# Hardware Interface Service

## Component Guide

### Version 1.0

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

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

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

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

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

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

The manufacturer of this Documentation is CA.

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

Copyright © 2011 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

# CA Technologies Product References

This document references the following CA Technologies products:

- CA ACF2™ for z/OS
- CA Auditor for z/OS (CA Auditor)
- CA Mainframe Software Manager™ (CA MSM)
- CA OPS/MVS® Event Management and Automation (CA OPS/MVS)
- CA SOLVE:Operations® Automation
- CA Top Secret® for z/OS

# Contact CA Technologies

**Contact CA Support**

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

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

**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.

If you would like 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

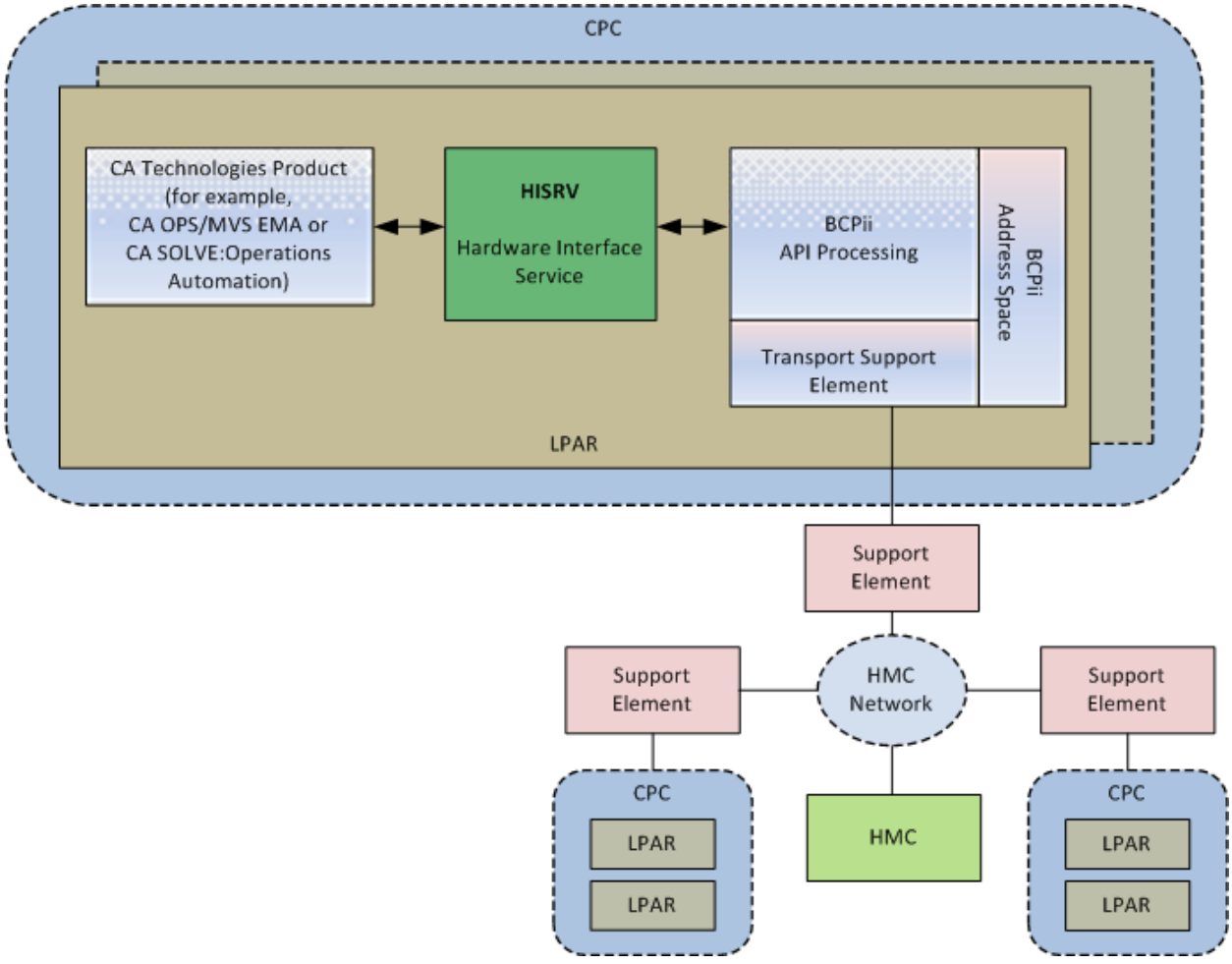
This guide describes how to install and implement Hardware Interface Service.

This section contains the following topics:



## How the Service Works

Hardware Interface Service enables a product to retrieve information from the Hardware Management Console (HMC). A product can send a query to the service, which in turn interrogates the HMC through the Base Control Program internal interface (BCPii).



# 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:



## Software Requirements

Your system must have a currently supported version of z/OS with BCPii.

## CA Common Services Requirements

The CA Common Services load library must be accessible to the Hardware Interface Service address space through the JCL STEPLIB or system LNKLST.

## Storage Requirements

Hardware Interface Service has the following 3390 DASD space requirements:

- If you are using CA MSM or ESD, the following z/OS UNIX file system space is required for the downloaded and unpacked files: 16 MB.
- For installation and setup, the following spaces are required:
  - Installation = 110 cylinders
  - IBM System Modification Program Extended (SMP/E) libraries = 40 cylinders
  - Setup = 2 cylinders
  - Setup temporary work area = 25 cylinders

# 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.

**Note:** The information in this section applies to the latest version of CA MSM. If you are using an earlier version, see the appropriate bookshelf on the CA Mainframe Software Manager product page.

## How to Use CA MSM: Scenarios

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

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

### How to Acquire a Product

The *Product Acquisition Service (PAS)* facilitates the acquisition of mainframe products and the service for those products, such as program temporary fixes (PTFs). The PAS retrieves information about the products to which your site is entitled and records these entitlements in a software inventory 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 15), 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, including browsing downloaded software packages, managing SMP/E consolidated software inventories (CSIs) 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. Do *one* of the following to select a CSI:
   - Create a new CSI:
     a. Set up the global zone.
     b. Create a target zone.
     c. Create a distribution zone.
   - Use an existing CSI from your working set:
     a. Update the global zone.
     b. Set up the target zone: either create a new target zone or use an existing target zone.
     c. Set up the distribution zone: either create a new 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 the 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 release, if necessary.
5. Review the installation summary and start the installation.

After the installation 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 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 deployment of mainframe products from the software inventory of the driving system to the target system, including 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.

**Important!** During deployment, include the following data set as a custom data set: *dsnpref*.HI10.*hisrv_name*.PARMLIB. The data set is created when you set up the service (see page 49).

# 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 the information provided, and click the link to confirm it.

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

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

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

3. Click New.

   You are prompted for the 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:



**Note:** When you have completed the procedures in this section, go to Configuring Your Product (see page 49).

## How to Install a Product Using Pax-Enhanced ESD

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

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

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

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

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

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

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

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

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

   `pax -rvf pax-filename`

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

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

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

**More Information:**

USS Environment Setup (see page 22)
Allocate and Mount a File System (see page 23)
Copy the Product Pax Files into Your USS Directory (see page 26)
Create a Product Directory from the Pax File (see page 31)
Copy Installation Files to z/OS Data Sets (see page 32)

## 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 19) topic explains how the download interface works.

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

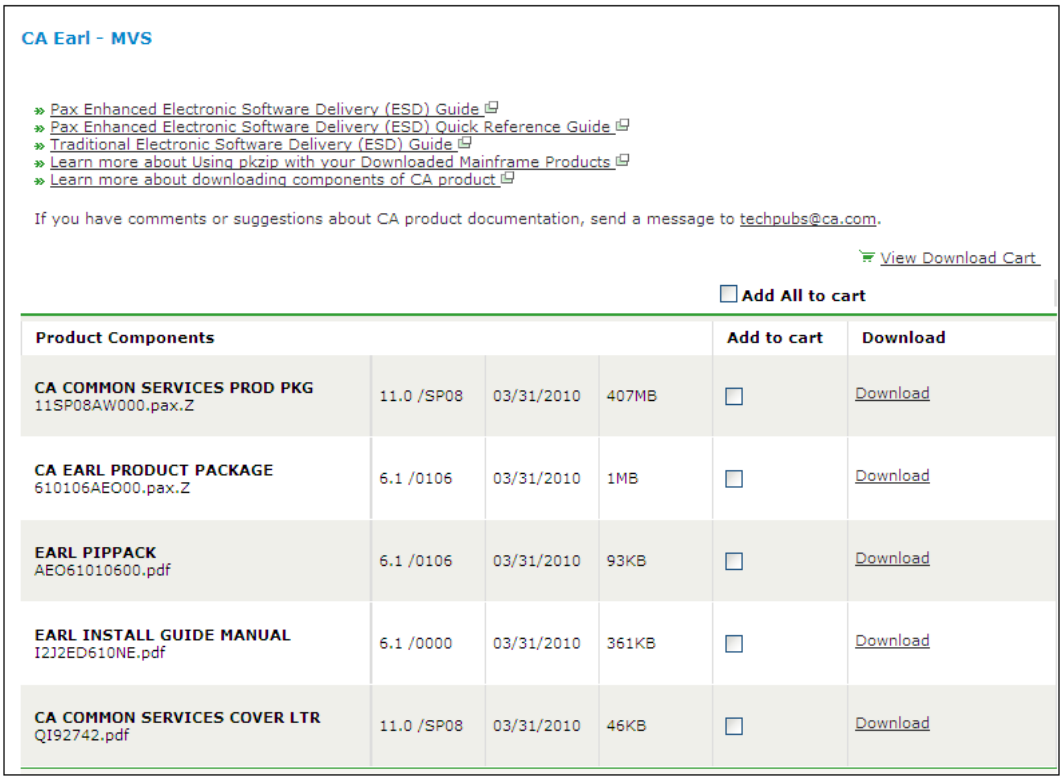
4. Perform the steps to install the product based on the product-specific steps.

   The product is installed on the mainframe.

## ESD Product Download Window

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

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



**CA Earl - MVS**

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

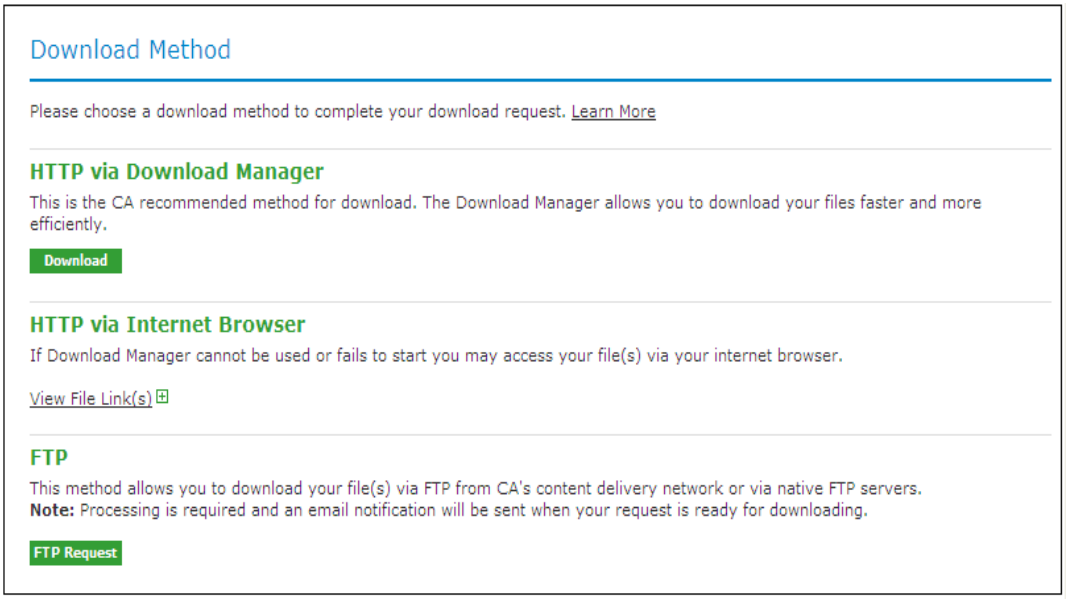
If you have comments or suggestions about CA product documentation, send a message to techpubs@ca.com.

View Download Cart

☐ Add All to cart

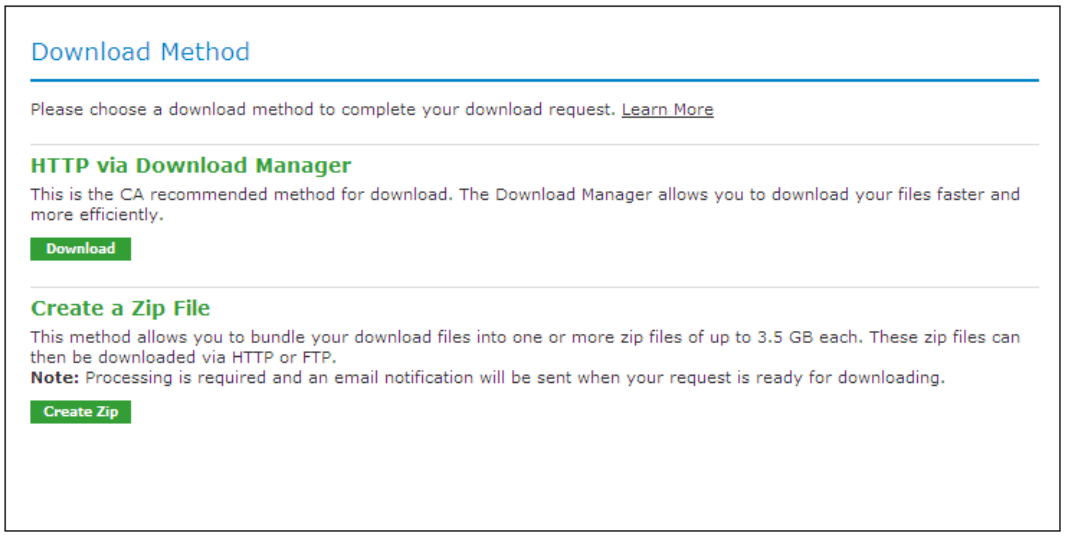
| Product Components | | | | Add to cart | Download |
|---|---|---|---|---|---|
| **CA COMMON SERVICES PROD PKG**<br>11SP08AW000.pax.Z | 11.0 /SP08 | 03/31/2010 | 407MB | ☐ | Download |
| **CA EARL PRODUCT PACKAGE**<br>610106AEO00.pax.Z | 6.1 /0106 | 03/31/2010 | 1MB | ☐ | Download |
| **EARL PIPPACK**<br>AEO61010600.pdf | 6.1 /0106 | 03/31/2010 | 93KB | ☐ | Download |
| **EARL INSTALL GUIDE MANUAL**<br>I2J2ED610NE.pdf | 6.1 /0000 | 03/31/2010 | 361KB | ☐ | Download |
| **CA COMMON SERVICES COVER LTR**<br>QI92742.pdf | 11.0 /SP08 | 03/31/2010 | 46KB | ☐ | Download |

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




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

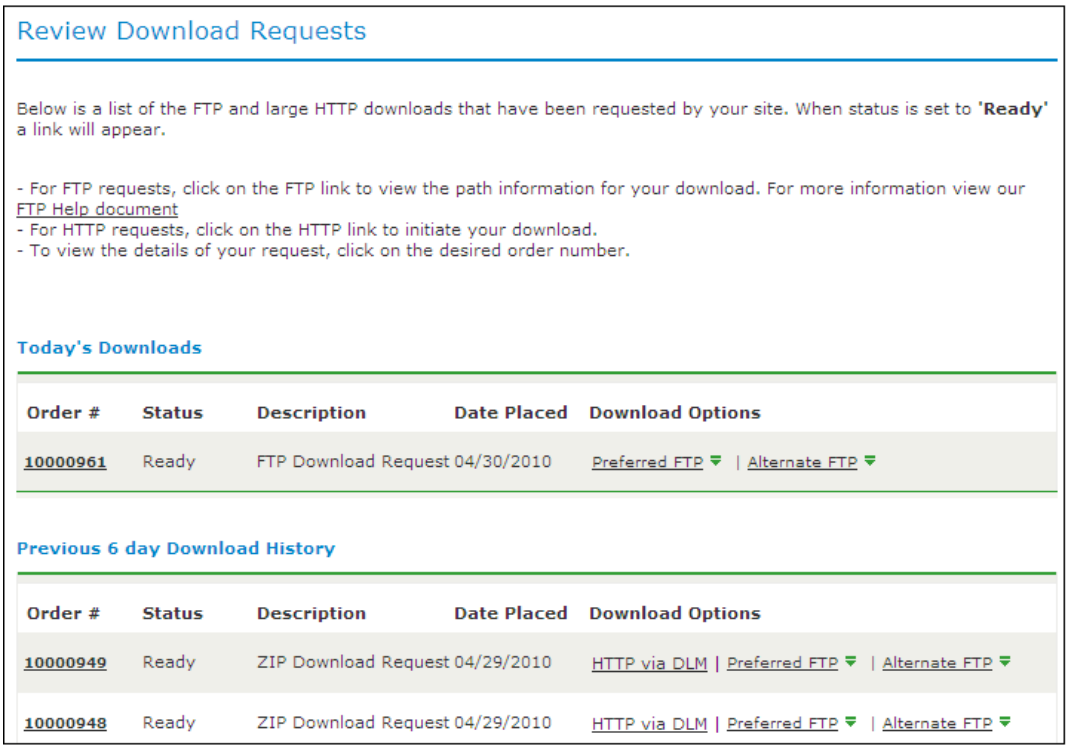
**Note:** For mainframe downloads using this HTTP method, click the Learn More link.



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

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

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



Review Download Requests

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

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

**Today's Downloads**

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

**Previous 6 day Download History**

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

## USS Environment Setup

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

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

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

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

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

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

# Allocate and Mount a File System

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

This procedure describes how to perform the following tasks:

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

  **Note:** You must have SUPERUSER authority to do this.
- Optionally, permit write access to anyone in the same group as the person who created the directory.

  **Important!** USS commands are case-sensitive.

**Follow these steps:**

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

   - On a zFS, use the following sample:

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

   - On an HFS, use the following sample:

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

   The file system is allocated.

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

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

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

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

   The mount point is created.

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

   - On a zFS, use the following sample:

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

   - On an HFS, use the following sample:

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

   The file system is mounted.

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

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

   Write access is granted.

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

# Copy the Product Pax Files into Your USS Directory

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

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

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

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

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

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

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

**More Information:**

How the Pax-Enhanced ESD Download Works (see page 19)
ESD Product Download Window (see page 19)

## Download Using Batch JCL

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

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

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

**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 are not able to download using the Preferred FTP method, check the security restrictions for all servers that company employees can download from that are outside of 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:** For details regarding FTP, see the FTP Help document link in the Review Download Requests window and the Learn More link available in the Download Methods window.

9. Submit the job.

   **Important!** If your FTP commands are incorrect, 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 running the JCL, the pax file resides in the mainframe USS directory that you supplied.

## Example: CAtoMainframe.txt, JCL

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

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

## Download Files to Mainframe through a PC

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

**Follow these steps:**

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

   The pax or zip file resides on your PC.

2. Open a Windows command prompt.

   The command prompt appears.

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

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

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

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

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

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

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

   The pax file is transferred to the mainframe.

### Example: FTP Commands

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

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

# Create a Product Directory from the Pax File

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

**Important!** To simplify the Pax-Enhanced ESD process, the PDF version of this guide includes a sample JCL job that you can copy directly to the mainframe. To access this job, click the paper clip icon in the lower left corner of the PDF reader. This opens a window displaying attachments. 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:** After making the changes noted in the job, if the PARM= statement exceeds 71 characters, uncomment and use the second form of UNPAXDIR instead. This sample job uses an X in column 72 to continue the PARM= parameters to a second line.

## 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 product-specific details you need to complete the installation procedure.

   You have identified product-specific installation details.

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

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

   The job is edited.

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

   Your view is of the product-specific directory.

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

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

   b. Perform one of the following steps:

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

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

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

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

6. Submit the UNZIPJCL job.

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

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

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

# Set Up Installation Data Set

The installation JCL members are in the *dsnpref*.CAI.HI10.CC2DJCL data set; *dsnpref* is a prefix you specify for your product data sets.

After you unzip the data sets, do *one* of the following:

- Rename *dsnpref*.CAI.HI10.CC2DJCL to *dsnpref*.HI10.INSTALL.JCL
- Copy the members in *dsnpref*.CAI.HI10.CC2DJCL into *dsnpref*.HI10.INSTALL.JCL

# 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.

The *dsnpref*.HI10.INSTALL.JCL data set contains the following sample jobs that help you install, configure, and maintain the service:

**HIS#INS**

Installs the software. The job performs Step 1 through Step 5 of the process.

**HIS#RALC**

Allocates a PARMLIB data set for the service. Step 6 of the process uses this job.

**HIS#XSMP**

Receives and applies maintenance.

# Install the Software

During the installation process, you provide the site-specific installation information that you previously collected. This information is used to customize the installation JCL jobs.

**Follow these steps:**

1. Open the HIS#INS member in an edit session, review the comments, and customize the member.
2. Submit the member to install the base functions.

   The software is applied and accepted, and now resides in the target and distribution libraries.

# Clean Up the USS Directory

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

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

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

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

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

**Follow these steps:**

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

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

   `rm paxfile`

   ***paxfile***

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

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

   `rm -r product-specific-directory`

   ***product-specific-directory***

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

   The product-specific directory is deleted.

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

# Maintenance

Maintenance includes program temporary fixes (PTFs) that supersede all authorized program analysis reports (APARs) that were created up to that time. Details of the superseded APARs are available as comments within the PTFs.

**Important!** If you installed the product using CA MSM, use CA MSM to apply maintenance.

Product maintenance is provided as system modification program (SMP) fixes. The fixes consist of PTFs applied using the IBM System Modification Program Extended (SMP/E) tool.

## Apply Maintenance

CA Support Online provides maintenance and HOLDDATA that have been published since the installation data was created. When the maintenance process is complete, the software is ready to deploy.

**Follow these steps:**

1. Check CA Support Online, and download any PTFs and HOLDDATA published since this release was created.
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 INSTALL.JCL maintenance member.
3. Customize the INSTALL.JCL member HIS#XSMP in an edit session:
   - Your JOB statement, CSI location, and zone names
   - SMPPTFIN and SMPHOLD DD statements to reference the FB 80 data sets for the PTFs and HOLDDATA
4. Submit HIS#XSMP.

   The PTFs and HOLDDATA are received and applied.

### 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 Hardware Interface Service:

**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.

**SYSMOD**

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

**DYNACT**

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

**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.

**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.

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. It resides in a separate file. It is commonly used for SYSMODs that have been distributed and later are discovered to cause problems.

Download the external HOLDDATA from CA Support 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 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 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:



**Note:** When you have completed the procedures in this section, go to Configuring Your Product (see page 49).

## Unload the Installation Software

The installation software helps you install Hardware Interface Service. The installation utility software is delivered on tape.

The installation software unloads into the *dsnpref*.HI10.INSTALL.JCL data set; *dsnpref* is a prefix you specify for your product data sets.

To unload the software, do *one* of the following:

- If *dsnpref*.HI10.INSTALL.JCL does not exist, unload into a new data set from tape (see page 41).
- If *dsnpref*.HI10.INSTALL.JCL exists from a previous installation and you are installing at the current release level, unload into an existing data set from tape (see page 43).

### Unload the Installation Software into a New Data Set from Tape

If *dsnpref*.HI10.INSTALL.JCL does not exist, unload the installation software from the tape on to your DASD and into a new data set.

**Follow these steps:**

1. Create an unload job by copying the following JCL:

```
//jobname  JOB  ..............
//STEP1    EXEC PGM=IEBCOPY
//SYSPRINT DD   SYSOUT=*
//SYSUT1   DD   DSN=CAI.SAMPJCL,
//              DISP=OLD,UNIT=?device_in,VOL=SER=?tapeser,
//              LABEL=(1,SL,EXPDT=98000)
//SYSUT2   DD   DSN=?dsnpref.HI10.INSTALL.JCL,
//              DISP=(NEW,CATLG,DELETE),
//              UNIT=?device_out,VOL=SER=?volser,
//              SPACE=(TRK,(20,1,10)),
//              DCB=(RECFM=FB,LRECL=80,BLKSIZE=0)
//SYSIN    DD   DUMMY
```

2. Replace the variables prefixed with a question mark (?) with your own values as follows:

   ***?device-in***

   Specifies the tape drive unit to mount the tape.

   ***?tapeser***

   Specifies the tape volume serial number in the form C2D73*x*. The value for this release is C2D730.

   ***?dsnpref***

   Specifies the data set prefix to use for the installation and maintenance data sets. Do not include the name of your planned product region in the prefix. If the data set high-level qualifiers you are using do not exist, define an alias entry in the master catalog.

   **Limits:** 29 characters

   ***?device_out***

   Specifies the type of the DASD device where you want to place the installation software.

   ***?volser***

   Specifies the volume serial number of the DASD.

   If SMS controls SYSUT2 allocation, replace UNIT= and VOL=SER= with STORCLAS=*?storclass*.

3. Submit and run the job.
4. Check that the job successfully completed.

## Unload the Installation Software into an Existing Data Set from Tape

If *dsnpref*.HI10.INSTALL.JCL exists from a previous installation at the current release level, unload the installation software from tape into the existing data set.

**Follow these steps:**

1. Create an unload job by copying the following JCL:

```
//jobname  JOB .............
//STEP1   EXEC PGM=IEBCOPY
//SYSPRINT DD  SYSOUT=*
//SYSUT1   DD  DSN=CAI.SAMPJCL,
//             DISP=OLD,UNIT=?device-in,VOL=SER=?tapeser,
//             LABEL=(1,SL,EXPDT=98000)
//SYSUT2   DD  DSN=?dsnpref.HI10.INSTALL.JCL,
//             DISP=OLD
//SYSIN    DD  *
  COPY I=((SYSUT1,R)),O=SYSUT2
  COPY I=((SYSUT2,R)),O=SYSUT2
/*
```

2. Replace the statements prefixed with a question mark (?) with your own values as follows:

   ***?device-in***

   Specifies the tape drive unit to mount the tape.

   ***?tapeser***

   Specifies the tape volume serial number in the form C2D73*x*. The value for this release is C2D730.

   ***?dsnpref***

   Specifies the data set prefix in the previous installation.

3. Submit and run the job.
4. Verify that the job successfully completed.

# 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.

The *dsnpref*.HI10.INSTALL.JCL data set contains the following sample jobs that help you install, configure, and maintain the service:

**HIS#INS**

Installs the software. The job performs Step 1 through Step 5 of the process.

**HIS#RALC**

Allocates a PARMLIB data set for the service. Step 6 of the process uses this job.

**HIS#XSMP**

Receives and applies maintenance.

# Install the Software

During the installation process, you provide the site-specific installation information that you previously collected. This information is used to customize the installation JCL jobs.

**Follow these steps:**

1. Open the HIS#INS member in an edit session, review the comments, and customize the member.
2. Submit the member to install the base functions.

   The software is applied and accepted, and now resides in the target and distribution libraries.

# Maintenance

Maintenance includes program temporary fixes (PTFs) that supersede all authorized program analysis reports (APARs) that were created up to that time. Details of the superseded APARs are available as comments within the PTFs.

**Important!** If you installed the product using CA MSM, use CA MSM to apply maintenance.

Product maintenance is provided as system modification program (SMP) fixes. The fixes consist of PTFs applied using the IBM System Modification Program Extended (SMP/E) tool.

## Apply Maintenance

CA Support Online provides maintenance and HOLDDATA that have been published since the installation data was created. When the maintenance process is complete, the software is ready to deploy.

**Follow these steps:**

1. Check CA Support Online, and download any PTFs and HOLDDATA published since this release was created.
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 INSTALL.JCL maintenance member.
3. Customize the INSTALL.JCL member HIS#XSMP in an edit session:
   - Your JOB statement, CSI location, and zone names
   - SMPPTFIN and SMPHOLD DD statements to reference the FB 80 data sets for the PTFs and HOLDDATA
4. Submit HIS#XSMP.

   The PTFs and HOLDDATA are received and applied.

### 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 Hardware Interface Service:

**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.

**SYSMOD**

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

**DYNACT**

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

**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.

**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.

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. It resides in a separate file. It is commonly used for SYSMODs that have been distributed and later are discovered to cause problems.

Download the external HOLDDATA from CA Support 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 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 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: Configuring Your Product

This section describes the minimum configuration tasks needed before Hardware Interface Service can be started, customized, and used in your environment.

This section contains the following topics:

Set Up the Service (see page 49)

## Set Up the Service

The HISPARMS member helps you set up the Hardware Interface Service.

**Follow these steps:**

1. Open the HIS#RALC member in an edit session, review the comments, and customize the member.

   **Note:** If you acquire the product using CA MSM, the HIS#RALC member is in the *dsnpref*.HI10.CC2DJCL data set. If you acquire the product using ESD or from tape, the HIS#RALC member is in the *dsnpref*.HI10.INSTALL.JCL data set.

2. Submit the member.

   The *dsnpref*.HI10.*hisrv_name*.PARMLIB data set is allocated.

3. Open the *dsnpref*.HI10.*hisrv_name*.PARMLIB(HISPARMS) member in an edit session, review the comments, and customize the copy.

   The parameters for the service are set up.

**More Information:**

Initialization Parameters (see page 57)

# Chapter 7: Preparing for Startup

This section describes what you need to do to start Hardware Interface Service.

This section contains the following topics:



## Prepare the Service Started Task

The *dsnpref*.HI10.INSTALL.JCL data set contains a template, HISRV, for the service started task. You customize a copy of the member for each service you want to set up. Review the copy to verify that it meets your site-specific requirements. You can then copy it to a procedure library with the required authority.

**Note:** To assist you with future deployment, you can update the started task member to use z/OS static system symbols.

**Follow these steps:**

1. Review and update the DD statements in the service started task member:

   **HISIN**

   Specifies the parameters data set.

   **HISLOG**

   Specifies the log data set. The data set has a variable blocked (VBA) record format (RECFM=U) and a record length of 137 (LRECL=137).

2. Copy the reviewed member to SYS*x*.PROCLIB.
3. Grant the user ID associated with the service UPDATE authority on the run-time data sets created by the installation and setup processes.
4. Authorize the user ID of the service for the BCPii application program interface (API) and resources (see page 52).

## Load Libraries

Most products have their own load library but also require the load libraries of supporting services. The following load libraries must be APF-authorized:

- CC2DLOAD

## Authorization of the Load Libraries

To APF-authorize your load libraries, add the run-time load libraries to the SYS1.PARMLIB(IEAAPF*xx*) APF list.

To dynamically APF-authorize the load libraries, issue the following z/OS command:

```
SETPROG APF,ADD,DSNAME=?loadlib,VOLUME=?volser
```

**?*loadlib***

Specifies the name of the load library.

**?*volser***

Specifies its volume serial number.

To dynamically APF-authorize load libraries controlled by SMS, issue the following z/OS command:

```
SETPROG APF,ADD,DSNAME=?loadlib,SMS
```

# Configure Service User ID Security

Hardware Interface Service requires BCPii authority to retrieve information from the HMC.

**Note:** In the following examples, *community_name* must be in uppercase (for example, BCPII) and *cpc_name* must be a full SNA network name of the Central Processor Complex (CPC) (for example, IBM390PS.MF01).

### Example: CA ACF2 for z/OS

To define the security resources and grant the service access to BCPii, issue CA ACF2 for z/OS commands in TSO, for example:

```
$KEY(HWI) TYPE(FAC)
$USERDATA('community_name')
APPLNAME.HWISERV UID(hisrv_user_id) SERVICE(READ) ALLOW
CAPREC.- UID(hisrv_user_id) SERVICE(READ) ALLOW
CAPREC.cpc_name UID(*************STCSYS) SERVICE(READ) ALLOW
CAPREC.cpc_name.- UID(*************STCSYS) SERVICE(UPDATE) ALLOW
UID(*) SERVICE(READ) ALLOW
TARGET.- UID(hisrv_user_id) SERVICE(READ) ALLOW
TARGET.cpc_name UID(*************STCSYS) SERVICE(READ) ALLOW
TARGET.cpc_name.- UID(*************STCSYS) SERVICE(UPDATE) ALLOW
UID(*) SERVICE(READ) ALLOW
```

### Example: CA Top Secret for z/OS

To define the security resources and grant the service access to BCPii, issue CA Top Secret for z/OS commands in TSO, for example:

```
TSS ADDTO(tssdept) IBMFAC(HWI)
TSS PER(hisrv_user_id) IBMFAC(HWI.APPLNAME.HWISERV) ACCESS(READ)
TSS PER(hisrv_user_id) IBMFAC(HWI.TARGET.cpc_name) ACCESS(READ)
APPLDATA('community_name')
TSS PER(hisrv_user_id) IBMFAC(HWI.TARGET.cpc_name.*) ACCESS(READ)
TSS PER(hisrv_user_id) IBMFAC(HWI.CAPREC.cpc_name) ACCESS(READ)
TSS PER(hisrv_user_id) IBMFAC(HWI.CAPREC.cpc_name.*) ACCESS(READ)
```

### Example: RACF

To define the security resources and grant the service access to BCPii, issue RACF commands in TSO, for example:

```
RDEFINE FACILITY HWI.TARGET.cpc_name UACC(NONE) APPLDATA('community_name')
RDEFINE FACILITY HWI.CAPREC.cpc_name UACC(NONE) APPLDATA('community_name')
RDEFINE FACILITY HWI.APPLNAME.HWISERV UACC(NONE)
PERMIT HWI.APPLNAME.HWISERV CLASS(FACILITY) ID(hisrv_user_id) ACCESS(READ)
PERMIT HWI.TARGET.cpc_name CLASS(FACILITY) ID(hisrv_user_id) ACCESS(READ)
PERMIT HWI.TARGET.cpc_name.* CLASS(FACILITY) ID(hisrv_user_id) ACCESS(READ)
PERMIT HWI.CAPREC.cpc_name CLASS(FACILITY) ID(hisrv_user_id) ACCESS(READ)
PERMIT HWI.CAPREC.cpc_name.* CLASS(FACILITY) ID(hisrv_user_id) ACCESS(READ)
```

## Security Validation Messages

To validate that you have configured security correctly, review the service HISLOG after the service has started.

If security configuration is correct, HISLOG has the following messages:

```
NK8030 HIS INITIAL TOPOLOGY COLLECTION STARTING. H/W INTERFACE: BCPII
NKAA20 10 - COLLECTING INFORMATION ABOUT THIS SYSTEM
NS1001 HISRV SUBSYSTEM INITIALIZATION COMPLETE. SSID: HIS
NKAA20 20 - RETRIEVING ALL CPC NAMES
NKAA20 30 - BUILDING TOPOLOGY UNDER CPCS
…
NK8031 HIS INITIAL TOPOLOGY COLLECTION FINISHED. H/W INTERFACE: BCPII ENTITIES: nn
```

If security configuration is incorrect, HISLOG has the following messages:

```
NK8030 HIS INITIAL TOPOLOGY COLLECTION STARTING. H/W INTERFACE: BCPII
NKAA20 10 - COLLECTING INFORMATION ABOUT THIS SYSTEM
NS1001 HISRV SUBSYSTEM INITIALIZATION COMPLETE. SSID: HIS
NKAA73 BCPII A/S IS NOT ACTIVE. DETECTION CODE: 1 (BCPII RC D/X: 3842 00000F02)
NK8032 HIS INITIAL TOPOLOGY COLLECTION ERROR. H/W INTERFACE: BCPII
```

# Enable Auditing by CA Auditor

If your auditors require CA Auditor or CA Common Inventory Service to know of this product running on your system, put a load module in your system LNKLST.

To define the load module to the system LNKLST, include the library *dsnpref*.HI10.CC2DLINK in the system LNKLST SYS1.PARMLIB(PROG*xx*), for example:

```
LNKLST ADD NAME(LNKLST00) DSNAME(dsnpref.HI10.CC2DLINK)
```

# Chapter 8: Starting Up

This section contains the following topics:



## Start the Service

To start the service, issue the following command from the MVS console:

```
S service_name,REUSASID=YES
```

*service_name* is the name of the service started task or job.

**Note:** To stop the service, issue the following command from the MVS console:
P *service_name.*

# Appendix A: Initialization Parameters

This section contains the following topics:



## Overview

The service has various initialization parameters. These parameters control important execution options and facilities.

The initialization parameters are specified in the PARMLIB(HISPARMS) member. To review the initialization parameters and to add further initialization parameters, open this member.

**Note:** If you specify a parameter more than once, the last specification is used.

# Parameter Descriptions

**HWICONAME=*company_name***

Specifies the name of the company. Products using the service can use this value. The value can be in mixed case. If the value contains blank, lowercase, or special characters, specify the value within quotes.

**Limits:** 32 characters maximum

**HWIDCNAME=*data_center_name***

Specifies the name of the data center. Products using the service can use this value. The value can be in mixed case. If the value contains blank, lowercase, or special characters, specify the value within quotes.

**Limits:** 32 characters maximum

**SSID={ HIS | *name* }**

Specifies the subsystem ID (SSID) that this invocation of the SSI is to use.

**Note:** You do not need to define the SSID explicitly. The SSID can be defined automatically.

**Default:** HIS

**Limits:** A valid one- to four-character name, with the first character alphabetic or national, and the remainder alphanumeric or national

**SSM={ NO | YES }**

Specifies whether to enable support for CA OPS/MVS System State Manager (SSM).

**Default:** NO

**SSMAPPL=*application_name***

Specifies the application name registered with CA OPS/MVS for this product or component.

**Limits:** Eight characters

**Important!** Each product or component registers a specific application name with CA OPS/MVS. *Do not change this name.*

The application name registered for Hardware Interface Service is HISRV.

**SSMHBI=*heartbeat_interval***

For SSM=YES, specifies how often to send heartbeats to CA OPS/MVS SSM. The heartbeat interval is in minutes. A value of zero indicates no heartbeat.

**Initial value:** 5

**Limits**: 0 through 60

# Appendix B: Commands

This section contains the following topics:



## Overview

The service provides several commands that can be used for control and to display statistics. You can use the MODIFY system command to issue these commands.

## Command Descriptions

**FSTOP**

Stops the service.

**Note:** The STOP system command is treated as the FSTOP command.

**SHOW HWIUSERS**

Lists the users of the service.

**STATUS**

Displays the status of the service.

# Appendix C: Messages

## Message Descriptions

### NKAA20

***text***

**Reason:**

*text* indicates a processing phase of the Hardware Interface Service BCPii interface.

The message is written to HISLOG.

**System Action:**

None.

**User Action:**

None.

### NKAA70

**BCPII ERROR. INFORMATION: *iii* - BCPII INFO FOLLOWS...**

**Reason:**

An error is returned by BCPii.

The message is written to HISLOG. An NKAA71 message follows with more information.

**System Action:**

None.

**User Action:**

For assistance, contact CA Support.

## NKAA71

**BCPII REQUEST INFO. REQ: *aa* RC (D,X): *bb cc* DIAG: *dd***

**Reason:**

A BCPii error is detected.

*aa* identifies the request (call) name.

*bb* is the return code (decimal).

*cc* is the return code (hexadecimal).

*dd* displays the diagnostic information.

The message is written to HISLOG.

**System Action:**

None.

**User Action:**

For assistance, contact CA Support.

## NKAA72

**ERROR. INFORMATION: *iii***

**Reason:**

A BCPii error is detected.

*iii* indicates the problem.

The message is written to HISLOG.

**System Action:**

None.

**User Action:**

For assistance, contact CA Support.

## NKAA73

**BCPII A/S IS NOT ACTIVE. DETECTION CODE: *aa* (BCPII RC D/X: *bb cc*)**

**Reason:**

Hardware Interface Service determines that the BCPii address space is not active or a serious problem with BCPii is found.

*aa* identifies the operation that was being performed when the error occurred.

*bb* is the BCPii return code (decimal).

*cc* is the BCPii return code (hexadecimal).

The message is written to HISLOG.

**System Action:**

None.

**User Action:**

For assistance, contact CA Support.

## NKAA74

**BCPII INTERFACE ERROR. REQUEST: *aa* RC: *bb***

**Reason:**

An error occurs in the BCPii interface.

*aa* identifies the request name.

*bb* is a reason code.

The message is written to HISLOG.

**System Action:**

None.

**User Action:**

For assistance, contact CA Support.

## NKAA85

**CALL TO BCPII FAILED. PROCESSING: *aa* TYPE: *bb*. INFORMATION FOLLOWS...**

**Reason:**

An error occurs while calling BCPii.

*aa* identifies the hardware entity name.

*bb* identifies the entity type.

The message is written to HISLOG. An NKAA71 message follows showing the specific BCPii request and return information.

**System Action:**

None.

**User Action:**

For assistance, contact CA Support.

## NKAA90

**ATTR: *aa* BCPII CODE (D): *bb* HWI CODE (D): *cc***

**Reason:**

Debugging options are in effect to log attribute value retrieval from BCPii.

*aa* identifies the attribute name.

*bb* is the BCPii attribute code.

*cc* is the Hardware Interface Service attribute code.

The message is written to HISLOG.

**System Action:**

None.

**User Action:**

None.

## NKAG80

**BCPII EVENT RECEIVED. $HWBE FOLLOWS...**

**Reason:**

An event from BCPii is received, and errors have been detected.

The message is written to HISLOG. A dump of the $HWBE control block follows.

**System Action:**

The $HWBE control block is logged (in character and hexadecimal) after this message.

**User Action:**

None.

## NKAG81

**(*xxx* $HWBE) UNREC BCPII EVENT CODE/SUBCODE. VALUES: *a b***

**Reason:**

An event from BCPii is received. The event has an invalid event code and subcode.

*a* is the event code (in decimal).

*b* is the subcode (in decimal).

The message is written to HISLOG. The message indicates whether the dumped $HWBE control block that it refers to precedes or follows it in the log.

**System Action:**

The event is ignored.

**User Action:**

None.

## NKAG82

**(*xxx* $HWBE) ERROR: *aaa***

**Reason:**

An event from BCPii is received, and an error was detected.

*aaa* describes the error.

The message is written to HISLOG. The message indicates whether the dumped $HWBE control block that it refers to precedes or follows it in the log.

**System Action:**

The event is ignored.

**User Action:**

For assistance, contact CA Support.

## NKA001

**BCPII HARDWARE INTERFACE INITIALIZATION COMPLETE.**

**Reason:**

The Hardware Interface Service BCPii interface has completed initialization.

This message is written to HISLOG.

**System Action:**

None.

**User Action:**

None.

## NKA080

**BCPII H/W I/F INITIALIZATION FAILED - *reason***

**Reason:**

The Hardware Interface Service BCPii interface has not initialized.

*reason* displays the reason of the failure.

The message is written to HISLOG.

**System Action:**

Hardware Interface Service fails to initialize.

**User Action:**

For assistance, contact CA Support.

## NKA401

**'BCPII' HARDWARE INTERFACE ACTIVE**

**Reason:**

The Hardware Interface Service is using the BCPii interface. This message is part of the response to the STATUS command.

**System Action:**

None.

**User Action:**

None.

## NK0001

**HIS FACILITY BASIC INITIALIZATION COMPLETE. VERSION: *vvv***

**Reason:**

Basic initialization of Hardware Interface Service is complete.

*vvv* identifies the version.

The message is written to HISLOG.

**System Action:**

None.

**User Action:**

None.

## NK0080

**HIS FACILITY INITIALIZATION FAILED - *reason***

**Reason:**

Basic initialization of Hardware Interface Service failed.

*reason* displays the reason for the failure:

**UNSUPPORTED OPERATING SYSTEM/VERSION: *name version***

Indicates that the service is not supported on this operating system or this version of the operating system.

**ONLY 1 H/W SERVER CAN BE EXECUTING**

Indicates that only one instance of the service can be active at a time.

**HARDWARE INTERFACE INIT FAILED. I/F: *aaa* RC: *bbb***

Indicates that the chosen hardware interface (such as BCPii) facility could not be initialized.

**SYSPLEX FACILITY INIT FAILED. RC: *aaa***

Indicates that the Sysplex topology facility failed to initialize.

**Note:** For other reasons, contact CA Support.

The message is written to HISLOG.

**System Action:**

The service terminates.

**User Action:**

For assistance, contact CA Support.

## NK0301

**HARDWARE INTERFACE SERVICE ACTIVE. VERSION: *vvv***

**Reason:**

Hardware Interface Service is active. This message is part of the response to the STATUS command.

*vvv* identifies the version.

**System Action:**

None.

**User Action:**

None.

## NK0380

**HIS SETUP ERROR: *reason***

**Reason:**

An error occurs during the initialization of Hardware Interface Service.

*reason* displays the reason for the error.

The message is written to HISLOG.

**System Action:**

The service terminates.

**User Action:**

For assistance, contact CA Support.

## NK0610

**APITOKEN JOBNAME ASID-TCB@ USERID**

**Reason:**

This message is issued in response to a SHOW HWIUSERS command and provides headings for the following information:

**APITOKEN**

Is the heading for the API token (connection token) assigned to the Hardware Interface Service user.

**JOBNAME**

Is the heading for the job name associated with the user.

**ASID-TCB@**

Is the heading for the ASID and TCB address of the user.

**USERID**

Is the heading for the user ID.

**System Action:**

None.

**User Action:**

None.

## NK0611

**EVEXIT-@ EVCORR1 EVCORR2**

**Reason:**

This message is issued in response to a SHOW HWIUSERS command and provides headings for the following information:

**EVEXI-@**

Is the heading for the address (in the user address space) of the event exit.

**EVCORR1**

Is the heading for the value of the first event correlator.

**EVCORR2**

Is the heading for the value of the second event correlator.

**System Action:**

None.

**User Action:**

None.

## NK0612

**EVSTATUS TOT#-EVT QUE#-EVT #-ABENDS**

**Reason:**

This message is issued in response to a SHOW HWIUSERS command and provides headings for the following information:

**EVSTASTUS**

Is the heading for the status of event delivery for the user.

**TOT#-EVT**

Is the heading for the total number of events delivered to the user.

**QUE#-EVT**

Is the heading for the current number of events queued to the user.

**#-ABENDS**

Is the heading for the number of ABENDs detected in the event exit for the user.

**System Action:**

None.

**User Action:**

None.

## NK0613

**CONN-DATA**

**Reason:**

This message is issued in response to a SHOW HWIUSERS command and provides a heading for the following information:

**CONN-DATA**

Is the heading for the connection data supplied by the user.

**System Action:**

None.

**User Action:**

None.

## NK0615

***apitoken jobname asid-tcb@ userid***

**Reason:**

This message is issued in response to a SHOW HWIUSERS command and provides information about a user.

For heading information, see message NK0610.

**System Action:**

None.

**User Action:**

None.

## NK0616

***evexit-@ evcorr1 evcorr2***

**Reason:**

This message is issued in response to a SHOW HWIUSERS command and provides information about a user.

For heading information, see message NK0611.

**System Action:**

None.

**User Action:**

None.

## NK0617

***evstatus tot#-evt que#-evt #-abends***

**Reason:**

This message is issued in response to a SHOW HWIUSERS command and provides information about a user.

For heading information, see message NK0612.

**System Action:**

None.

**User Action:**

None.

## NK0618

***conn-data***

**Reason:**

This message is issued in response to a SHOW HWIUSERS command and provides information about a user.

For heading information, see message NK0613.

**System Action:**

None.

**User Action:**

None.

## NK5110

**HIS API CONN (*a*) T: *b* A-T: *c* J: *d* U: *e* I: *f***

**Reason:**

An API user connects.

***a***

Identifies the connection type:

- I indicates an implicit connection.
- X indicates an explicit connection.

***b***

Is the APITOKEN value for the user.

**c**

Is the ASID and TCB for the user.

***d***

Is the job name for the user.

**e**

Is the user ID for the user.

***f***

Contains five characters that provide the following information:

- Character 1 indicates whether the user is in cross-memory mode (X) or not (H).
- Character 2 indicates whether the user is authorized (A) or not (U).
- Character 3 indicates whether server security has been requested (S) or not (N).
- Character 4 indicates whether tracing has been requested (Y) or not (T).
- Character 5 is the TCB association:
  - X indicates a cross-memory user.
  - T indicates the connecting TCB.
  - J indicates JSTCB.

The message is written to HISLOG.

**System Action:**

None.

**User Action:**

None.

## NK5111

**... CONN DATA: *d***

**Reason:**

An API user connects.

*d* displays any supplied connection data.

The message is written to HISLOG.

**System Action:**

None.

**User Action:**

None.

## NK5115

**HIS API DISC (*a*) T: *b* A-T: *c* J: *d* U: *e***

**Reason:**

An API user disconnects.

***a***

Identifies the connection type:

- I indicates an implicit connection.
- X indicates an explicit connection.

***b***

Is the APITOKEN value for the user.

**c**

Is the ASID and TCB for the user.

***d***

Is the job name for the user.

**e**

Is the user ID for the user.

The message is written to HISLOG.

**System Action:**

None.

**User Action:**

None.

## NK5116

**... CONN DATA: *d***

**Reason:**

An API user disconnects.

*d* displays any supplied connection data.

The message is written to HISLOG.

**System Action:**

None.

**User Action:**

None.

## NK6180

**API EVENT EXIT ABENDED... JOBNAME: *a* ASID-TCB: *b*-*c* EXIT@: *d* (DISABLED)**

**Reason:**

An API event exit abends.

Information about the exit is displayed.

The message is written to HISLOG.

**System Action:**

The event exit is disabled. The exit is not called again.

**User Action:**

Correct the event exit.

## NK8030

**HIS INITIAL TOPOLOGY COLLECTION STARTING. H/W INTERFACE: *name***

**Reason:**

The initial topology collection is starting.

*name* identifies the hardware interface name.

The message is written to HISLOG.

**System Action:**

Topology collection starts.

**User Action:**

None.

## NK8031

**HIS INITIAL TOPOLOGY COLLECTION FINISHED. H/W INTERFACE: *name* ENTITIES: *count***

**Reason:**

The initial topology collection has finished.

*name* identifies the hardware interface name.

*count* is the number of entities found.

The message is written to HISLOG.

**System Action:**

None.

**User Action:**

None.

## NK8032

**HIS INITIAL TOPOLOGY COLLECTION ERROR. H/W INTERFACE: *name***

**Reason:**

The initial topology collection had an error.

*name* identifies the hardware interface name.

The message is written to HISLOG. Other messages in HISLOG indicate the specific problem.

**System Action:**

Hardware Interface Service continues to run.

**User Action:**

None.

# Index

## R



## S



## T



## U