongly recommend that you concatenate CAI.CVDELOAD to the DD statement DFHRPL.

Note: Several CA Deliver modules are loaded (MVS load) from the CICS STEPLIB or LINKLIST. Verify that the entire CA Deliver load library is defined in the CICS STEPLIB or is included in the linklist.

Step 2: Define Transaction and Programs to CICS

To access CA Deliver using CICS, define the required transactions and programs for the CICS interface. The sample job to make these definitions is located in the CVDEJCL member CICSDLVR. For more information about the CICS interface, see this JCL.

Note: Define a separate, unique transaction identifier for each CA Deliver database that you want to access under CICS.

CICS Resource Definition Online Storage Protection

If you have CICS storage protection activated, resource definition online settings are required, as follows:

- For all transactions:

  ```
  TASKDATALOC=ANY
  TASKDATAKEY=CICS
  ```

- For all programs:

  ```
  DATALOCATION=ANY
  EXECKEY=CICS
  ```

PLT Start-up List

Add these table entries to the last phase of the PLT startup list to initialize the subtask that is used for cross-memory access:

```
DFHPLT TYPE=ENTRY,PROGRAM=DFHDELIM
DFHPLT TYPE=ENTRY,PROGRAM=EC2CINIT
```

PLT Shutdown List

Add these table entries to the first phase of the PLT shutdown list to ensure that the subtask that executes as part of the CA Deliver online facility correctly shuts down when CICS shuts down:

```
DFHPLT TYPE=ENTRY,PROGRAM=EC2CIEND
DFHPLT TYPE=ENTRY,PROGRAM=DFHDELIM
```

Optional DCT Entries

Specify a value for the DESTID parameter in the EBCXMOPT macro in the EC2XMCTR module and corresponding DCT entries. This value defines a transient data destination for messages issued by the subtask.

Note: Specify a blank for DESTID to suppress the generation of informational messages from the subtask.

The DCT entries for a DESTID of XMC2 are:

```
RMOLOG   DFHDCT TYPE=SDSCI,   FOR CICS MESSAGES AND SHUTDOWN
               BLKSIZE=250,   STATISTICS
               BUFNO=1,
               DSCNAME=RMOLOG,
               RECFORM=VARUNBM,
               RECSIZE=242,
               TYPEFLE=OUTPUT
XMC2G    DFHDCT TYPE=EXTRA,
               DESTID=XMC2,
               DSCNAME=RMOLOG
```

Step 3: (Optional) Invoke the System from a CICS Menu System

If you want to invoke CA Deliver from a user-written CICS menu system, then return to that menu system when you exit from CA Deliver, do the following:

Invoke CA Deliver from the menu system by using this CICS command:

```
EXEC CICS START TRANSID(DELIVER transaction-id)
     TERMID(EIBTRMID)
     FROM(data-area)
     LENGTH(4)
```

where:

TRANSID(DELIVER transaction-id)

Specifies the CA Deliver transaction ID.

TERMID(EIBTRMID)

Specifies the terminal that a CA Deliver transaction will communicate with.

FROM (data-area)

Specifies the optional variable length character string.

The format of the data-area parameter is:

tran,

where:

tran

Specifies the return menu CICS transaction to be started when CA Deliver finishes.

Note: None of the data-area parameters is required.

LENGTH (4)

Specifies the number of bytes in the data field being passed.

Note:

When CA Deliver receives control, it retrieves the four-byte return transaction ID and saves it from iteration to iteration.

If the retrieve fails, CA Deliver retains the information that it was started directly from a terminal, not a menu system.

When CA Deliver finishes processing, it determines whether it should return to a menu system by starting the return transaction.

If there is a saved transaction ID, CA Deliver starts the return transaction before it exits to CICS by issuing:

```
EXEC CICS START TRANSID(RETURN transaction-id)
     TERMID(EIBTRMID)
     NOCHECK
```

CICS Notes

The cross memory CICS access involves two different address spaces: the CICS address spaces and the XMS address spaces.

CICS Address Spaces

The user's CICS transactions and the cross memory support subtask reside in the address spaces.

- If multiple CICS regions are used to access CA Deliver, each CICS region will have an XMS support subtask.
- If you are using CICS/MRO, CA Deliver normally runs in an AOR (application region).

XMS Address Spaces

Be aware of the following:

- The primary RMOXMS region can be started with the XMSSUB=YES or XMSSUB=NO parameter.
- CICS has a router subtask in its region and does not require the XMSSUB=YES function. However, we recommend that you start the primary XMS region with XMSSUB=YES.
- If multiple RMOXMS regions are started, they must be started with XMSSUB=NO parameter.

  Only the primary XMS region can have XMSSUB=YES specified.
- The XMS regions must have the XMS=YES parameter to be accessible.
- The SUBSYS= parameter must match the EC2XMCTR table entry for the CICS transaction.

- The EBCXMCTR table must be assembled during installation to define the relationship between CA View and CA Deliver database high-level qualifiers.

  The table contains an EBCXMOPT macro to define initialization options and the EBCXMTRN macro for each CICS user transaction.

The EBCXMTRN macro also contains options for the specific database as follows:

- SUBSYS= parameter can be used to route the CA Deliver transaction to an alternate XMS subsystem ID. The SUBSYS= of the cross memory task must match the SUBSYS= parameter specified in the EBCXMCTR table entry.
- TRANID=parameter specifies the CA Deliver transaction identifier for CICS.
- RECON=YES can be used to allow reconnection (after a CICS terminal error) at the point of exit.

  Note: Do not specify RECON=YES if you use a multi-session manager that assigns LU names from a pool of names. Coding RECON=YES under these conditions could allow a user to be connected to another user's session. For more information, see Multi-Session Managers later in this chapter.
- TIMEOUT= specifies how long CICS is to wait for the XMS session to respond after the user enters input, in seconds.

  We recommend as high a value as possible but not less than 240 (4 minutes).

CICS XMS Subtask Startup

Use *one* of these methods to start the XMS subtask automatically:

1. When the CICS region is started, use the DFHPLTPI definition to automatically start the XMS subtask.
2. Define a transaction for the EC2CINIT program to allow for manual startup.
3. Write a CICS program to transfer control (XCTL) to EC2CINIT when you want to start the XMS subtask.

Until the XMS subtask is started, expect the transactions referencing EC2XMCIC to terminate with an error message that indicates that the XMS subtask is not active.

Note:

- When the CICS region is terminated, the DFHPLTSD definition is to be used to terminate the XMS subtask.

  You can manually terminate the XMS subtask through a user application program that LINKs the EC2CIEND or you can use the optional transaction defined for EC2CIEND for manual termination.

- If you want to terminate the XMS subtask manually, we recommend that you use the DFHPLTSD entry to terminate the XMS subtask. This definition is needed to clean up linkages to the XMS address spaces.
- To prevent users from shutting down the XMS subtask, secure the optional transaction for program EC2CIEND.

Multi-Session Managers Using Virtual LU Names

Multi session manager products, for example CA TPX Session Management (CA TPX), can be configured to assign an LU name to a user's terminal at the time the user selects the CICS application.

Important! This assignment means that a user can enter CICS each time with a different terminal ID which can cause problems for CA Deliver application.

For example: If a user uses a multi-session manager to end a session, or shuts the PC down, CA Deliver does not know that the user has left. Another user might select CICS, be assigned to the same LU name as the previous user, and enter CA Deliver with the same terminal ID as the previous user. CA Deliver believes that there are two active users on the same terminal.

To prevent this situation, you can add a small amount of code to the CICS Autoinstall Control Program.

Note: The default name of this program is DFHZATDX and its source is located in SDFHSAMP.

If you are not a CICS systems programmer, discuss this situation with the person in your company who is responsible for CICS support and maintenance.

The sample code that follows shows how to clear an active user from the CA Deliver application at terminal deletion time. Insert this code in your Autoinstall Control Program.

The source that is shipped with CICS contains this line:

* ==> *PUT DELETE CODE HERE*

Insert the code after that line.

```
          LOAD  EP=EC2XSLOC,ERRET=RETURN
          LR    R6,R0                  GET EBCXSLOC ADDRESS
          ICM   R8,B'1111',0(R6)       ADDR OF MAIN CONTROL BLOCK
          BZ    RETURN                 GET OUT IF NONE
          LA    R7,4(,R8)              LOOK LIKE FIRST USER BLOCK
XSU_LOOP DS    0H
          ICM   R7,B'1111',8(R7)       USER BLOCK ADDR
          BZ    RETURN                 GET OUT IF DONE
          CLC   DELETE_TERM_ID,104(R7) FOR THIS TERMINAL?
          BNE   XSU_LOOP               NO
          TM    120(R7),X'01'          ACTIVE ENTRY?
          BZ    XSU_LOOP               NO
          OI    120(R7),X'02'          SHOW SESSION DONE
          B     RETURN                 EXIT PROGRAM
```

This code does the following:

1. Attempts to load program EC2XSLOC
   - If the load fails, this is not the region containing CA Deliver and it exits.
   - If CA Deliver is active in this region, the first word of EC2XSLOC contains the address of the main control block.

     If this word is zero, CA Deliver is not active and the program exits.
2. Scans the chain of CA Deliver user control blocks to find the terminal to be deleted
   - If the program finds the terminal ID, it makes sure that the user block is in use and is active, and then it clears the appropriate fields.
   - If the block does not represent an active user, the program continues to search the chain to the end.
   - If the program gets to the end of the chain without finding the terminal ID, the program exits.
   - If you implement this change to the terminal deletion section of the Autoinstall Control Program, you can prevent the problems caused by the methods that were used to leave the CA Deliver application.

Install the IMS Online Retrieval Option

Use these steps to install the IMS online retrieval option.

Important! This facility uses the cross-memory feature distributed with CA Deliver and must be installed with that feature. For more information about cross-memory, see Installing Cross-Memory Services.

Installation Steps

This list summarizes the steps required to install the IMS Online Retrieval Option. Detailed instructions are in the sections that follow.

1. Code the IMS TRANSACT, PSB and APPLCTN macros.
2. Run the PSB, ACB, and SYSGEN Procedures.
3. Load EC2IMSUX Modules.
4. Move load modules to IMSVS.PGMLIB.

Important! All JCL and macros provided in this section are provided as general examples only and must be modified for your site's systems and standards.

Step 1: Code the Macros

Use the examples in this section as a guide as you code these macros, and implement them in your IMS system.

- (IMS) TRANSACT macro
- PSB macros
- APPLCTN macro

TRANSACT Macro

One or more transactions must be defined for the IMS online retrieval program RMOXMIMS. Normally, only one transaction identifier is defined, although you can define multiple transactions.

This TRANSACT macro identifies the RMOXMIMS transaction to IMS:

```
TRANSACT NAME=EC2XMIMS,SPA=(18)
```

PSB Macros

This PSB must be generated for the EC2XMIMS transaction:

```
PCB       TYPE=TP,ALTRESP=YES,MODIFY=YES
PSBGEN    PSBNAME=EC2XMIMS,LANG=ASSEM,COMPAT=YES
```

APPLCTN Macro

This APPLCTN must be generated for the RMOXMIMS transaction:

```
APPLCTN    PSB=EC2XMIMS
```

Step 2: Run the PSB, ACB, and SYSGEN Procedures

Use the macros created in Step 1. Code the Macros as input for these procedures:

```
PSBGEN
ACBGEN
IMS SYSGEN
```

Step 3: Load EC1IMSUX Modules

Move load modules EC2IMSUX to IMSVS.PGMLIB.

Note: EC2IMSUX is in CAI.CVDELOAD and must be copied to IMSVS.PGMLIB.

IMS Notes (New Version)

Be aware of the following:

- The new IMS/DC Transaction Program (EC2XMIMS) is a replacement for the older RMOXMIMS program.
- The EC2XMIMS does not need to be linkedited to the ASMTDLI interface program. The transaction is now conversational with a SPASIZE=18 (this can be adjusted).
- If you use extended color, the SEGSIZE= may need to be increased, because extended color data streams can be a 50% increase over the monochrome data stream size.

  To determine the SEGSIZE= value, take the terminal that will use the interface with the largest screen size, in bytes, and apply this formula:

  ```
  ROWS * COLS * 1.5 = SEGSIZE
  ```

  For example, a 3278-5 with a 27 x 132 screen size would be (27 * 132 * 1.5) = 5346. If the SEGSIZE= is too small, the terminal user will get an RC= "A6" message indicating that a message insert failed.

IMS/DC Parameter Relationships

The cross-memory IMS/DC access involves up to three different address spaces as follows:

- IMS/DC message processing region address spaces

  The user's IMS/DC transaction resides here. If multiple IMS/DC users are processing concurrently (input being processed by the XMS system), a separate IMS/DC message region is used for each user.

  IMS/DC can control the maximum number of IMS/DC transactions executing at one time.

- The XMS support subtask
  - The subtask is started when the XMSSUB=YES input parameter is used when an XMS address space is started.
  - The subtask can be in a separate XMS address space or share the address space with XMS or VTAM sessions.
  - The XMSSUB=YES must only be used in an XMS address space with a default subsystem ID (SUBSYS=XMC2 or not specified).
  - If multiple XMS address spaces are started, only one can have the XMSSUB=YES specified.

  Note: All IMS/DC, TSO/XMS, ISPF/XMS and CA Roscoe/XMS sessions share the same XMS subtask.

- XMS address spaces

  See the topic that follows.

IMS/DC Cross-Memory Notes

Be aware of the following:

- The primary RMOXMS region is to be started with the XMSSUB=YES parameter.

  This region can be in a separate XMS address space or share the address space with XMS or VTAM sessions.

- The XMSSUB=YES parameter must only be used in an XMS address space with a default subsystem ID (SUBSYS=XMC2 or not specified).

- If multiple RMOXMS regions are started, they must be started with XMSSUB=NO parameter.

  Only the primary XMS region can have XMSSUB=YES specified.

- The XMS regions must have the XMS=YES parameter to make it accessible.

- The EBCXMCTR table must be assembled during installation to define the relationship between CA View and CA Deliver database high-level qualifiers. The table contains an EBCXMOPT macro to define initialization options and the EBCXMTRN macro for each CICS user transaction.

The EBCXMTRN macro also contains options for the specific database:

- SUBSYS= parameter of the cross-memory task.

  The parameter must match the SUBSYS= parameter specified in the EBCXMCTR table entry.

- RECON=YES can be used to allow reconnection (after an ISPF terminal error) at the point of exit.

- TIMEOUT= specifies how long ISPF is to wait for the XMS session to respond after the user enters input, in seconds.

  We recommend a value as high as possible but not less than 240 (4 minutes).

To abort the XMS session and return the user to ISPF or the TSO command prompt, press the ATTN key.

Note: The SUBMAX= parameter controls the number of user connections, not the USERMAX= parameter. USERMAX=only applies when you are using the subtask with the CICS interface.

To control screen size manually, use these operands. The SNA query command can also be used to determine the device characteristics.

Enter	For Terminal Type
M2	3278-2 24 x 80 default screen size
M2H	3278-2 24 x 80 highlighting

Enter	For Terminal Type
M2X	3279-2 24 x 80 color highlighting
M2C	3279-2 24 x 80 color
M3	3278-3 32 x 80
M3H	3278-3 32 x 80 highlighting
M3X	3279-3 32 x 80 color highlighting
M3C	3279-3 32 x 80 color
M4	3278-4 43 x 80 highlighting
M4H	3278-4 43 x 80 highlighting
M4X	3279-4 43 x 80 color highlighting
M4C	3279-4 43 x 80 color
M5	3278-5 27 x 132
M5H	3278-5 27 x 132 highlighting
M5X	3279-5 27 x 132 color highlighting
M5C	3279-5 27 x 132 color
M6	3290 62 x 80
M6H	3290 62 x 80 highlighting
M7	3290 31 x 160
M7H	3290 31 x 160 highlighting
M8	3290 62 x 160
M8	3290 62 x 160 highlighting

For other modifications to your system, see your VTAM programmer.

TSO, ISPF, CA Roscoe and Cross-Memory Address Spaces

TSO, ISPF, or CA Roscoe cross-memory access involves address spaces and subtasks as follows:

- TSO or CA Roscoe address spaces

  The TSO command, ISPF, or CA Roscoe application program resides here. If ISPF/XMS is being used with ISPF split-screen active, up to two sessions can be executing at the same time, to the same database or different databases.

- The XMS support subtask

  This subtask is started when XMSSUB=YES input parameter is used when starting an XMS address space. The subtask can be in a separate XMS address space, or it can share the address space with XMS or VTAM sessions.

  - The XMSSUB=YES must only be used in an XMS address space with a default subsystem ID (SUBSYS=XMC2 or not specified).
  - If multiple XMS address spaces are started, only one can have the XMSSUB=YES specified.

  Note: All IMS/DC,TSO/XMS, ISPF/XMS, and CA Roscoe/XMS sessions share the same XMS subtask.

- XMS address spaces

  The XMS regions must have the XMS=YES parameter to make them accessible.

  Note: The SUBSYS= parameter must match the EC2XMCTR table entry for the database.

  Multiple address spaces can be used if needed.

Multiple Cross-Memory Region Requirements

Be aware of the following:

- All cross-memory regions started under the same SUBSYS ID are chained together.
- The REGIONID positional parameter is the first value of the PARM= statement for the cross-memory task.

  You must specify a different REGIONID for each started cross-memory region.
- The value of the XMSSUB parameter for the primary region depends on the type of XMS region you are defining.

See this table for the XMSSUB values. Specify XMSSUB=NO for all other started regions.

Primary Region Type	XMSSUB Recommendation
Non-VTAM	Must use XMSSUB=YES
CICS	Recommend using XMSSUB=YES
VTAM-only	XMSSUB=NO use allowed

Note:

- You must specify XMS=YES for all other started regions except for VTAM only regions where XMS=NO is permissible.
- Each VTAM cross-memory region requires a different *applid*. The *applid* is specified using the RMOAPPL= parameter.
- Each VTAM cross-memory region requires VTAMPASS=YES.
- The VTAM administrator must verify that each VTAM cross-memory applid has this setting:

  ```
  AUTH=(PASS,ACO).
  ```

Prepare to Start the Cross Memory Task

Follow these steps:

1. (Optional) Add the start procedure to PROCLIB for the cross-memory online task.
2. (Optional) Modify, assemble, and link edit the EC2XMCTR module.
3. Define security requirements for CA Top Secret Security (eTrust CA-Top Secret).

Start the Cross Memory Task

Start the XMS CBROSDRV procedure.

Chapter 9: Installing the Features

This chapter describes the CA Deliver features and provides information about how to:

1. Change the date format on panels
2. Set up the CA 11 interface
3. Set up CA 11 to run with CA Deliver
4. Install the CA GSS (Global Subsystem) interface
5. Install the CA Deliver host command environment into CA GSS

This section contains the following topics:

Change the Date Format Shown on Panels

The date format, date separator character, and time separator characters are specified in the RMODFMT load module.

The date format is specified in the first byte (hex location 00) of the load module as a hexadecimal value of 00 through 07 as follows:

Date Format	Hexadecimal Value
MM/DD/YYYY (default)	00
DD/MM/YYYY	01
YYYY/MM/DD	02
YYYY/DD/MM	03
MM/DD/YY	04
DD/MM/YY	05
YY/MM/DD	06
YY/DD/MM	07

- A date separator character can be assigned in the second byte (hex location 01) of the load module. The default data separator is a slash (/).
- A time separator character can be assigned in the third byte (hex location 03) of the load module.

  The default time separator is a colon (:).

  Note: Use printable characters that are not likely to be confused with syntactical data, such as a comma or a quotation mark for the date and time separator characters.
- Use USERMOD BRNSDFMT in CAI.CVDEJCL to set values in RMODFMT.

  Change the values in the REP statements in the AMASPZAP input to the values that you want.

For example, if you selected MM/DD/YY for your default format, a dash (-) for the date separator, and no change for the time separator, change the AMASPZAP statements in BRNSDFMT as follows:

From:
```
++ZAP(RMODFMT).
 NAME RMODFMT RMODFMT
 VER  0000  0061,7A00
 REP  0000  0061,7A00
$$
```

To:
```
++ZAP(RMODFMT).
 NAME RMODFMT RMODFMT
 VER  0000  0061,7A00
 REP  0000  0460,7A00
$$
```

- The first field in the VER and REP statements contains the location in the module that is being changed. In this case, it is 0000. Do not change this value.
- The second field contains four hexadecimal values separated into groups of two by a comma.
- The VER statement verifies that the values in this statement are the same as the values found at location 0000 in RMODFMT.
- The REP statement gives the values that will replace the data at location 0000 in RMODFMT.

In the preceding example:

- The first position in field 2 in the REP statement was changed from 00 to 04 to specify the MM/DD/YY date format as defined in the preceding table.

- The second position was changed from 61 (/) to 60 (-).
- The third position is unchanged since we are not changing the time separator in this example.
- The fourth position is never changed.

Note: If you want to make a change to RMODFMT, you must reapply this USERMOD.

Set Up the CA 11 Interface

To set up an interface between CA 11 and CA Deliver, verify that one or more of the following conditions exist:

- You use two or more CA Deliver databases.
- CA Deliver and CA 11 run on different operating systems and use the CA Deliver network input feature.
- Another vendor program is installed which does not allow you to specify the CA Deliver database name through parameters on the EXEC statement.
- You use both CA Deliver and CA Balancing Report Control (CA Balancing).

To set up an interface between CA 11 and CA Deliver:

1. Create a sequential data set to specify parameters for the CA Deliver and CA 11 interface program.

   In this data set, specify the names of the CA Deliver databases and the destination where CA 11 runs.

2. If CA 11 is executing on a different operating system, specify the name of this data set in the RMOPARMS DD statement when you set up the CA 11 procedure catalog for CA Deliver.

   In this data set, specify the subsystem name of the CA L-Serv Database Manager that is to manages the CA Balancing database (if CA Balancing is used with CA Deliver).

Data Set Attributes

These attributes are needed to specify the data set referenced in the RMOPARMS DD statement:

- DSORG=PS
- RECFM=FB
- LRECL=80

Data Set Statements

In this data set, specify these two control statements:

- One or more names of the CA Deliver databases that are used.
- The name of the JES2 or JES3 destination on which CA 11 runs, if it is executing on a different operating system.

Syntax of Control Statements in the Data Set

The syntax of the statement used to specify the name of a CA Deliver database is:

```
NAME high-level-name
```

where *high-level-name* represents the name of the CA Deliver database.

The syntax of the statement used to specify the name of the destination on which CA 11 runs is:

```
FROM-NODE NAME=JES2/JES3-dest-where-CA 11-runs
```

where *JES2/JES3-dest-where-CA 11-runs* represents the name of the originating destination on which CA 11 runs.

These control statements are also described in the *Reference Guide*.

If there are identical job definitions in different CA Deliver databases, maintain the order of the CA Deliver databases in the data set referenced in the RMOPARMS DD statement for your entire execution.

Set Up CA 11 to Run with CA Deliver

To use CA 11 with CA Deliver and store reports in CA View, use CA View Release 11.6 or higher and CA Deliver Release 11.6 or higher, and then follow these steps:

1. Change the program name in the first step of your JCL for the CA 11 job:

```
//STEP1    EXEC    PGM=U11RMS,PARM='U11RMS-parms', or,
//STEP1    EXEC    PGM=UCC11RMS,PARM='UCC11RMS-parms'
```

2. Change the utility name RMORMS:

   ```
   //STEP1     EXEC     PGM=RMORMS,PARM='U11RMS-parms', or,
   //STEP1     EXEC     PGM=RMORMS,PARM='UCC11RMS-parms'
   ```

   If the program in the CA 11 JCL shown above is anything other than U11RMS, or if you have any program that wraps around the CA 11 program, contact CA Technical Support.

   Note: For a description of RMORMS, see the *Reference Guide*.

3. Do *one* of the following:

   - If two or more CA Deliver databases are used or CA Balancing is used, add this RMOPARMS DD data set name statement to the JCL for the CA 11 job:

     ```
     //RMOPARMS     DD     DSN=sequential-data set-name,DISP=SHR
     ```

   - If only one is used, insert the name of the single CA Deliver database as a parameter in front of the CA 11 program name parameters:

     ```
     //STEP1    EXEC     PGM=RMORMS,PARM='RMO-db;U11RMS-parms', or,
     //STEP1    EXEC     PGM=RMORMS,PARM='RMO-db;UCC11RMS-parms'
     ```

4. Determine if CA Deliver executes on a destination other than CA 11 and if the CA Deliver network input feature is used, then do *one* of the following:

   - If the answer is yes to one of the above, go to Step 5.
   - If the answer is no to both of the above, go to Step 9.

5. Insert this statement on the last line of the RMOPARMS data set:

   ```
   FROM-NODE JES2/JES3-dest-where-CA 11-runs
   ```

6. Insert the following DD statement in the first step (the RMORMS Step) of your JCL:

   ```
   //RMONETn  DD  SYSOUT=(x,,form-name),DEST=dest-where-RMO-runs
   ```

   Note: CA Deliver uses the output from this DD statement to determine whether the job that is currently running is a rerun job.

7. Set the initialization parameter NETRERUN to YES.

8. Load the CA Deliver modules to the destination where CA 11 is going to execute:

   - EC2MSG
   - EC2SDIM
   - EC2SVC35
   - RMORCH
   - RMORMS

9. Set the initialization parameter MAXHIST to the maximum number of generations that are expected to rerun jobs.

To back out only reports produced within the last five generations, set MAXHIST=5.

Note: If the historical data report that you want to rerun has been purged, CA Deliver cannot delete or flag these reports. You must manually delete these reports.

For more information about deleting reports manually, see the *CA Deliver Administrator Guide*.

10. To rerun jobs that produce bundled reports and to specify when and how the bundles are to be produced, use:
    - The LATE, INTERVAL, WAIT, and BUNDLE CONFIRM fields on the Bundle Definition Attributes panel
    - The Print Bundle Now tabular command P on the Active Bundle List panel

    Note: For more information about the Bundle Definition Attributes Panel, the Active Bundle List panel and the Print Bundle Now tabular command P, see the *Administration Guide*.

    CA Deliver cannot delete or flag bundle-holding copies if bundles have already been queued for printing.

    The RMORMS utility transmits the current rerun information from the originating system on which CA Deliver is not installed to the receiving systems.
11. Review the RMSWARN initialization parameter in the *Reference Guide*. This parameter affects how RMORMS reacts when the started task is not active.

Install the Host Command Environment into CA GSS

CA GSS (Global Subsystem) for MVS Release 2.6 is required for this installation.

To install the CA Deliver host command environment interface module into CA GSS, do the following:

1. Be sure that MVS/TSO is running.
2. Ensure that CA GSS is installed on your system.
3. Look at the data set and member that are allocated to the PARMLIB DDNAME in CA GSS.
4. Edit the data set/member and add the following line:

   ADDRESS DELIVER RMOINTF
5. Add the CA Deliver load library to the concatenation of the CA GSS command procedure.
6. Restart CA GSS.

Appendix A: Installation Worksheets

This appendix contains worksheets to use to record your installation, initialization, and started task parameters

This section contains the following topics:

Installation Worksheet

This worksheet contains the SMP/E and system-related items required for the product installation. Fill out this worksheet carefully and retain this information for future reference.

Step 1: Global Install Parameters

- Enter \ and your standard SYSOUT class for CA product installs and SMP output.

  Default: SYSOUT=_____ SYSOUT=_____

- Enter the name for the started task.

  Default: STCNAM=CAHBB0ST STCNAM=_____

Step 2: Data Set Qualifiers and SMP Parameters

- Enter the data set high-level qualifiers you plan to assign to the common distribution, target, and SMP libraries.

  Default: CAI='CAI.' CAI=_____

  Default: DSHLQ='CAI.' DSHLQ=_____

- Enter your generic unit name for permanent work DASD volumes.

  Default: PERMDA=SYSDA PERMDA=_____

- Enter your generic unit name for temporary work DASD volumes.

  Default: WORK=SYSDA WORK=_____

- Enter the DASD pack you plan to use as your SMP temporary library volume.

  Default: TLIB=DUMSER TLIB=_____

Initialization Parameter Worksheet

Parameter	Value
ARCH	
ARCH__	
ARCH__	
ARCH__	
ARCH__	
ARCH__	
ARCH__	
ARCH__	
ARCH__	
ARCH__	
ARCH__	
ARCH__	
ARCH__	
AUTHTID	
AUTOACT	
BANNER	
BEGINDAY	
BNDLBNR1	
BNDLBNR2	
BNDLBNR3	
BNDLCLS	
BNDLCONF	
BNDLDEST	

Parameter	Value
BNDLHDTL	
BNDLINT	
BNDLMOUT	
BNDLSCAN	
BNDLWAIT	
BOT	
CCX	
DAYS	
DEFDEL	
DEFOUT	
DEFREPRT	
DEFRVIEW	
DYNRCHAR	
EFORMAT	
EMAILQ	
EXTSEC	
FEATURE	
FREEALL	
GSS	
HDETAIL	
HISTCNT	
INBSSN	
JOBCLSL	
JOBREF	
LOGO	
MAXHIST	
MAXJESQ	
NAME	
NETCLSL	
NETDEST	

Parameter	Value
NETFORM	
NETONLY	
NETREQUE	
NETRERUN	
NETUNDEF	
OFFPW	
OUTPUT	
PRBTASK	
PREVRUN	
REDISP	
RMSWARN	
RPTENQ	
RPTNPROD	
SAR	
SARBUFCT	
SECMSG	
SETCMD	
SETPAGE	
SETPW	
SMF	
SMF30	
START	
STKCHNn	
STKMODE	
STKNOTXT	
STNAMEn (1, 2, 3, 4, 5)	
STOPPW	
SYSCLSL	
SYSID	

Parameter	Value
TEXT	
TIME	
WARNING	
WEBSVR1	
WEBSVR2	
WEBSVR3	
WEBSVR4	
WRITER	

Started Task Worksheet

Use this worksheet to list the data set names that are to be used in various steps of the installation process.

Initialization Parameter

DDname: RMOPARMS

Data set name: _____

Job Name Translation Control

DDname: RMOJTAB

Data set name: _____

Appendix B: Integration with CA OPS/MVS EMA

This section contains the following topics:

Overview

CA Deliver provides seamless integration with CA OPS/MVS by automatically communicating both active status events and heart beat events to CA OPS/MVS. The enabling technology for this is through a generic event API call that CA OPS/MVS provides the other mainframe products so that they can communicate events to CA OPS/MVS.

You do not need to do anything for CA Deliver to enable this event communication interface to CA OPS/MVS. If CA Deliver and CA OPS/MVS are active in the same z/OS image, CA Deliver automatically communicates these automation events to CA OPS/MVS.

By generating active status events CA Deliver and other CA products are able to communicate to CA OPS/MVS's System State Manager (SSM) component when they are starting, up, stopping or down.

SSM is a built-in feature that uses an internal relational data framework to proactively monitor and manage started tasks, online applications, subsystems, JES initiators, and other z/OS resources including your CA mainframe products. SSM compares the current state of online systems, hardware devices, and the other resources with their desired state, and then automatically makes the necessary corrections when a resource is not in its desired state. This provides proactive and reactive state management of critical resources.

Before the CA OPS/MVS interface existed, CA OPS/MVS could automate active status events for your CA products; however this typically required monitoring unique messages for each CA product. With this interface, CA OPS/MVS can capture these events for any of your CA products with a single automation event rule.

With the heart beat event, CA Deliver can communicate a normal, warning, or problem overall health status and reasoning to CA OPS/MVS on a regular interval. Once CA Deliver begins generating heart beat events for CA OPS/MVS, CA OPS/MVS can also react to the lack of a heart beat event from CA Deliver, treating this as an indication that there is either a potential problem with CA Deliver, or there is a larger system-level problem that is taking place.

Ensure that CA OPS/MVS Is Enabled for Capturing These Events

To ensure that this CA OPS/MVS interface is active, make sure the CA OPS/MVS parameter APIACTIVE is set to its default of ON. This allows CA OPS/MVS to acknowledge and process the events generated by CA Deliver and other CA products through this interface.

CA Deliver Active State Events

CA Deliver provides a direct interface to the CA OPS/MVS System State Manager (SSM) application to notify CA OPS/MVS of the current operating state of the given CA Deliver address space. The CA OPS/MVS SSM application can use this information to automatically control the operation of the CA Deliver address space, as well as any other address space that is dependent upon the CA Deliver address space being active. For more information on using CA OPS/MVS SSM see the CA OPS/MVS User Guide.

The CA Deliver product active state is presented to CA OPS/MVS and can be processed by the following rule:

```
)API CASTATE
```

The available OPS/REXX variables for CA Deliver product state management are:

OPS/REXX Variable	Value
API.APPLICATION	CA Deliver
API.VERSION	Current release
API.LEVEL	00000
API.EVENTID	CASTATE
API.MSGID	CASTATE
API.TEXT	State of CA Deliver

The API.TEXT variable has the following format:

State of *appl_id* is *current_state*'

appl_id

Specifies the same value as the API.APPLICATION variable

current_state

STARTING

Indicates that CA Deliver is initializing

UP

Indicates that CA Deliver is active

STOPPING

Indicates that CA Deliver is terminating

DOWN

Indicates that CA Deliver is exiting the system

For more information on how to use the CASTATE API, see the member SSMCAAPI of opsmvsHLQ.STATEMAN.RULES.

CA Deliver Heartbeat Events

CA Deliver provides a continuous heartbeat event directly to CA OPS/MVS. CA OPS/MVS can use this information in several ways to determine the operational health of the CA Deliver product.

CA Deliver issues a heartbeat update every nnnn seconds that notifies CA OPS/MVS of the current operational health of the CA Deliver product.

If CA Deliver detects a health state change, it immediately generates a heartbeat update without waiting for the nnnn second heartbeat interval to expire. In this way, CA Deliver provides CA OPS/MVS with a constant operational health state view of the CA Deliver product.

CA OPS/MVS can also react to the lack of a heartbeat update from CA Deliver and an indication that there is either a potential problem with CA Deliver, or there is a larger system level problem that is taking place.

The CA Deliver product heartbeat event is presented to CA OPS/MVS and can be processed by the following rule:

```
)API CAHEARTBT
```

The available OPS/REXX variables for CA Deliver state management are:

OPS/REXX Variable	Value
API.APPLICATION	CA Deliver
API.VERSION	Current release
API.LEVEL	00000
API.EVENTID	CAHEARTBT
API.MSGID	CAHEARTBT
API.TEXT	State of CA Deliver

The API.TEXT variable has the following format:

appl_id Status: *heartbeat*_state Reason: reason_text

appl_id

Specifies the value of the API.APPLICATION variable.

heartbeat_state

Heart_beat_state can be one of the following:

NORMAL

Indicates that CA Deliver is operating normally, without any detected problems.

WARNING

PROBLEM

reason_text

reason_text explains the problem as reported by the event API call.

For information on how you use the CAHEARTBT API, see members APIHRTB1, APIHRTB2, and APIHRTB3 of opsmvsHLQ.SAMPLE.RULES.

Index

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X