CA Hyper-Buf® VSAM Buffer Optimizer

Installation Guide

r11.5

CA Technologies Product References

This document references the following CA Technologies products:

- CA Hyper-Buf® VSAM Buffer Optimizer (CA Hyper-Buf)
- CA Mainframe Software Manager™ (CA MSM)
- CA Top Secret® (CA Top Secret)
- CA ACF2™ (CA ACF2)

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

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

Contents

Chapter 1: Overview

This guide describes how to install and implement CA Hyper-Buf.

This section contains the following topics:

Audience

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

- JCL
- TSO/ISPF
- z/OS environment and installing software in this environment
- z/OS UNIX System Services
- Your IT environment, enterprise structure, and region structure

Consult with the following personnel, as required:

- Systems programmer for z/OS definitions
- Storage administrator for DASD allocations
- Security administrator for security changes

How the Installation Process Works

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

- Acquisition—Transports the software to your z/OS system.
- Installation using SMP/E—Optionally creates a new CSI 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 MSM provides a web-based interface to make the standardized installation process easier. Using CA MSM, someone with limited knowledge of JCL and SMP/E can install a product.

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

To install your product, do the following:

1. Prepare for the installation by confirming that your site meets all installation requirements (see page 11).
2. Use one of the following methods to acquire the product:
   - Download the software from CSO using CA MSM (see page 15).
   - Download the software from CSO using Pax-Enhanced Electronic Software Delivery (ESD) (see page 21).
   - Order a tape.
3. Perform an SMP/E installation using one of the following methods:
   - If you used CA MSM to acquire the product, start the SMP/E step from the SMP/E Environments tab in CA MSM.
   - If you used ESD to acquire the product, you can install the product manually or use the Insert New Product option in CA MSM to complete the SMP/E install.
   - If you used a tape (see page 45), 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 MSM, deployment is required; it is a prerequisite for configuration.
   - If you are using a manual process, deployment is an optional step.

   Note: Deployment is considered part of starting your product (see page 53).

Chapter 2: Preparing for Installation

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

This section contains the following topics:

Hardware Requirements

CA Hyper-Buf has the following hardware requirements:

- IBM mainframe zSeries or equivalent.
- One or more 3380, 3390, or equivalent disk drives is required.

Note: If you are using IBM's Storage Management Subsystem (SMS), you must not mix device types in a storage group used for CA Hyper-Buf.

Software Requirements

CA Hyper-Buf has the following software requirements:

- An IBM-supported version of the z/OS operating system.
- TSO with ISPF/PDF must be installed on the system.
- Installation of CA Hyper-Buf requires installation of CA Common Services for z/OS. CA Common Services for z/OS component CAIRIM is required for CA LMP support. CA LMP is required by all CA products.

CA Technologies Common Services Requirements

The CA License Management Program (CA LMP) provides a standardized and automated approach to the tracking of licensed software. It uses common realtime enforcement software to validate the user's configuration. CA LMP reports on activities related to the license, usage, and financials of CA products. The routines which accomplish this are integrated into the CA z/OS dynamic service code, S910 (the CAIRIM service). CA LMP features include:

- Common Key Data Set can be shared among many CPUs.
- *Check digits* are used to detect errors in transcribing key information.
- Execution Keys can be entered without affecting any CA software product already running.
- No special maintenance requirements.

The CAI Resource Initialization Manager (CAIRIM) 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 commonly encountered when installing system software. These routines are grouped under the CA MVS Dynamic Service Code, S910. CAIRIM features include:

- Obtaining SMF data
- Verification of proper software installation
- Installation of MVS interfaces
- Automatic startup of CA and other vendor products
- Proper timing and order of initialization

LMP Key Requirements

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:

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

CA Hyper-Buf is licensed with an LMP key. You acquire the LMP key with one of the following methods:

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

Storage Requirements

Target Libraries

Library Name	Tracks	Description
CBS3LINK	60	Common load library
CBS3PROC	15	Common procedure library
CBS3OPTN	15	Common options library
CBS3MENU	15	ISPF message library
CBS3PENU	15	ISPF panel library
CBS3JCL	15	Sample JCL library
CBS3SAMP	15	Various samples library
CBS3CLS0	15	CLIST library
CBS3XML	15	XML library

Distribution Libraries

Library Name	Tracks	Description
ABS3MOD0	60	Load library
ABS3PROC	15	Procedure library
ABS3OPTN	15	Options library
ABS3MENU	15	ISPF message library
ABS3PENU	15	ISPF panel library
ABS3JCL	15	Sample JCL library
ABS3SAMP	15	Samples library
ABS3CLS0	15	CLIST library
ABS3XML	15	XML library

Concurrent Releases

You can continue to use your current release while installing this release of CA Hyper-Buf in another SMP/E CSI environment. If you plan to continue to run a previous release, consider the following points:

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

  Note: CA MSM installs into a new CSI by default.
- Define DDDEF entries in your new zones to point SMP/E to the proper libraries for installation. Verify that they point to the new release libraries.

Chapter 3: Installing Your Product Using CA MSM

These topics provide information to get you started managing your product using CA MSM. You can use the online help included in CA MSM to get additional information.

Before using these topics, you must already have CA MSM installed at your site. If you do not have CA MSM installed, you can download it from the Download Center at the CA Support Online website, which also contains links to the complete documentation for CA MSM.

How to Use CA MSM: Scenarios

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

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

How to Acquire a Product

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

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

Follow these steps:

1. Set up a CA Support Online account.

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

2. Determine the CA MSM URL for your site.

   To access CA MSM (see page 19), you require its URL. You can get the URL from your site's CA MSM administrator and log in using your z/OS credentials. When you log in for the first time, you are prompted to create a CA MSM account with your credentials for the CA Support Online website. This account enables you to download product packages.

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

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

   If you cannot find the product you want to acquire, update the catalog. CA MSM refreshes the catalog through the CA Support Online website using the site IDs associated with your credentials for the CA Support Online website.

4. Download the product installation packages.

   After you find your product in the catalog, you can download the product installation packages.

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

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

How to Install a Product

The *Software Installation Service (SIS)* facilitates the installation and maintenance of mainframe products in the software inventory of the driving system. This facilitation includes browsing downloaded software packages, managing SMP/E consolidated software inventories on the driving system, and automating installation tasks.

You can use the SIS component of CA MSM to install a CA Technologies product.

Follow these steps:

1. Initiate product installation and review product information.
2. Select an installation type.
3. Review installation prerequisites if any are presented.

4. 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: Either create a target zone or use an existing target zone.
     c. Set up the distribution zone: Either 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.
5. Review the installation summary and start the installation.

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 MSM before beginning the deployment process.

How to Maintain Existing Products

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

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

Follow these steps:

1. Migrate the CSI to CA MSM to maintain an existing CSI in CA MSM.

   During the migration, CA MSM stores information about the CSI in the database.
2. Download the latest maintenance for the installed product releases from the Software Catalog tab.

   If you cannot find a release (for example, because the release is old), you can add the release to the catalog manually and then update the release to download the maintenance.

3. Apply the maintenance.

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

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

How to Deploy a Product

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

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

Follow these steps:

1. Set up the system registry:
   a. Determine the systems you have at your enterprise.
   b. Set up remote credentials for those systems.
   c. Set up the target systems (Non-Sysplex, Sysplex or Monoplex, Shared DASD Cluster, and Staging), and validate them.
   d. Add FTP information, including data destination information, to each system registry entry.
2. Set up methodologies.
3. Create the deployment, which includes completing each step in the New Deployment wizard.

   After creating the deployment, you can save it and change it later by adding and editing systems, products, custom data sets, and methodologies, or you can deploy directly from the wizard.

   Note: If you must deploy other products to the previously defined systems using the same methodologies, you must create a separate deployment.
4. Deploy the product, which includes taking a snapshot, transmitting to target, and deploying (unpacking) to your mainframe environment.

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

Access CA MSM Using the Web-Based Interface

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

Follow these steps:

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

   The login page appears.

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

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

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

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

3. Click New.

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

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

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

   You are prompted to review your user settings.

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

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

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

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

Chapter 4: Installing Your Product from Pax-Enhanced ESD

This section contains the following topics:

How to Install a Product Using Pax-Enhanced ESD

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

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

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

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

1. Allocate and mount the file system. This process requires a USS directory to receive the pax file and to perform the unpack steps. We recommend that you allocate and mount a file system that is dedicated to Pax-Enhanced ESD and create the directory in this file system. Ensure that all users who will be working with pax files have write authority to the directory.

2. Copy the product pax files into your USS directory. To download files, choose one of the following options:

   - Download a zip file from CA Support Online to your PC, unzip the file, and then upload the product pax files to your USS file system.
   - FTP the pax files from CA Support Online directly to your USS directory.

   Note: Perform Steps 3 through 6 for each pax file that you upload to your USS directory.

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

   pax `-rvf` *pax-filename*

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

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

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

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

More Information:

USS Environment Setup (see page 26)
Allocate and Mount a File System (see page 27)
Copy the Product Pax Files into Your USS Directory (see page 30)
Create a Product Directory from the Pax File (see page 35)
Copy Installation Files to z/OS Data Sets (see page 36)
Receive the SMP/E Package (see page 37)

How the Pax-Enhanced ESD Download Works

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

Use the following process to download files using Pax-Enhanced ESD:

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

   The CA Support Online web page appears.

2. Under Download Center, select Products from the first drop-down list, and specify the product, release, and genlevel (if applicable), and click Go.

   The CA Product Download window appears.

3. Download an entire CA Technologies product software package or individual pax files to your PC or mainframe. If you download a zip file, you must unzip it before continuing.

   For both options, The ESD Product Download Window (see page 23) topic explains how the download interface works.

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

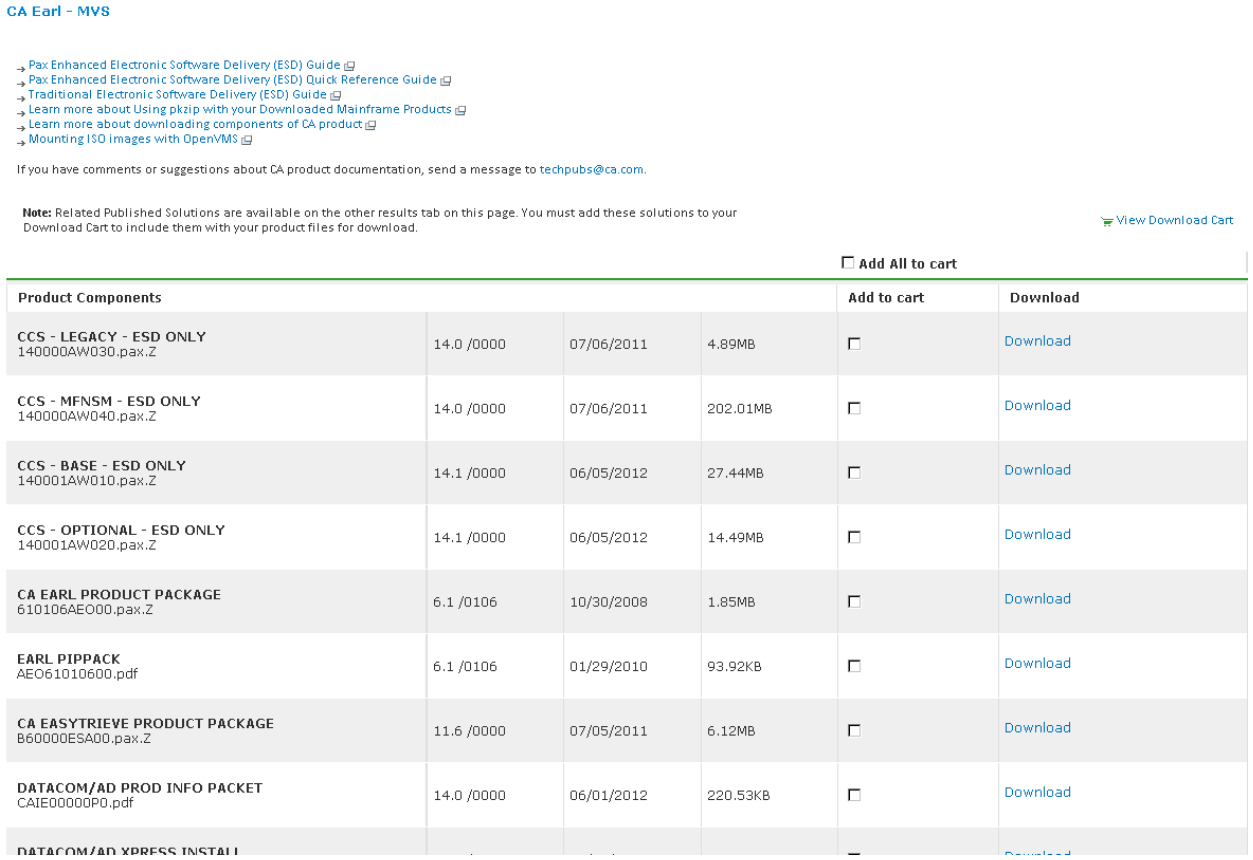
4. Perform the steps to install the product based on the product-specific steps.

   The product is installed on the mainframe.

ESD Product Download Window

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

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



CA Earl - MVS

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

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

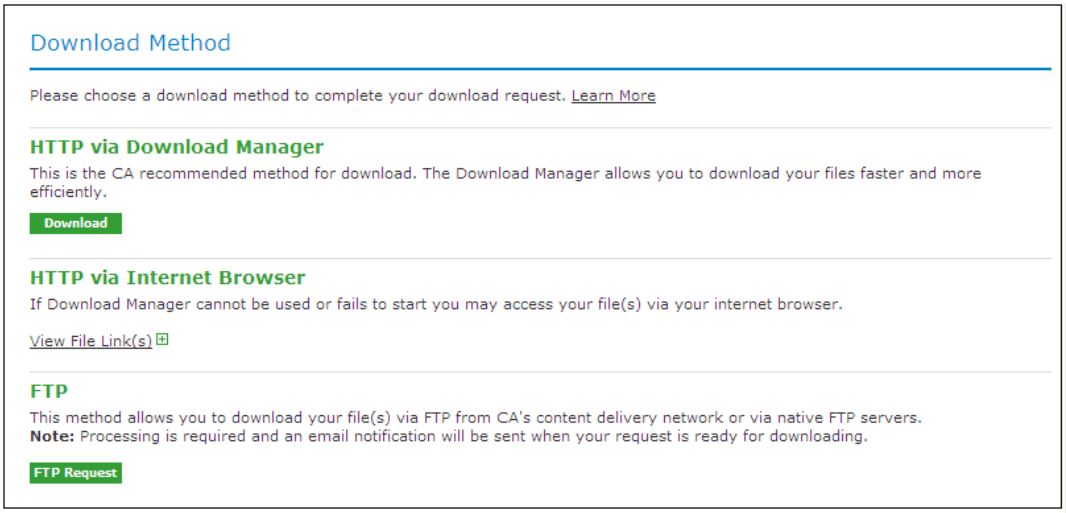
Note: Related Published Solutions are available on the other results tab on this page. You must add these solutions to your Download Cart to include them with your product files for download.

View Download Cart

Add All to cart

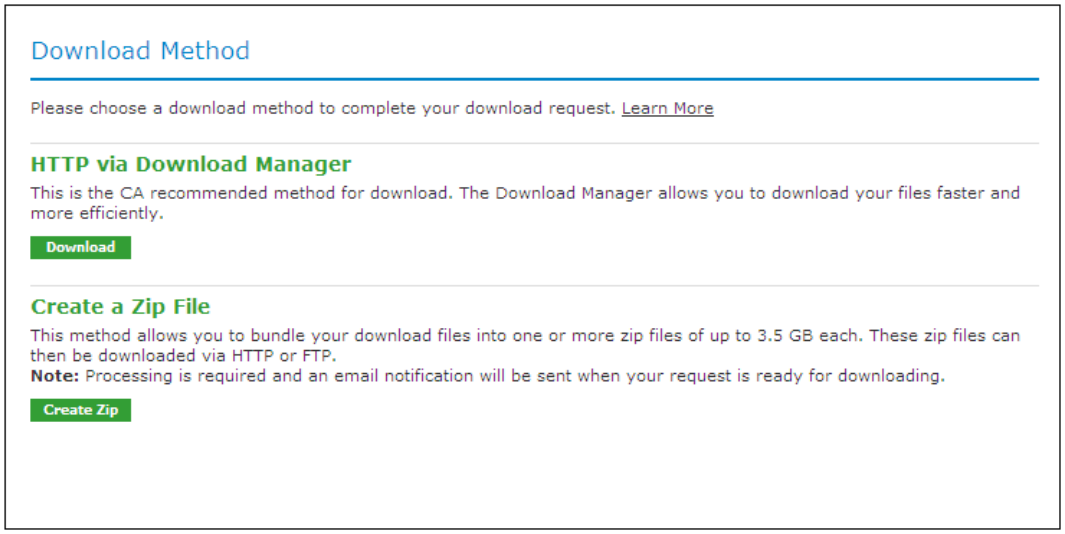
Product Components				Add to cart	Download
CCS - LEGACY - ESD ONLY 140000AW030.pax.Z	14.0 /0000	07/06/2011	4.89MB	☐	Download
CCS - MFNSM - ESD ONLY 140000AW040.pax.Z	14.0 /0000	07/06/2011	202.01MB	☐	Download
CCS - BASE - ESD ONLY 140001AW010.pax.Z	14.1 /0000	06/05/2012	27.44MB	☐	Download
CCS - OPTIONAL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

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



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

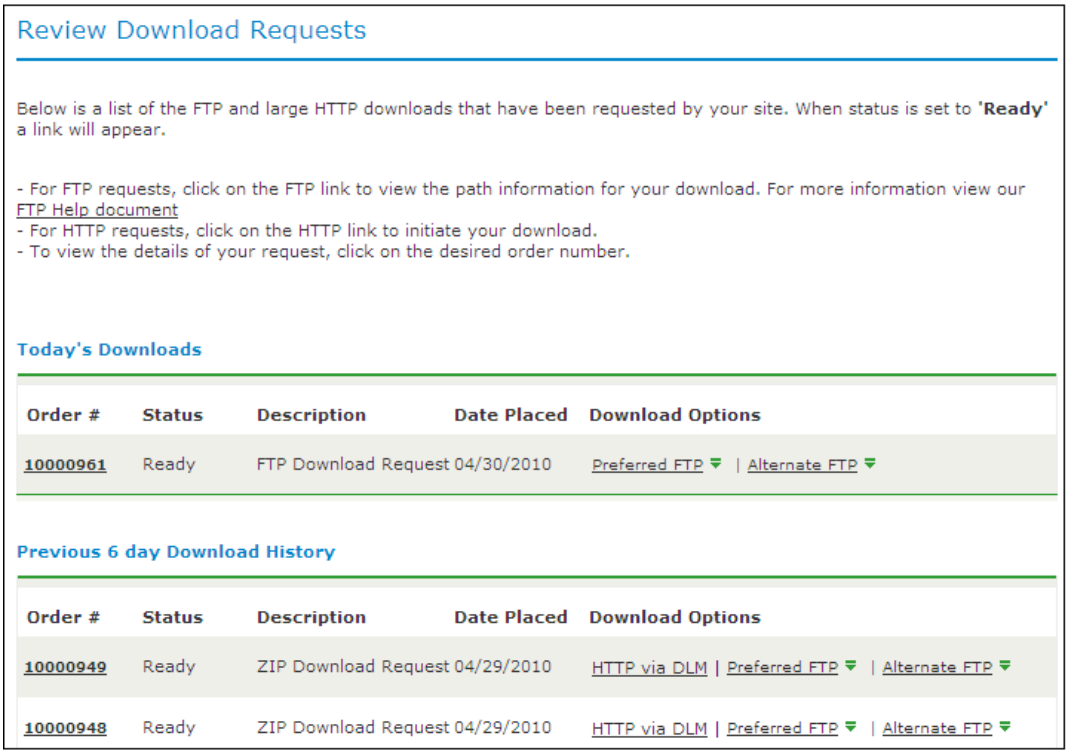
Note: For mainframe downloads using this HTTP method, click the Learn More link.



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

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

The Create a Zip File option first creates the zip, and when ready, offers the options that the Zip Download Request examples show in the next illustration.



Review Download Requests

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

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

Today's Downloads

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

Previous 6 day Download History

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

USS Environment Setup

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

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

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

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

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

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

Allocate and Mount a File System

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

This procedure describes how to perform the following tasks:

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

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

  Important! USS commands are case-sensitive.

Follow these steps:

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

   - On a zFS, use the following sample:

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

   - On an HFS, use the following sample:

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

   The file system is allocated.

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

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

   ```
   cd /u/maint/
   mkdir CA
   cd CA
   mkdir CAESD
   ```

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

   The mount point is created.

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

   - On a zFS, use the following sample:

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

   - On an HFS, use the following sample:

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

   The file system is mounted.

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

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

   Write access is granted.

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

Copy the Product Pax Files into Your USS Directory

To begin the CA Technologies product installation procedure, copy the product pax file into the USS directory that you set up. Use one of the following methods:

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

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

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

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

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

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

More Information:

How the Pax-Enhanced ESD Download Works (see page 23)
ESD Product Download Window (see page 23)

Download Using Batch JCL

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

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

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

Follow these steps:

1. Supply a valid JOB statement.
2. Replace *yourTCPIP.PROFILE.dataset* with the name of the TCP/IP profile data set for your system. Consult your local network administrators, if necessary.

   The job points to your profile.
3. Replace *YourEmailAddress* with your email address.

   The job points to your email address.
4. Replace *yourUSSESDdirectory* with the name of the USS directory that you use for ESD downloads.

   The job points to your USS directory.
5. Locate the product component to download on the CA Support Product Download window.

   You have identified the product component to download.
6. Click Download for the applicable file.

   Note: For multiple downloads, add files to a cart.

   The Download Method window opens.
7. Click FTP Request.

   The Review Download Requests window displays any files that you have requested to download.

   Note: We send you an email when the file is ready to download or a link appears in this window when the file is available.

8. Select one of the following methods:

   Preferred FTP

   Uses CA Technologies worldwide content delivery network (CDN). If you cannot download using this method, review the security restrictions for servers that company employees can download from that are outside your corporate network.

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

   Alternate FTP

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

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

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

   Note: The following links provide details regarding FTP: the FTP Help document link in the Review Download Requests window and the Learn More link available in the Download Methods window.

9. Submit the job.

   Important! If your FTP commands are incorrect, it is possible for this job to fail and still return a zero condition code. Read the messages in the job DDNAME SYSPRINT to verify the FTP succeeded.

   After you run the JCL job, the pax file resides in the mainframe USS directory that you supplied.

Example: CAtoMainframe.txt, JCL

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

```
//GETPAX   JOB (ACCOUNTNO),'FTP GET ESD PACKAGE',
//          MSGCLASS=X,CLASS=A,NOTIFY=&SYSUID
//*********************************************************************
//* This sample job can be used to download a pax file directly from  *
//* CA Support Online to a USS directory on your z/OS system.         *
//*                                                                   *
//* When editing the JCL ensure that you do not have sequence numbers *
//* turned on.                                                        *
//*                                                                   *
//* This job must be customized as follows:                           *
//* 1. Supply a valid JOB statement.                                  *
//* 2. The SYSTCPD and SYSFTPD JCL DD statements in this JCL may be   *
//*    optional at your site. Remove the statements that are not      *
//*    required. For the required statements, update the data set     *
//*    names with the correct site-specific data set names.           *
//* 3. Replace "Host" based on the type of download method.           *
//* 4. Replace "YourEmailAddress" with your email address.            *
//* 5. Replace "yourUSSESDdirectory" with the name of the USS         *
//*    directory used on your system for ESD downloads.               *
//* 6. Replace "FTP Location" with the complete path                  *
//*    and name of the pax file obtained from the FTP location        *
//*    of the product download page.                                  *
//*********************************************************************
//GETPAX   EXEC PGM=FTP,PARM='(EXIT',REGION=0M
//SYSTCPD  DD   DSN=yourTCPIP.PROFILE.dataset,DISP=SHR
//SYSFTPD  DD   DSN=yourFTP.DATA.dataset,DISP=SHR
//SYSPRINT DD   SYSOUT=*
//OUTPUT   DD   SYSOUT=*
//INPUT    DD   *
Host
anonymous YourEmailAddress
lcd yourUSSESDdirectory
binary
get FTP_location
quit
```

Download Files to Mainframe through a PC

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

Follow these steps:

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

   The pax or zip file resides on your PC.

2. Open a Windows command prompt.

   The command prompt appears.

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

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

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

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

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

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

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

   The pax file is transferred to the mainframe.

Example: FTP Commands

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

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

Create a Product Directory from the Pax File

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

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

Follow these steps:

1. Supply a valid JOB statement.
2. Replace *yourUSSESDdirectory* with the name of the USS directory that you use for ESD downloads.

   The job points to your specific directory.
3. Replace *paxfile.pax.Z* with the name of the pax file.

   The job points to your specific pax file.
4. Submit the job.

   The job runs and creates the product directory.

Note: If the PARM= statement exceeds 71 characters, uncomment and use the second form of UNPAXDIR instead. This sample job uses an X in column 72 to continue the PARM= parameters to a second line.

Sample Job to Execute the Pax Command (Unpackage.txt)

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

```
//ESDUNPAX JOB (ACCOUNTNO),'UNPAX ESD PACKAGE ',
// MSGCLASS=X,CLASS=A,NOTIFY=&SYSUID
//*********************************************************************
//* This sample job can be used to invoke the pax command to create   *
//* the product-specific installation directory.                      *
//*                                                                   *
//* This job must be customized as follows:                           *
//* 1. Supply a valid JOB statement.                                  *
//* 2. Replace "yourUSSESDdirectory" with the name of the USS         *
//*    directory used on your system for ESD downloads.               *
//* 3. Replace "paxfile.pax.Z" with the name of the pax file.         *
//* NOTE: If you continue the PARM= statement on a second line, make  *
//*       sure the 'X' continuation character is in column 72.        *
//*********************************************************************
//UNPAXDIR EXEC PGM=BPXBATCH,
// PARM='sh cd /yourUSSESDdirectory/; pax -rvf paxfile.pax.Z'
//*UNPAXDIR EXEC PGM=BPXBATCH,
//* PARM='sh cd /yourUSSESDdirectory/; pax                            X
//*            -rvf paxfile.pax.Z'
//STDOUT DD SYSOUT=*
//STDERR DD SYSOUT=*
```

Copy Installation Files to z/OS Data Sets

Use this procedure to invoke the SMP/E GIMUNZIP utility to create MVS data sets from the files in the product-specific directory.

Follow these steps:

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

   You have identified the product-specific installation details.

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

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

   The job is edited.

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

   Your view is of the product-specific directory.

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

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

      Note: The default Java location is the following:

      `/usr/lpp/java/Java_version`

   b. Perform one of the following steps:

      - Change the SMPCPATH DD PATH to your SMP/E Java application classes directory, typically /usr/lpp/smp/classes/.
      - Change HASH=YES to HASH=NO on the GIMUNZIP parameter.

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

5. Change all occurrences of 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* 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)*.

Receive the SMP/E Package

If you are installing the package into a new SMP/E environment, see the product documentation and the sample jobs included with the product to set up an SMP/E environment before you proceed. The sample jobs can be found in *yourHLQ*.SAMPJCL.

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

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

How to Install Products Using Native SMP/E JCL

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

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

Prepare the SMP/E Environment for Pax Installation

The members that are used in this procedure prepare the data sets, initialize the zones, and create the DDDEFs for CA Hyper-Buf.

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

Follow these steps:

1. Customize the macro GVMSEDIT 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 GVMSEDIT 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* for the unzip to DASD ESD JCL.

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

2. Open the SAMPJCL member GVM1ALL in an edit session and execute the GVMSEDIT macro from the command line.

   GVM1ALL is customized.

3. Submit GVM1ALL.

   This job produces the following results:

   - The target and distribution data sets for CA Hyper-Buf are created.
   - Unique SMPLTS, SMPMTS, SMPSCDS, and SMPSTS data sets for this target zone are created.

4. Open the SAMPJCL member GVM2CSI in an edit session and execute the GVMSEDIT macro from the command line.

   GVM2CSI is customized.

5. Submit GVM2CSI.

   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 *yourhlq*.SAMPJCL members in sequence. Do not proceed with any job until the previous job has completed successfully.

To run the installation jobs

1. Open the SAMPJCL member GVM3RECD in an edit session and execute the GVMSEDIT macro from the command line.

   GVM3RECD is customized.

2. Submit the *yourhlq*.SAMPJCL member GVM3RECD to receive SMP/E base functions.

   CA Hyper-Buf is received and now resides in the global zone.

3. Open the SAMPJCL member GVM4APP in an edit session and execute the GVMSEDIT macro from the command line.

   GVM4APP is customized.

4. Submit the *yourhlq*.SAMPJCL member GVM4APP to apply SMP/E base functions.

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

   Important! The APPLY of CA Hyper-Buf Release 11.5 deletes all previous releases of CA Hyper-Buf.

5. Open the SAMPJCL member GVM5ACC in an edit session and execute the GVMSEDIT macro from the command line.

   GVM5ACC is customized.

6. Submit the *yourhlq*.SAMPJCL member GVM5ACC to accept SMP/E base functions.

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

Clean Up the USS Directory

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

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

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

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

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

Follow these steps:

1. Navigate to your Pax-Enhanced ESD USS directory.

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

   `rm paxfile`

   paxfile

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

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

   `rm -r product-specific_directory`

   product-specific_directory

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

   The product-specific directory is deleted.

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

Apply Maintenance

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

Follow these steps:

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

   The PTFs and HOLDDATA become accessible to the *yourHLQ*.SAMPJCL maintenance members.
3. The GVMSEDIT macro was customized in the installation steps. Verify that you still have the values from the base installation.
4. Open the SAMPJCL member GVM6RECP in an edit session and execute the GVMSEDIT macro from the command line.

   GVM6RECP is customized with your JOB statement, CSI location, and zone names.
5. Customize the GVM6RECP SMPPTFIN and SMPHOLD DD statements to reference the FB 80 data sets for the PTFs and HOLDDATA.
6. Submit GVM6RECP.

   The PTFs and HOLDDATA are received.
7. Open the SAMPJCL member GVM7APYP in an edit session and execute the GVMSEDIT macro from the command line.

   GVM7APYP is customized.
8. Submit GVM7APYP.

   The PTFs are applied.
9. (Optional) Open the SAMPJCL member GVM8ACCP in an edit session and execute the GVMSEDIT macro from the command line.

   GVM8ACCP is customized.
10. (Optional) Submit *yourHLQ*.SAMPJCL member GVM8ACCP.

    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.

SYSMOD

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

Code a bypass operand on your APPLY command to install SYSMODs that have internal holds. Code the bypass 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. The HOLDDATA is commonly used for SYSMODs that have been distributed and later are discovered to cause problems.

Download the external HOLDDATA from CA 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.

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

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

A special HOLDDATA class that is called ERREL exists. We have determined that the problem fixed by the SYSMOD is more important than the one that it causes. We recommend that you apply these SYSMODs.

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.

Chapter 5: Installing Your Product from Tape

This section contains the following topics:

Unload the Sample JCL from Tape

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

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

Follow these steps:

1. Run the following sample JCL:

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

unitname

Specifies the tape unit to mount the tape.

nnnnnnn

Specifies the tape volume serial number.

yourHLQ

Specifies the data set prefix for the installation.

sysda

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

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

2. Continue with one of the following options:

   - If you already have set up the SMP/E environment, go to Run the Installation Jobs for a Tape Installation.
   - If you have *not* set up the SMP/E environment, go to Prepare the SMP/E Environment for Tape Installation.

How to Install Products Using Native SMP/E JCL

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

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

Prepare the SMP/E Environment for Tape Installation

The members that are used in this procedure prepare the data sets, initialize the zones, and create the DDDEFs for CA Hyper-Buf.

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

Follow these steps:

1. Customize the macro GVMSEDIT 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 that you edit an installation member, type GVMSEDIT on the command line, and press Enter to replace the defaults with your specifications.

   The macro is ready to customize your y*ourHLQ*.SAMPJCL members.

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

2. Open the SAMPJCL member GVM1ALL in an edit session and execute the GVMSEDIT macro from the command line.

   GVM1ALL is customized.

3. Submit GVM1ALL.

   This job produces the following results:

   - The target and distribution data sets for CA Hyper-Buf are created.
   - Unique SMPLTS, SMPMTS, SMPSCDS, and SMPSTS data sets for this target zone are created.

4. Open the SAMPJCL member GVM2CSI in an edit session and execute the GVMSEDIT macro from the command line.

   GVM2CSI is customized.

5. Submit GVM2CSI.

   This job produces the following results:

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

Run the Installation Jobs for a Tape Installation

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

To run the installation jobs

1. Open the SAMPJCL member GVM3RECT in an edit session and execute the GVMSEDIT macro from the command line.

   GVM3RECT is customized.

2. Submit the *yourhlq*.SAMPJCL member GVM3RECT to receive SMP/E base functions.

   CA Hyper-Buf is received and now resides in the global zone.

3. Open the SAMPJCL member GVM4APP in an edit session and execute the GVMSEDIT macro from the command line.

   GVM4APP is customized.

4. Submit the *yourhlq*.SAMPJCL member GVM4APP to apply SMP/E base functions.

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

   Important! The APPLY of CA Hyper-Buf Release 11.5 deletes all previous releases of CA Hyper-Buf.

5. Open the SAMPJCL member GVM5ACC in an edit session and execute the GVMSEDIT macro from the command line.

   GVM5ACC is customized.

6. Submit the *yourhlq*.SAMPJCL member GVM5ACC to accept SMP/E base functions.

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

Apply Maintenance

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

Follow these steps:

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

   The PTFs and HOLDDATA become accessible to the *yourHLQ*.SAMPJCL maintenance members.
3. The GVMSEDIT macro was customized in the installation steps. Verify that you still have the values from the base installation.
4. Open the SAMPJCL member GVM6RECP in an edit session and execute the GVMSEDIT macro from the command line.

   GVM6RECP is customized with your JOB statement, CSI location, and zone names.
5. Customize the GVM6RECP SMPPTFIN and SMPHOLD DD statements to reference the FB 80 data sets for the PTFs and HOLDDATA.
6. Submit GVM6RECP.

   The PTFs and HOLDDATA are received.
7. Open the SAMPJCL member GVM7APYP in an edit session and execute the GVMSEDIT macro from the command line.

   GVM7APYP is customized.
8. Submit GVM7APYP.

   The PTFs are applied.
9. (Optional) Open the SAMPJCL member GVM8ACCP in an edit session and execute the GVMSEDIT macro from the command line.

   GVM8ACCP is customized.
10. (Optional) Submit *yourHLQ*.SAMPJCL member GVM8ACCP.

    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.

SYSMOD

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

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.

Code a bypass operand on your APPLY command to install SYSMODs that have internal holds. Code the bypass 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. The HOLDDATA is commonly used for SYSMODs that have been distributed and later are discovered to cause problems.

Download the external HOLDDATA from CA 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.

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

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

A special HOLDDATA class that is called ERREL exists. We have determined that the problem fixed by the SYSMOD is more important than the one that it causes. We recommend that you apply these SYSMODs.

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.

Chapter 6: Starting Your Product

This section describes what you need to do to start CA Hyper-Buf.

This section contains the following topics:

Authorize CA Hyper-Buf

Now that CA Hyper-Buf is installed into the receiving libraries, there are several more steps that must be taken before CA Hyper-Buf is ready for activation. Note that in this section, CBS3LINK can refer to the CBS3LINK library itself or, if you prefer, another library into which you have copied the executable modules found in CBS3LINK.

1. Make the executable library APF authorized.

   The CBS3LINK library that holds the executable modules must be APF authorized before use. The MVS authorization should be made permanent by placing the appropriate statements in the appropriate PROG member of SYS1.PARMLIB prior to the next IPL of the system. Check with your systems programmer or systems administrator to make this permanent change. This can be done temporarily with the following MVS command:

   ```
   SETPROG
   APF,ADD,DSNAME=name.of.dataset,VOL=volume
   ```

   where *name.of.dataset* is the name of your CBS3LINK library and volume is the DASD volume where this library resides.

2. Put the authorized executable library in the linklist.

   The CBS3LINK that you just made authorized must be placed in the linklist. When CA Hyper-Buf is started, certain modules must be loaded from a linklisted data set. This step should be coordinated with the systems programmer or systems administrator. The CBS3LINK data set can be made a permanent linklist data set by placing the appropriate statements in the PROG member of SYS1.PARMLIB prior to the next IPL of the system. You can also add the CBS3LINK to the linklist dynamically. The following commands may be used to do this, but use caution and check with the systems programming personnel before you issue these MVS commands. These are MVS commands that are documented in the IBM MVS System Commands Manual.

   ```
   SETPROG
   LNKLST,DEFINE,NAME=HBUF115,COPYFROM=CURRENT
   ```

   This command defines a new linklist, but is not yet active.

   ```
   SETPROG
   LNKLST,ADD,NAME=HBUF115,DSNAME=cbs3link.dataset,ATTOP
   ```

   Substitute the name of the CBS3LINK data set for *cbs3link.dataset* in the above command. This adds the cbs3link.dataset to the new linklist.

   ```
   SETPROG LNKLST,ACTIVATE,NAME=HBUF115
   ```

   This command activates the new linklist with the CBS3LINK data set.

3. Update the TSO program authorization member.

To activate or deactivate CA Hyper-Buf with the ISPF interface, you must identify two programs to TSO that will run authorized. This is accomplished by updating SYS1.PARMLIB member IKJTSO*xx*, where *xx* is the suffix of the member that is read at IPL. Member GVBTSO00 of the ABS3SAMP data set contains a model of the information you need to add to the SYS1.PARMLIB member. Check with the systems programmer or systems administrator for this update. Once the statements have been added to the appropriate IKJTSO*xx* member, the following TSO command can be issued to activate this updated member:

```
SET  IKJTS0=xx
```

Where *xx* is the suffix of the IKJTSO member you just updated.

Define Security Profiles

To allow the security system to control the administrative functions of CA Hyper-Buf , a resource class of @HBUFADM must be defined to the security system, and all users that are allowed to activate or deactivate CA Hyper-Buf must be given *control* access to this resource. If this step is not done, any TSO user may be able to activate or deactivate CA Hyper-Buf, which is highly inadvisable. The Link Pack Area of z/OS is dynamically updated when CA Hyper-Buf is started. It is possible that your security system has this resource protected against such dynamic updates. Therefore, the modules that are dynamically updated must be identified to the security system. The modules are IFG0192A, IGG0191A, IFG0202L, and IFG0200T. These modules are also dynamically updated when CA Hyper-Buf is stopped. CA Hyper-Buf is designed to make security calls with CA Top Secret, CA ACF2. and RACF. Following are the examples of how to define the CA Hyper-Buf resources to each of these security systems:

- IBM Security Server (RACF) Definitions:

  SAMPLE RACF CLASS DESCRIPTOR ENTRY (CDE) MACRO

```
&HBUFADM ICHERCDE CLASS=@HBUFADM,                          x
                  DFTRETC=8, DEFAULT RETURN CODE           x
                  DFTUACC=READ, DEFAULT UNIVERSAL ACCESS   x
                  ID=148, RECOMMENDED IDJ
                  POSIT=14 FLAGS POSITION
```

  SAMPLE RACF COMMAND TO ACTIVATE THE CLASS DEFINITION

```
SETR CLASSAC (&HBUFADM) GENERIC (@HBUFADM)
```

  SAMPLE RACF COMMAND TO DEFINE THE CONTROL ENTITY

```
RDEF @HBUFADM CONTROL NOTIFY (USERID) OWNER (USERID) IACC (READ)
```

  SAMPLE RACF COMMAND TO GRANT UPDATE ACCESS (SEE NOTE)

```
PE CONTROL ACCESS (UPDATE) CLASS (@HBUFADM) ID(userid)
```

  Note: Specify userids who you want to be able to START, or STOP CA Hyper-Buf as well as REFRESH constraints.

  SAMPLE RACF COMMAND TO REFRESH INSTORAGE PROFILES

```
SETR CLASSACT (@HBUFADM) GENERIC (@HBUFADM) REFRESH

RDEFINE FACILITY CSVDYLPA.ADD.IFG0192A UACC(NONE)
RDEFINE FACILITY CSVDYLPA.ADD.IGG0191A UACC(NONE)

RDEFINE FACILITY CSVDYLPA.ADD.IFG0202L UACC(NONE)
RDEFINE FACILITY CSVDYLPA.ADD.IFG0200T UACC(NONE)

RDEFINE FACILITY CSVDYLPA.DELETE.IFG0192A UACC(NONE)
RDEFINE FACILITY CSVDYLPA.DELETE.IGG0191A UACC(NONE)
RDEFINE FACILITY CSVDYLPA.DELETE.IFG0202L UACC(NONE)
RDEFINE FACILITY CSVDYLPA.DELETE.IFG0200T UACC(NONE)

PERMIT CSVDYLPA.ADD.IFG0192A CLASS(FACILITY) ID(OPER1) ACCESS(UPDATE)
```

```
PERMIT CSVDYLPA.ADD.IGG0191A CLASS(FACILITY) ID(OPER1) ACCESS(UPDATE)
PERMIT CSVDYLPA.ADD.IFG0202L CLASS(FACILITY) ID(OPER1) ACCESS(UPDATE)
PERMIT CSVDYLPA.ADD.IFG0200T CLASS(FACILITY) ID(OPER1) ACCESS(UPDATE)

PERMIT CSVDYLPA.DELETE.IFG0192A CLASS(FACILITY) ID(OPER1) ACCESS(UPDATE)
PERMIT CSVDYLPA.DELETE.IGG0191A CLASS(FACILITY) ID(OPER1) ACCESS(UPDATE)
PERMIT CSVDYLPA.DELETE.IFG0202L CLASS(FACILITY) ID(OPER1) ACCESS(UPDATE)
PERMIT CSVDYLPA.DELETE.IFG0200T CLASS(FACILITY) ID(OPER1) ACCESS(UPDATE)
```

Note: Replace OPER1 with the USERID that is used on the started task or batch job that starts and stops CA Hyper-Buf.

- CA Top Secret Definitions:

```
TSS ADD(MASTER) IBMFAC(CSVDYLPA)
TSS PER(userid) IBMFAC(CSVDYLPA.ADD.IFG0192A) ACCESS(READ)
TSS PER(userid) IBMFAC(CSVDYLPA.ADD.IFG0200T) ACCESS(READ)
TSS PER(userid) IBMFAC(CSVDYLPA.ADD.IFG0202L) ACCESS(READ)
TSS PER(userid) IBMFAC(CSVDYLPA.ADD.IGG0191A) ACCESS(READ)

TSS PER(userid) IBMFAC(CSVDYLPA.DELETE.IFG0192A) ACCESS(READ)
TSS PER(userid) IBMFAC(CSVDYLPA.DELETE.IFG0200T) ACCESS(READ)
TSS PER(userid) IBMFAC(CSVDYLPA.DELETE.IFG0202L) ACCESS(READ)
TSS PER(userid) IBMFAC(CSVDYLPA.DELETE.IGG0191A) ACCESS(READ)

TSS ADD(RDT) RESCLASS(@HBUFADM) RESCODE(3F) ATTR(DEFPROT)
ACLST(READ UPDATE CONTROL) DEFACC(READ)

TSS ADD(userid) @HBUFADM(CONTROL)
```

Note: Where *userid* is the CA Top Secret ACID that is used when activating or or deactivating CA Hyper-Buf.

- CA ACF2 Rules:

```
SET C(GSO) SYSID(xxxxxxxx)      where xxxxxxxx is the current system sysid
INSERT CLASMAP.ADM RESOURCE(@HBUFADM) RSRCTYPE(ADM) ENTITYLN(8)
F ACF2,REFRESH(CLASMAP)
SET R(ADM)
COMPILE
$KEY(CONTROL) TYPE (ADM)
  UID(userid) SERVICE(UPDATE) ALLOW
  UID(*) SERVICE(READ) ALLOW

STORE
SET R(FAC)
COMPILE
$KEY(CSVDYLPA) TYPE(FAC)
 ADD.IFG1092A UID(userid) SERVICE(UPDATE) ALLOW
 ADD.IFG0200T UID(userid) SERVICE(UPDATE) ALLOW
 ADD.IFG0202L UID(userid) SERVICE(UPDATE) ALLOW
 ADD.IGG0191A UID(userid) SERVICE(UPDATE) ALLOW
 DELETE.IFG0192A UID(userid) SERVICE(UPDATE) ALLOW
 DELETE.IFG0200T UID(userid) SERVICE(UPDATE) ALLOW
 DELETE.IFG0202L UID(userid) SERVICE(UPDATE) ALLOW
```

```
DELETE.IGG0191A UID(userid) SERVICE(UPDATE) ALLOW
```

Note: Where *userid* is the CA Top Secret ACID that will be activating and deactivating CA Hyper-Buf.

Establish Initial Constraints

To use as a started task procedure to start and stop CA Hyper-Buf, use PROCCOPY in the ABS3SAMP library to copy the two procedures, GVBDBFON and GVBDBOFF, to a suitable procedure library. Also, copy the default CONSTRAINT members, GVBSTART and GVBADVAN to a suitable non-SMP/E controlled library, where they can be changed as needed. The GVBDBFON procedure reads the GVBSTART member by default, but will need to be modified to point to the correct library.

Chapter 7: Post Installation

This section contains the following topics:

The ISPF Interface

To access the CA Hyper-Buf ISPF dialog, allocate the following data sets to the TSO user dynamically, or in the TSO LOGON proc.

DDNAME	DSNAME SUFFIX	TYPE
SYSPROC	CBS3CLS0	CLIST
ISPMLIB	CBS3MENU	MESSAGES
ISPPLIB	CBS3PENU	PANELS

These files are SMP/E controlled. To modify the panels, either use USERMOD or copy the desired files to the appropriate libraries and edit the files there. Also verify that the programs in the CBS3LINK data set are available from the LINKLIST or from a STEPLIB in the TSO LOGON proc.

To add an option to an existing ISPF menu

1. Add a line for CA Hyper-Buf in the)BODY section. For example:

   ```
   % H +CA-HYPER-BUF - Dynamic Buffering %
   ```

2. Add a corresponding line in the)PROC section.

   ```
   H,'CMD(%GVBPRIM  NEWAPPL(HBUF) NOCHECK'
   ```

Note: While using a REXX EXEC or CLIST to invoke CA Hyper-Buf, the data sets must be allocated using the LIBDEF command. The call to CA Hyper-Buf is:

```
"SELECT CMD(%GVBPRIM) NEWAPPL(HBUF) PASSLIB"
```

Index