CA Tape Encryption

Installation Guide

Release 14.5.00

Second Edition

CA Technologies Product References

This document references the following CA Technologies products:

- CA 1® Tape Management (CA 1)
- CA ACF2™ for z/OS (CA ACF2)
- CA Auditor for z/OS (CA Auditor)
- CA Disk™ Backup and Restore (CA Disk)
- CA Earl™ (CA Earl)
- CA Tape Encryption
- CA TLMS® Tape Management (CA TLMS)
- CA Top Secret® for z/OS (CA Top Secret)
- CA View® Output Archival and Viewing (CA View)
- CA Vtape™ Virtual Tape System (CA Vtape)

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

Provide Feedback

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 CA Tape Encryption.

This section contains the following topics:

Audience

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

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

You may need to work with the following personnel:

- Systems programmer, for z/OS and VTAM definitions
- Security administrator, for library and started task access authority
- SMS or storage administrator, for DASD allocations

How to Activate CA Encryption Key Manager

CA Encryption Key Manager and CA Tape Encryption are delivered in the same SMP/E FMID. The LMP keys shipped with your order determine the functions available. If you already have CA Encryption Key Manager installed, you can bypass these installation procedures and activate CA Tape Encryption and the options you are licensed for.

To activate CA Tape Encryption

1. Upgrade to Release 14.5.00.
2. Update your LMP keys.
3. Obtain the BES procedure distributed in Release 14.5.00 CTAPPROC data set and customize it for your installation. This procedure has the requirements for TCP/IP communication. You must run the most current version of the BES procedure to enable NKM.
4. Perform the configuration steps outlined in either the *Option for Networked Key Management User Guide,* the *Option for IBM User Guide* or the *Option for Application Management User Guide..*

Note: If you plan to implement the Option for Networked Key Management, any systems sharing a BES database that is not at the Release 14.5.00 level, requires a compatibility PTF. For more information, see the cover letter.

How the Installation Process Works

The following steps describe the installation process:

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

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

5. Apply maintenance, if applicable.
6. Configure each component that has configuration parameters.

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

The hardware requirements for CA Tape Encryption are:

- Any hardware that supports z/OS 1.6 and above, and the IBM z/Architecture™ (ARCHLVL=2).
- The following processors are supported:
  - IBM z800
  - IBM z900
  - IBM z890
  - IBM z990
  - IBM z9
  - IBM z10
  - IBM z11
- The Cryptographic Coprocessor Facility (CCF) is not required for IBM z800 or z900 processors, however for optimal system performance CA recommends that you have one installed.
- You are not required to activate the CP Assist for Cryptographic Functions (CPACF) feature for IBM z890, z990, z9, or z10 processors; however for optimal system performance CA recommends that you activate it. (In most cases, CPACF is shipped in the enabled state on IBM z9 and z10 processors.)

  Note: The z9 Business Class (BC) and z9 Enterprise Class (EC) systems are supported, and are referred to in the documentation as z9. z9 zIIP specialty processors are optional but strongly recommended to improve performance and minimize central processors overhead.

You can use the Integrated Cryptographic Service Facility (ICSF) Cryptographic Key Data Set (CKDS) instead of the BES database to store your symmetric encryption keys if a cryptographic coprocessor is present.

Cryptographic Hardware Supported

For optimal performance, install or enable CCF or CPACF. On systems where CCF is installed ICSF is also required. Review the ICSF install requirements for your system and the ICSF options you intend to implement.

Two cryptographic hardware options are available for use on various systems:

Cryptographic Coprocessor Facility (CCF)

A standard component on z900 and a no-cost option for z800. On z800 and z900 systems, ICSF requires CCF.

CP Assist for Cryptographic Functions (CPACF)

A standard component on z9, z10, and z11 and a no-cost option for z890 and z990.

Other available cryptographic hardware components do not necessarily improve encryption performance, as described in the following list:

- Peripheral Component Interconnect (PCI)-based coprocessors (PCICC, PCIXCC, and Crypto Express2), which provide secure key storage, hardware hashing, and SSL support.
- PCI-based accelerators (PCICA, Crypto Express2 configured in accelerator mode), which provide high performance SSL assistance.

Support for the IBM TS1120 and TS1130 encryption capable drives is also provided when the [assign the value for TEKM in your book] is licensed.

Cryptographic Algorithms Supported

CA Tape Encryption provides software implementations of the AES128, AES192, and AES256 algorithms. These algorithms are provided to insure that you can encrypt and decrypt tape files at a disaster recovery site where crypto-processors may not be available. The performance of these software-based algorithms is slower than the same algorithms implemented in hardware (CPACF) or in the IBM ICSF software implementations. For this reason, CA recommends selecting an algorithm supported by your cryptographic hardware. This gives you significant performance improvement.

CA Tape Encryption provides software implementations of the MD5, SHA-1, and SHA-256 hashing algorithms. These algorithms are provided so that you can run CA Tape Encryption at recovery sites where a hardware implementation of the algorithm may not be available.

The DES64, 3DES128, and 3DES192 algorithms are available in hardware on all systems with a CCF or CPACF processor installed. CA Tape Encryption does not have a software implementation of the DES64, 3DES128, and 3DES192 algorithms. Ensure that the algorithm is provided by CCF, CPACF, or ICSF at your disaster recovery site.

Note: Software versions of the AES and hashing algorithms are available on all systems.

The following list identifies when a hardware implementation of an algorithm is available:

IBM z800 or z900 with CCF

The algorithms supported in hardware are the:

- DES64, 3DES128, and 3DES192 symmetric algorithms.
- SHA-1 hashing algorithm.
- RSA asymmetric encryption algorithm.

IBM z800 or z900 without CCF

There are no algorithms supported in hardware.

IBM z890 or z990 with CPACF

The algorithms supported in hardware are the:

- DES64, 3DES128, and 3DES192 symmetric algorithms.
- SHA-1 hashing algorithm.
- RSA asymmetric encryption algorithm. Hardware support is provided by a PCI-based coprocessor. If the hardware is not present, the encryption is performed by software with low CP overhead.

IBM z890 or z990 without CPACF

There are no algorithms supported in hardware.

IBM z9 with CPACF

The algorithms supported in hardware are the:

- DES64, 3DES128, 3DES192, and AES128 symmetric algorithms.
- SHA-1 and SHA-256 hashing algorithms.
- RSA asymmetric encryption algorithm. Hardware support is provided by a PCI-based coprocessor. If the hardware is not present, the encryption is performed by software with low CP overhead.

IBM z10 or z11 with CPACF

The algorithms supported in hardware are the:

- DES64, 3DES128, 3DES192, AES128, AES192 and AES256 symmetric algorithms.
- SHA-1 and SHA-256 hashing algorithms.
- RSA asymmetric encryption algorithm. Hardware support is provided by a PCI-based coprocessor. If the hardware is not present, the encryption is performed by software with low CP overhead.

Note: The RSA encryption algorithm is employed only when encrypting symmetric keys for B2B tapes.

Software Requirements

The software requirements for CA Tape Encryption are:

- IBM supported releases of z/OS 1.6 and above, running in 31-bit or 64-bit mode.

  Note: You need z/OS 1.6 to perform encryption using any AES algorithm.

- IBM's Integrated Cryptographic Service Facility (ICSF). ICSF is a software element of z/OS that works with hardware cryptographic features and the security system (CA ACF2, CA Top Secret, or IBM Security Server RACF) to provide secure, high-speed cryptographic services in the z/OS environment. ICSF is only required for systems without CPACF, Secure Keys or for software algorithms not supported by CPACF.

  ICSF libraries must be available during the installation of CA Tape Encryption. (The CA Tape Encryption SMP/E process must have access to the CSF.SCSFMOD0 ICSF DLIB dataset.) However, ICSF does not need to be active while CA Tape Encryption is running.

- CA Tape Encryption supports the following versions of ICSF (identified by FMID):

  - HCR770B
  - HCR7720
  - HCR7730
  - HCR7731
  - HCR7740
  - HCR7750

  You may need to contact IBM to obtain a current version of ICSF. CA Tape Encryption does not support HCR770A on z800 and z900 platforms. (HCR770A might be packaged with z/OS 1.7 and earlier versions of z/OS.) On z890, z990, and z9 platforms, HCR770A may be used to satisfy the SMP/E install requirements of CA Tape Encryption only, but this ICSF version should not be running in your systems.

- SMP/E must have access to the following IBM libraries:

  - CSF.SCSFMOD0 as DDDEF SCSFMOD0
  - CEE.SCEELIB as DDDEF SCEELIB
  - CBC.SCLBSID as DDDEF SCLBSID
  - SYS1.SIEASID as DDDEF SIEASID
  - CEE.SCEEBND2 as DDDEF SCEEBND2

- Any of these storage management systems:
  - CA 1
  - CA TLMS
  - CA Disk
  - CA Vtape

  Customers running non-CA tape management systems are also supported through the CA Tape Encryption Third Party Option.
- The CA Tape Encryption SAF Interface supports the following security systems:
  - CA ACF2
  - CA Top Secret
  - IBM Security Server RACF
- The IBM TS1120 Encryption Key Manager (EKM) application, running under z/OS UNIX System Services and Java, is required to perform device-based encryption on an encryption-enabled TS1120 using the [assign the value for TEKM in your book] to manage the TS1120 keys. The IBM EKM application is also required to support the IBM TS1130 encrypting drive.

Maintenance for CA Products

Additional maintenance is required for CA ACF2, CA Top Secret, CA 1, CA TLMS, CA Disk, and CA Vtape to enable the interfaces between these products and CA Tape Encryption. The exact PTFs required to enable this interface for each product are documented in the cover letter shipped with the product. Integration with IBM DFSMSrmm is also provided and requires additional maintenance from IBM. For integration with non-CA storage products, check with the vendor to determine support requirements.

Multisystem Requirements

The CA Tape Encryption primary database and mirror database must be on shared DASD to allow these files to be read and written by all subsystems configured to be part of the same CA Tape Encryption complex.

CA Tape Encryption uses a hardware RESERVE to protect the BES database. The QNAME used with the RESERVE is “BESX”, the RNAME is the name of the BES primary data set, and the UCB address used is the UCB address of the volume containing the BES primary data set. The BES primary and mirror data sets should not be placed on volumes containing system catalogs, JES spool data sets or any other high activity data sets. If you have a DASD resource serialization manager such as CA Multi-Image Manager (MIM) or IBM Global Resource Serialization (GRS) you may want to convert the QNAME=BESX hardware reserves to SCOPE=SYSTEMS enqueues.

Note: A reserve is not issued for the BES mirror data set. CA Tape Encryption relies on the reserve of the primary data set to provide the necessary serialization for both the primary and the mirror data sets.

CA Tape Encryption uses ENQ with SCOPE=SYSTEM and QNAME=BES*n* (where *n* is a value from 1 to 8) for various other purposes. These enqueues should not be changed by your DASD resource serialization manager since they are intended to serialize within a single system.

Considerations for ExHPDM Users

CA Tape Encryption provides support for the Extended High-Performance Data Mover (ExHPDM) product from Sun Microsystems / Storage Tek. ExHPDM users are cautioned that ExHPDM run times may be elongated when encrypting data with CA Tape Encryption. Run-time elongation may be more significant when the Integrated Compression feature of CA Tape Encryption is also selected for the encrypted volumes. CA recommends that ExHPDM users should evaluate if data compression is needed for the ExHPDM encrypted volumes and in that case, to test production-like workloads to verify if the required resources will be available in the production environment.

For information on enabling compression in ExHPDM environments where FDR and DFDSS are used, see the *Administration Guide*.

CA Common Services Requirements

The CA Common Services used with CA Tape Encryption include:

- CAIRIM
- EARL Service
- CA Health Checker Common Service
- CA LMP

If there are other CA products used at your site, some of these services may already be installed.

In general, CA Tape Encryption requires CA Common Services for z/OS r11 or higher. The CA Health Checker common service requires CA Integration Platform Services installed at r11 SP8 plus any additional maintenance listed at http://ca.com/support.

Maintenance is also required for the CA Earl service. Refer to the cover letter for details on the required maintenance.

Note: For information on CA Common Services, see the *Administration Guide.*

Storage Requirements

Ensure that you have the following storage available:

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

Integration with IBM DFSMSrmm

IBM's tape management product DFSMSrmm interfaces with CA Tape Encryption to provide lifecycle management for tapes encrypted using symmetric key processing. If CA Encryption Key Manager Option for IBM is also licensed, certificates associated with IBM TS1120 or TS1130 tapes may also be tracked in DFSMSrmm.

For information about the PTFs required to enable this interface, contact IBM.

Processing Restrictions

The following restrictions apply to CA Tape Encryption processing:

- CA Tape Encryption only supports Standard Label (SL) tapes. Encryption or decryption capabilities are not provided for non-SL tapes.
- Applications using the z/OS Checkpoint Restart facility are not supported.
- CA Tape Encryption dynamically converts SL tape volumes to SUL volumes.
- The Multiplatform Decryption Utility (MDU), which your non-z/OS business partners use to decrypt data encrypted by CA Tape Encryption, only supports the decryption of standard fixed or fixed-blocked datasets.
- CA Tape Encryption updates the HDR1 record and inserts User Header Labels and User Trailer Labels with encryption processing information. Header and trailer labels are installed through a DCB exit (DCBX) that is dynamically added by CA Tape Encryption.

  Important! Any programs or utilities that dynamically modify the DCB exit list must be tested with CA Tape Encryption to ensure that there are no incompatibilities.

  Do not encrypt sort work (SORTWKnn) files. The advanced data management techniques used by various sort programs can interfere with the DCB exit processing used by CA Tape Encryption.
- Data blocks smaller than 16 bytes are not supported by CA Tape Encryption.
- The CA View Output Archival and Viewing utility SARTCP modifies the HDR1 after tape open processing by rewinding the tape and rewriting the HDR1 , resulting in the loss of data saved in the HDR1 by CA Tape Encryption. To support encryption of any output tapes that are created by the SARTCP utility, you must obtain maintenance to SARTCP. Without this maintenance, CA Tape Encryption will exclude SARTCP tapes from encryption processing.
- IBM Tivoli Storage Manager for z/OS and Compuware File-AID are not supported. These products either do not support User Labels or use BlockID positioning that makes them incompatible with CA Tape Encryption.
- CA Tape Encryption allows you to select the data sets you want to encrypt. For many mainframe applications, tape is the primary medium. A tape data set may be the first and only copy of your business critical data, as opposed to a backup of such data. If you plan to encrypt a primary data set when it is being written to tape, you should thoroughly test your application's encryption and decryption processing to ensure that there are no possible incompatibilities with CA Tape Encryption.
- DISP=OLD / DISP=SHR Restrictions. When DISP=OLD or DISP=SHR processing is used, CA Tape Encryption prevents a job from rewriting a data set in unencrypted mode. CA Tape Encryption abends a job performing RECREATE processing to prevent a previously encrypted data set from being rewritten in unencrypted format.

Note: In tape management systems this is referred to as RECREATE processing. RECREATE processing is the attempt to rewrite the same data set to the same tape volume serial number and file sequence number.

Physical tapes created by CA Vtape (Backstore and Recycle volumes) can be encrypted by CA Tape Encryption because they conform to the requirements listed in this section. They are z/OS SL tapes and they do not use User Header Labels. However, physical container volumes created by IBM and StorageTek virtual tape systems cannot be encrypted because they do not conform to these requirements.

The CA Tape Encryption SAF Interface uses published CA ACF2 and CA Top Secret APIs together with standard RACROUTE macro calls in determining resource authorization protection and data set selection. Therefore, if your environment has special security-related system exits or implements external security manager processing parameters that override or modify SAF router calls and return codes, the SAF Interface cannot be used.

Chapter 3: Installing Your Product Using CA MSM

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

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

When you have completed the procedures in this section, go to Configuring Your Product (see page 73).

This section contains the following topics:

CA MSM Documentation

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

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

How to Install a Product Using CA MSM

Use the following process to install a product using CA MSM. 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, create one through the CA Support web site. In addition, contact your system administrator to obtain the CA MSM URL.

1. Access CA MSM. Log in to CA MSM, and select the Software Catalog tab to display the products to which your organization is entitled. If you cannot find the product you want to acquire, update the catalog. CA MSM refreshes the catalog through CA Support Online using the site IDs associated with your CA Support Online credentials.
2. Download the product installation packages. CA MSM downloads (acquires) the packages (including any maintenance packages) from the CA FTP site.
3. Determine the applicable gen level. Identify the packages at the product gen level that you need.
4. Install your product. A wizard guides you through the installation process. A CSI is created for the installed product as part of the installation process.

   After you complete the installation dialog, your product libraries are created, and you are ready for deployment and customization.
5. Deploy and configure you product.

Access CA MSM Using the Web-Based Interface

You access CA MSM using the web-based interface. You must have at least *one* of the following web browsers: Microsoft Internet Explorer 6.0 or 7.0, or Mozilla Firefox 2.0 or 3.0.

You need the URL of CA MSM from the CA MSM administrator.

To access CA MSM using the web-based interface

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

   The login page appears.

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 CA Support Online account.

   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.

Acquiring Products

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

Update Software Catalog

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

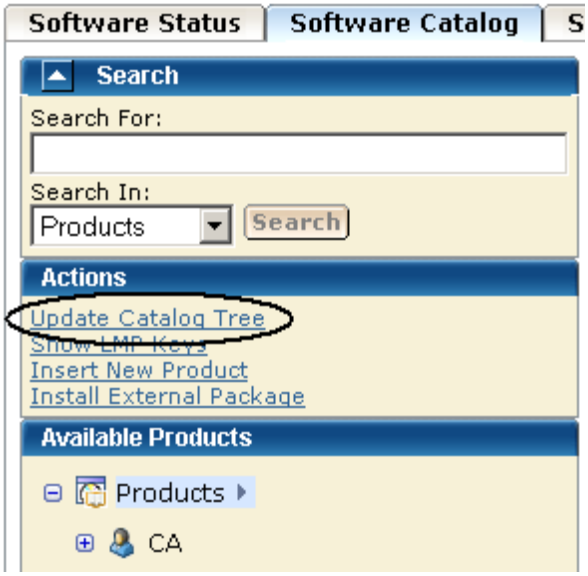
If you update the catalog tree and some changes are missing, check your user settings on the CA Support Online website.

To update your software catalog

1. Click the Software Catalog tab.

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

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



   You are prompted to confirm the update.

3. Click OK.

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

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

Download Product Installation Package

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

To download a product installation package

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

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

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

   The product releases are listed.

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

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

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

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

   The product packages are downloaded.

Migrate Installation Packages Downloaded External to CA MSM

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

Migrating these packages to CA MSM provides a complete view of all your product releases. After a package is migrated, you can use CA MSM to install the product (see page 33).

To migrate information about a product installation package downloaded by other means

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

   Note: A product not acquired from the CA Support Online website does not appear in Software Catalog until you perform this step.

   An entry is added for the product.

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

   The packages for the gen level are listed.

3. Click the Add External Package button.

   You are prompted to enter a path for the package.

4. Specify the USS path to the package you want to migrate, and click OK.

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

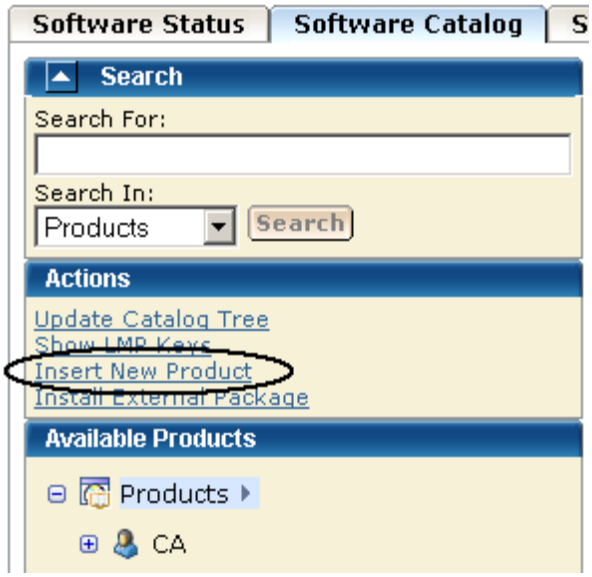
   Note: To see the added package, refresh the page.

Add a Product

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

To add a product package to CA MSM

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



   You are prompted to supply information about the product.

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

   The product is added to the software catalog.

3. Click the gen level of the product you want to install on the product tree at the left.

   The Base Install Packages section appears at the right.

4. Click the Add External Package button.

   You are prompted to identify the package.

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

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

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

Installing Products

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

Install a Product

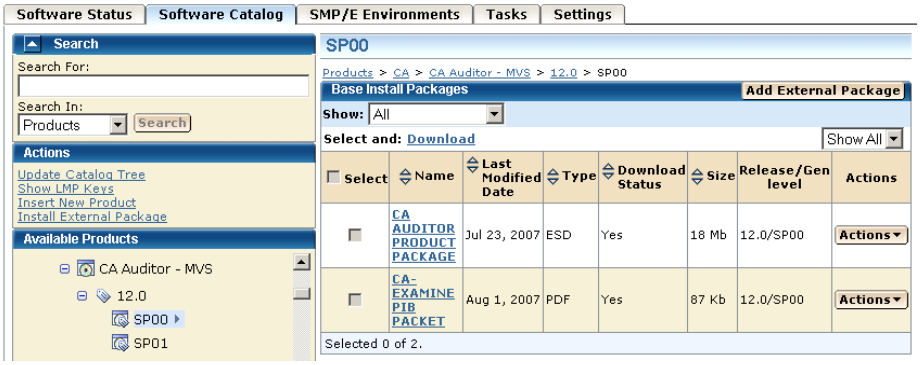
You can install a downloaded product through the Software Catalog, Base Install Packages section. The process starts a wizard that guides you through the installation. At the end of the wizard, a task dynamically invokes the SMP/E and other utilities required to install the product.

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

To install a product

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

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



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

2. Do one of the following:

   - If the package was acquired using CA MSM, locate the product package that you want to install, click the Actions drop-down to the right of the package, and select Install.

     or

   - If the package was acquired external to CA MSM, click the Install External Packages link under the Actions section in the left pane, enter the location of the package, and click OK.

   The Introduction tab of the wizard appears.

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

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

   You are prompted to select the type of installation.

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

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

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

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

   - If no prerequisites exist, click Next.

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

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

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

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

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

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

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

   If you select Create a New SMP/E CSI, you are prompted to specify the CSI parameters (see page 35).

   Note: Only CSIs for the SMP/E environments in your working set are listed. (You can configure your working set from the SMP/E Environments tab.) If you select a CSI about which CA MSM has incomplete information, the wizard prompts you with extra parameters.

   After a CSI is selected or a new CSI is specified, you are prompted for the target zone to use.

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

   Note: If you select Create a New SMP/E Target Zone, you perform additional steps similar to the steps for the Create a New SMP/E CSI option.

   After a target zone is selected or specified, you are prompted for the distribution zone to use.

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

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

9. Review the summary, and click Install.

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

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

Important! After you install the product, you still need to implement and deploy the product.

Create a CSI

You can create a CSI while you are installing a product (see page 33). During the process, you are asked to specify data set allocation parameters, which you can then customize for each data set.

To create a CSI

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

   You are prompted to define a CSI.

2. Specify a name for the environment represented by the CSI, and the following VSAM and data set allocation parameters. You can leave the other parameters at their defaults.

   - Specify the prefix for the name of the CSI VSAM data set.
   - Specify the prefix for the names of the SMP/E data sets.
   - Select whether to use SMS, and complete the appropriate fields.

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

3. Click Next.

   A list of the data sets to be created for the CSI appears.

4. Review the data set names. Click the Override Globals link to change allocation parameters, and then click Next.

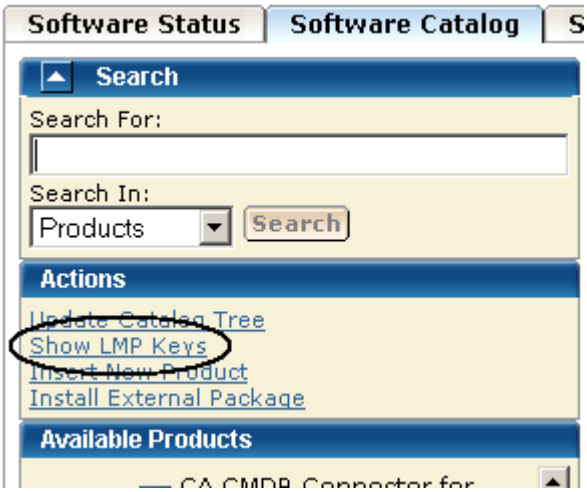
   You are prompted to specify any additional parameters. A new CSI is specified.

Download LMP Keys

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

To retrieve and list the LMP keys for your products

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



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

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

   The list is refreshed for the selected site ID.

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

3. Click Update Keys.

   You are prompted to confirm the update.

4. Click OK.

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

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

Maintaining Products

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

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

How to Apply Maintenance Packages

Use this process to download and apply product maintenance packages.

1. Identify your download method. This section details the steps to use the following download methods:

   - Download Product Maintenance Packages (see page 38)
   - Download Product Maintenance Packages for Old Product Releases and Service Packs (see page 39)
   - Manage Maintenance Downloaded External to CA MSM (see page 40)

   Contact your system administrator, if necessary.

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

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

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.

Download Product Maintenance Packages

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

To download product maintenance packages

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

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

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

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

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

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

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

   The maintenance packages are downloaded.

More information:

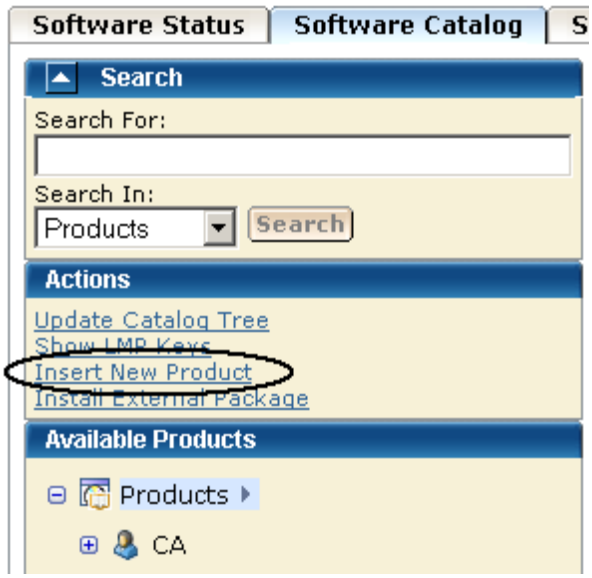
Download Maintenance Packages for Old Product Releases and Service Packs (see page 39)
Apply Maintenance (see page 41)

Download Maintenance Packages for Old Product Releases and Service Packs

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

To download maintenance packages for a product release not in the software catalog

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



   You are prompted to supply information about the product release.

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

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

   The product release is added to the software catalog.

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

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

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

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

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

More information:

Apply Maintenance (see page 41)

Manage Maintenance Downloaded External to CA MSM

Some maintenance, such as unpublished maintenance, APARs, and USERMODs, are acquired by means other than through CA MSM. You can add information about these maintenance packages to CA MSM from the Software Catalog tab.

Migrating these maintenance packages to CA MSM enables you to have a complete view of all the maintenance for a product release. After a package is migrated, you can use CA MSM to apply the maintenance (see page 41).

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

To migrate information about a maintenance package downloaded by other means

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

   The maintenance packages for the release are listed.

2. Click the Add External Maintenance button.

   You are prompted to enter a path for the package.

3. Specify the data set name for the package or the USS path to the package you want to migrate, and click OK.

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

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

More information:

Apply Maintenance (see page 41)

Apply Maintenance

After maintenance has been downloaded for a product, you can apply (install) the maintenance to an existing SMP/E product installation environment. The process starts a wizard that guides you through the maintenance steps. At the end of the wizard, a task dynamically invokes the SMP/E and other utilities required to apply the maintenance.

Note: You can also apply maintenance to an SMP/E environment through the SMP/E Environments, Maintenance tab.

To apply maintenance to a product

1. Click the Software Catalog tab, and select the product from the tree at the left.

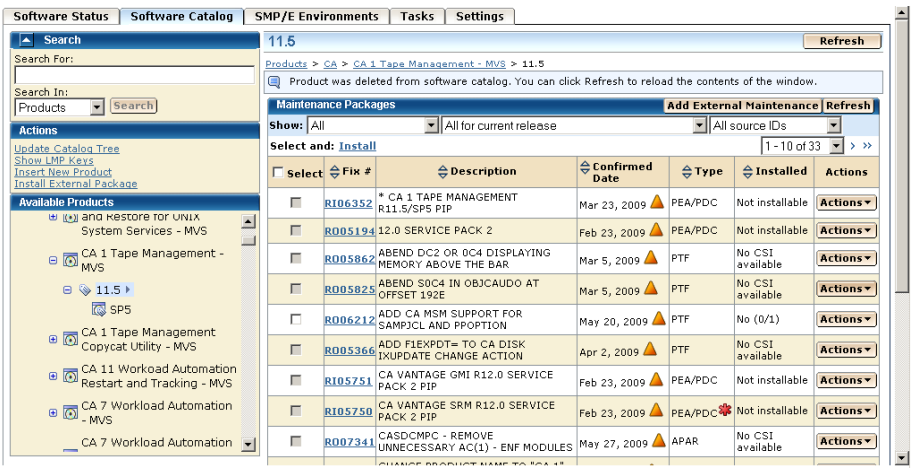
   Maintenance information appears at the right for the releases you have.

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

   The maintenance information is updated.

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

   The maintenance packages are listed, for example:



   Red asterisks identify HIPER maintenance packages.

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

   The Maintenance Package Details dialog appears, identifying any prerequisites.

   Click Close to return to the Maintenance Packages section after you review the information for a package.

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

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

   The Introduction tab of the wizard appears.

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

   The packages to install are listed.

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

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

8. Select the environments in which you want to install the packages, and click Next.

   - If prerequisites exist and are available, review them and click Next. CA MSM installs these prerequisites as part of the process. If a prerequisite is *not* available, the wizard cannot continue. You must acquire the prerequisite and restart the process.
   - If HOLDDATA (see page 37) entries exist, review and select them, and click Next.

   A summary of the task appears.

9. Review the summary, and click Finish.

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

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

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

More information:

Download Product Maintenance Packages (see page 38)
Download Maintenance Packages for Old Product Releases and Service Packs (see page 39)
Manage Maintenance Downloaded External to CA MSM (see page 40)

USERMODs

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

You can create a USERMOD manually, or we can provide an unpublished maintenance package as a USERMOD. In this case, the USERMOD file, which contains the ++USERMOD statement and the body of the USERMOD, must be managed as an externally downloaded package (see page 40).

Back Out Maintenance

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

To back out a maintenance package from a product release

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

   Products installed in the environment are listed.

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

   The features in the component are listed.

   Note: If you want to back out maintenance from all the products in the environment, you can click the Maintenance tab to list all the maintenance packages for the environment.

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

   The maintenance packages for the feature are listed.

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

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

   The Introduction tab of the wizard appears.

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

   The packages to back out are listed.

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

   The Prerequisite tab of the wizard appears.

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

   A summary of the task appears.

8. Review the summary, and click Restore.

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

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

Note: When you have completed the procedures in this section, go to Configuring Your Product (see page 73).

Chapter 4: Installing Your Product from Pax-Enhanced ESD

This section contains the following topics:

How to Install a Product Using Pax-Enhanced ESD

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

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

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

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

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

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

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

   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-file-name`*

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

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

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

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

More Information:

USS Environment Setup (see page 50)
Allocate and Mount a File System (see page 51)
Copy the Product Pax Files into Your USS Directory (see page 53)
Create a Product Directory from the Pax File (see page 58)
Copy Installation Files to z/OS Data Sets (see page 59)

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. For additional ESD information, go to ca.com/mainframe. Under Events, we offer an ESD webcast to further explain the Pax-Enhanced ESD process.

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 47) 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.

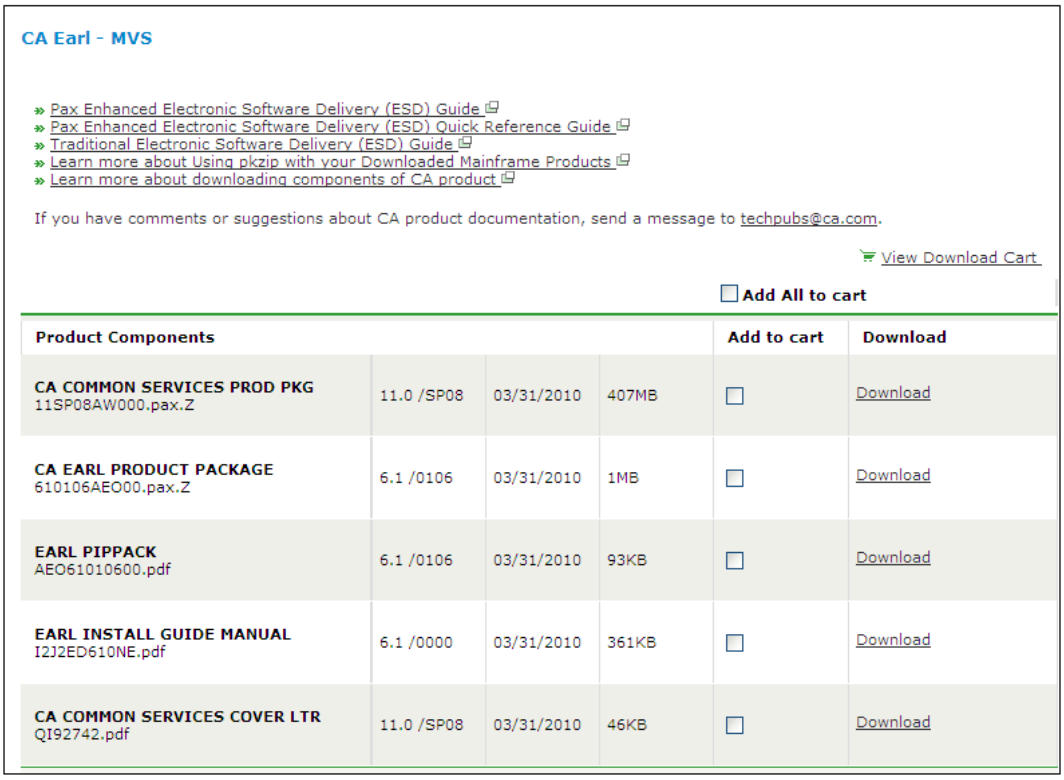
4. Perform the steps to install the product based on the product-specific steps.

   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

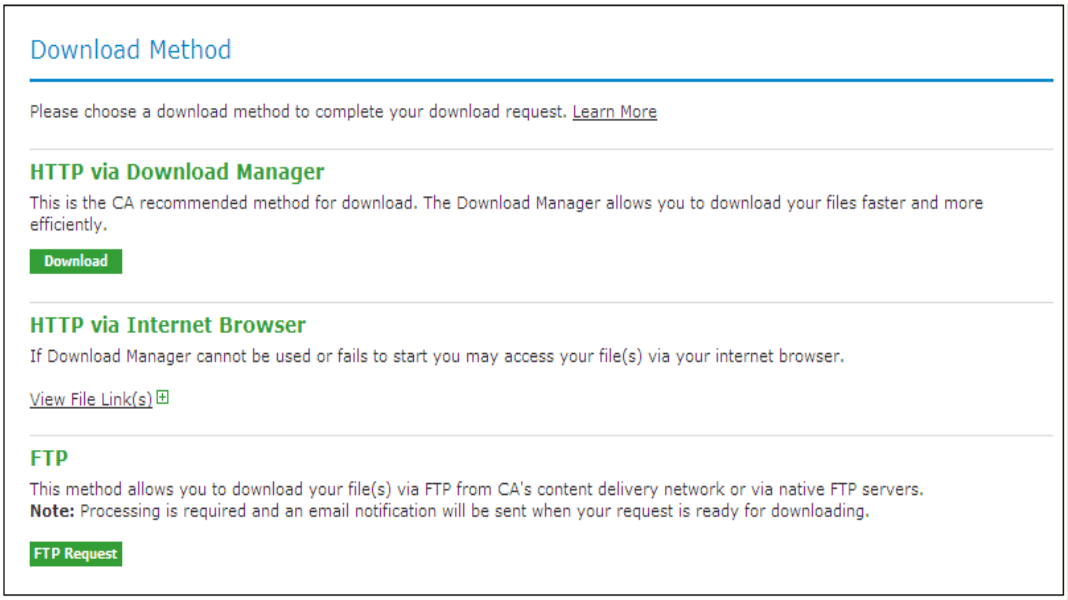
If you have comments or suggestions about CA product documentation, send a message to techpubs@ca.com.

View Download Cart

☐ Add All to cart

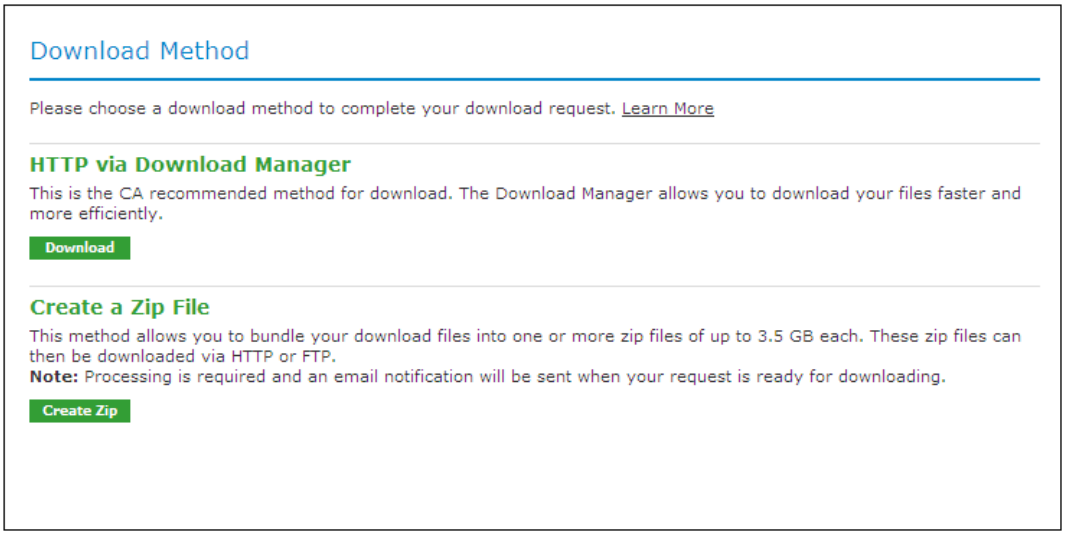
Product Components				Add to cart	Download
CA COMMON SERVICES PROD PKG 11SP08AW000.pax.Z	11.0 /SP08	03/31/2010	407MB	☐	Download
CA EARL PRODUCT PACKAGE 610106AEO00.pax.Z	6.1 /0106	03/31/2010	1MB	☐	Download
EARL PIPPACK AEO61010600.pdf	6.1 /0106	03/31/2010	93KB	☐	Download
EARL INSTALL GUIDE MANUAL I2J2ED610NE.pdf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

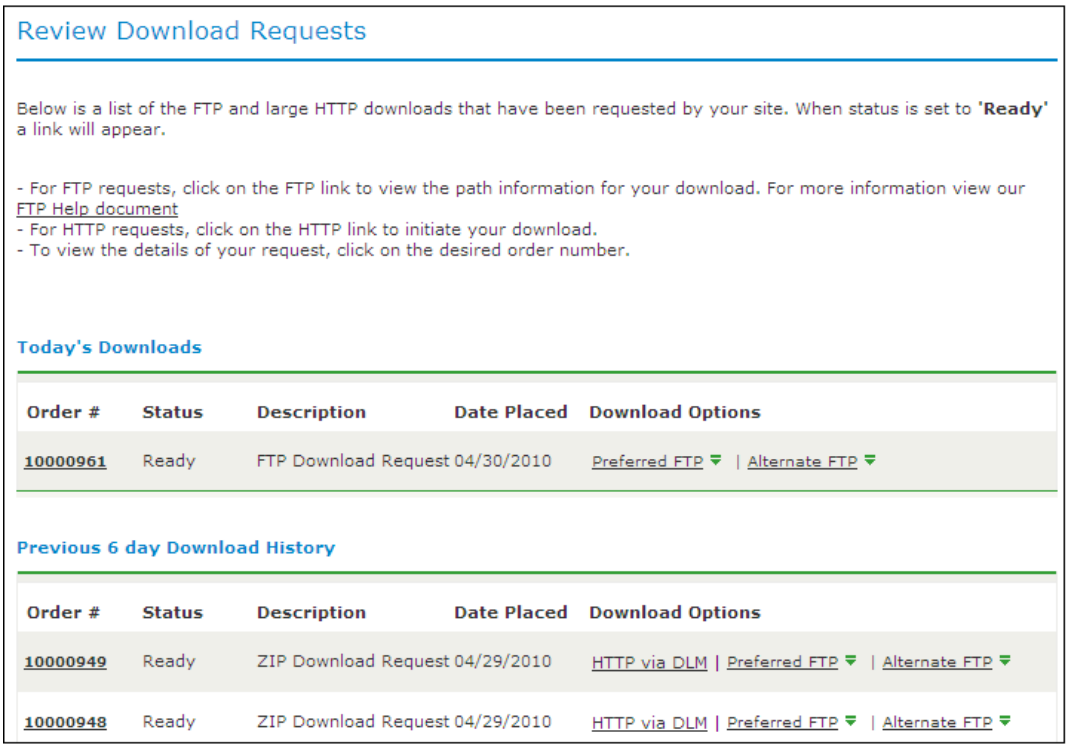
Note: For mainframe downloads using this HTTP method, click the Learn More link.



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 Pax-Enhanced ESD downloads.

This procedure details how to perform the following tasks:

- Allocate a zFS or an HFS file system.
- Create a mount point in an existing maintenance directory.
- Mount the file system on the newly created mount point.
- Optionally permit write access to anyone in the same group as the person who created the directory.

Important! USS commands are case-sensitive.

To allocate and mount the file system

1. Allocate the HFS. For example:

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

   The HFS is allocated.

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

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. For example, from TSO, enter the following command:

   ```
   MOUNT       FILESYSTEM('yourHFS 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 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 46)
ESD Product Download Window (see page 47)

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.

To download files using batch JCL

1. Supply a valid JOB statement.
2. Replace *yourTCPIP.PROFILE.dataset* with the name of the TCPIP 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 world-wide 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.

To upload files to the mainframe through a PC

1. Follow the procedures in How the Pax-Enhanced ESD Download Works (see page 10) 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.

To create a product installation directory using the Unpackage.txt sample job

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.

Example 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.

To copy the Pax-Enhanced ESD installation files to z/OS data sets

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)*.

Receiving the SMP/E Package

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

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

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

How to Install Products Using Native SMP/E JCL

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

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

Prepare the SMP/E Environment for Pax Installation

The members used in this procedure prepare the data sets, initialize the zones, and create the DDDEFs for CA Tape Encryption.

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

To prepare the SMP/E environment for your product

1. Customize the macro TBESEDIT with your site-specific information and then copy the macro to your SYSPROC location. Replace the rightmost parameters for each ISREDIT CHANGE macro command. Each time you edit an installation member, type TBESEDIT on the TSO 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 TBESEDIT macro each time you open a new SAMPJCL member. To edit all SAMPJCL members simultaneously, read and follow the instructions in the TBEEDALL member.

2. Open the SAMPJCL member TBE1ALL in an edit session and execute the TBESEDIT macro from the command line.

   TBE1ALL is customized.

3. Submit TBE1ALL.

   This job produces the following results:

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

4. Open the SAMPJCL member TBE2CSI in an edit session and execute the TBESEDIT macro from the command line.

   TBE2CSI is customized.

5. Submit TBE2CSI.

   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 TBE3RECD in an edit session and execute the TBESEDIT macro from the command line.

   TBE3RECD is customized.

2. Submit the *yourhlq*.SAMPJCL member TBE3RECD to receive SMP/E base functions.

   CA Tape Encryption is received and now resides in the global zone.

3. Open the SAMPJCL member TBE4APP in an edit session and execute the TBESEDIT macro from the command line.

   TBE4APP is customized.

4. Submit the *yourhlq*.SAMPJCL member TBE4APP to apply SMP/E base functions.

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

5. Open the SAMPJCL member TBE5ACC in an edit session and execute the TBESEDIT macro from the command line.

   TBE5ACC is customized.

6. Submit the *yourhlq*.SAMPJCL member TBE5ACC to accept SMP/E base functions.

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

Clean Up the USS Directory

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

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

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

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

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

To delete the pax files and product-specific directories

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

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

   `rm paxfile`

   paxfile

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

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

   `rm -r product-specific-directory`

   product-specific-directory

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

   The product-specific directory is deleted.

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

Apply Maintenance

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

To apply maintenance

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 TBESEDIT macro was customized in the installation steps. Verify that you still have the values from the base install.
4. Open the SAMPJCL member TBE6RECP in an edit session and execute the TBESEDIT macro from the command line.

   TBE6RECP is customized with your JOB statement, CSI location, and zone names.
5. Customize the TBE6RECP SMPPTFIN and SMPHOLD DD statements to reference the FB 80 data sets for the PTFs and HOLDDATA.
6. Submit TBE6RECP.

   The PTFs and HOLDDATA are received.
7. Open the SAMPJCL member TBE7APYP in an edit session and execute the TBESEDIT macro from the command line.

   TBE7APYP is customized.
8. Submit TBE7APYP.

   The PTFs are applied.
9. (Optional) Open the SAMPJCL member TBE8ACCP in an edit session and execute the TBESEDIT macro from the command line.

   TBE8ACCP is customized.
10. (Optional) Submit *yourhlq*.SAMPJCL member TBE8ACCP.

    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's policy.

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

HOLDDATA

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

Note: When you have completed the procedures in this section, go to Configuring Your Product (see page 73).

Chapter 5: Installing Your Product from Tape

This section contains the following topics:

Unload the Sample JCL from Tape

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

To unload the sample JCL from tape

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.

nnnnnn

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 the SMP/E environment set up, go to Run the Installation Jobs for a Tape Installation.
   - If you *do not* have the SMP/E environment set up, 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 used in this procedure prepare the data sets, initialize the zones, and create the DDDEFs for CA Tape Encryption.

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

To prepare the SMP/E environment for your product

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

   The macro is ready to customize your TBE.SAMPJCL members.

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

2. Open the SAMPJCL member TBE1ALL in an edit session and execute the TBESEDIT macro from the command line.

   TBE1ALL is customized.

3. Submit TBE1ALL.

   This job produces the following results:

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

4. Open the SAMPJCL member TBE2CSI in an edit session and execute the TBESEDIT macro from the command line.

   TBE2CSI is customized.

5. Submit TBE2CSI.

   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 TBE3RECT in an edit session and execute the TBESEDIT macro from the command line.

   Note: Comment out any unwanted FMIDs.

   TBE3RECT is customized.

2. Submit the *yourhlq*.SAMPJCL member TBE3RECT to receive SMP/E base functions.

   CA Tape Encryption is received and now resides in the global zone.

3. Open the SAMPJCL member TBE4APP in an edit session and execute the TBESEDIT macro from the command line.

   Note: Comment out any unwanted FMIDs.

   TBE4APP is customized.

4. Submit the *yourhlq*.SAMPJCL member TBE4APP to apply SMP/E base functions.

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

5. Open the SAMPJCL member TBE5ACC in an edit session and execute the TBESEDIT macro from the command line.

   Note: Comment out any unwanted FMIDs.

   TBE5ACC is customized.

6. Submit the *yourhlq*.SAMPJCL member TBE5ACC 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. When the maintenance process is complete the product is ready to deploy.

To apply maintenance

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 TBESEDIT macro was customized in the installation steps. Verify that you still have the values from the base install.
4. Open the SAMPJCL member TBE6RECP in an edit session and execute the TBESEDIT macro from the command line.

   TBE6RECP is customized with your JOB statement, CSI location, and zone names.

5. Customize the TBE6RECP SMPPTFIN and SMPHOLD DD statements to reference the FB 80 data sets for the PTFs and HOLDDATA.
6. Submit TBE6RECP.

   The PTFs and HOLDDATA are received.

7. Open the SAMPJCL member TBE7APYP in an edit session and execute the TBESEDIT macro from the command line.

   TBE7APYP is customized.

8. Submit TBE7APYP.

   The PTFs are applied.

9. (Optional) Open the SAMPJCL member TBE8ACCP in an edit session and execute the TBESEDIT macro from the command line.

   TBE8ACCP is customized.

10. (Optional) Submit *yourhlq*.SAMPJCL member TBE8ACCP.

    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's policy.

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

HOLDDATA

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

Maintenance for Other CA Products

You must apply maintenance to CA 1 and CA TLMS to enable communication between the tape management system and CA Tape Encryption.

Important! CA Tape Encryption will not function without this maintenance.

If you are using the CA Tape Encryption SAF Interface and you use CA ACF2 or CA Top Secret you must apply the appropriate product maintenance to provide this support.

For more information, see the cover letter for the exact PTFs that must be applied for each product.

If you have IBM DFSMSrmm, obtain maintenance from IBM that enables the DFSMSrmm CDS BESKEY index to identify tapes encrypted by CA Tape Encryption.

Note: When you have completed the procedures in this section, go to Configuring Your Product (see page 73).

Chapter 6: Configuring Your Product

This section describes the minimum configuration tasks needed before CA Tape Encryption can be started, customized, and used in your environment.

This section contains the following topics:

Copy the CA Encryption Key Manager Procedures

This procedure copies the CA Tape Encryption procedures from the CTAPPROC library to the system procedure library on the system where CA Tape Encryption will run.

To copy the CA Tape Encryption procedures

1. Copy the CTAPJCL, CTAPPARM, and CTAPEARL data sets to working data sets.

   You are protected from losing any customization if new members of these data sets are provided through SMP/E maintenance.

2. Modify and run the JCL provided in member BTE09PRC in the CTAPJCL data set.

   The CA Tape Encryption procedures are copied from the CTAPPROC library to the system procedure library on the system where CA Tape Encryption will run.

3. Update each procedure to reflect the data set names in use at your site.

Define the Primary and Mirror Databases

The primary and mirror databases are defined as VSAM Linear data sets.

To allocate the CA Tape Encryption primary and mirror databases

1. If CA Tape Encryption runs in a shared environment, place the databases on shared DASD. Define the two databases on separate DASD volumes.

   If installing CA Tape Encryption in multiple environments with separate primary and mirror databases, use a different name for the primary and mirror databases in each environment.

2. Update job BTE10DDB in CTAPJCL to specify the PREFIX in use at your company.

The BES primary and mirror databases are automatically formatted and initialized when they are first opened by a BES task.

Update ICSF and the Security System

Updating your security system permissions ensures that your BES and ICSF resources work correctly.

To update your security

1. Update your security system to provide the following:
   - Control access to the PREFIX used for BES databases
   - Update access to:
     - IRR.DIGTCERT.LISTRING (If B2B tapes are to be created.)
     - ICSF CKDS (If you save keys in the CKDS.)
   - Read access to general resource classes:
     - CSFKEYS
     - CSFSERV
2. Define the following ICSF startup parameters:
   - Configure ICSF with parameter SSM(YES)
   - CHECKAUTH(NO) (Recommended for improved performance.)

Note: For more information about resource classes, see the IBM ICSF Administrator's Guide, the *IBM Security Server RACF Security Administrator's Guide*, the *CA ACF2 for z/OS Administrator Guide*, and the *CA Top Secret for z/OS User Guide*

Authorize the CA Tape Encryption Load Library

Authorizing the load library allows the programs to be executed.

To authorize the load library

1. Update the appropriate PROG*xx* member of SYS1.PARMLIB on your target system to specify the CA Tape Encryption load library name and the VOLSER it resides on.
2. Place the CA Tape Encryption load library (CAI.CTAPLINK) and the ICSF load library in your LNKLIST (link list) concatenation. This is consistent with IBM's recommendation to place the ICSF load library in your LNKLIST concatenation.
3. Update the appropriate PROG*xx* or LNKLST*xx* member of SYS1.PARMLIB on your target system to specify the CA Tape Encryption load library name and the ICSF load library if not already done.
4. If the HLQ (High Level Qualifier) is not defined in the master catalog, udd the VOLSER parameter for the DASD volume where the CA Tape Encryption load library resides.

Concurrent Releases

If you are running an older version of CA Tape Encryption or CA Encryption Key Manager in the same LPAR as the Release 14.5.00 release, issue the command RELOAD=SECURITY to the most current BES subsystem. The BES SAF security facility must be at Release 14.5.00 or greater to enable application requests to the CA Encryption Key Manager Option for Application Management.

CA Auditor Considerations

CA Tape Encryption installs load module CAIXCEA@ into the CTAPLINK data set. CAIXCEA@ is the CA Auditor Product Description Module (PDM) for CA Tape Encryption. CAIXCEA@ is updated to reflect the service pack or release level as new levels of CA Tape Encryption are made available.

If you:

- Have CA Auditor and wish to include CA Tape Encryption in the list of products audited, this module should reside in the currently active LPA.
- Do *not* have CA Auditor, update the BES procedure to add a STEPLIB DD for the CTAPLINK data set so that module CAIXCEA@ can be located to identify the current release and service pack level of CA Encryption Key Manager.

Define the System Options in the Parameter Library

Before commencing this step, determine if the BES database will be encrypted with a single pass phrase or dual pass phrases.

A request for the pass phrase is issued whenever CA Tape Encryption is started on a CPU other than the one that the first install was performed on. For example, if you start CA Tape Encryption at a disaster recovery site with a copy of the home site database or after upgrading your CPU, the request is issued. If the correct pass phrase is not entered, CA Tape Encryption does not start up and you will not be able to read or write any encrypted tapes.

Some experts consider a single pass phrase a security exposure. Anyone who knows the pass phrase can gain access to your encryption information or could change the current pass phrase. CA Tape Encryption allows the use of two pass phrases entered by separate individuals. These pass phrases are combined, hashed and saved in the database for future reference like the single pass phrase.

With dual pass phrases and proper physical security, no individual is able to gain access to your encryption information or change the current pass phrase.

To define system options

1. Modify the following STARTUP member parameters:

   DsnameBESPrimaryDB=*name*

   Specify the name of the BES primary database to reflect the data set name created in Define the CA Tape Encryption Primary and Mirror Databases (see page 74).

   DsameBESMirrorDB=*name*

   Specify the name of the BES mirror database to reflect the data set name created in Define the CA Tape Encryption Primary and Mirror Databases (see page 74).

   LicensedEncryptedDatasetsMonthly=*value*

   Specify a value that corresponds to the type of license purchased for CA Tape Encryption.

   PassPhraseCount=[1|2]

   Specify if single or dual pass phrase control is used on the data in the BES database. The options are:

   1

   (Default) Single pass phrase. A database encrypted with a single pass phrase can be converted to use dual pass phrases. Single phrase control is compatible with previous releases.

   2

   Dual pass phrases. A database encrypted with a dual pass phrases cannot be converted to use a single pass phrase.

   All of the BES address spaces that share the database must be at the same maintenance level.

   If you plan to use dual pass phrase control, set PassPhraseID1 and PassPhraseID2 to identify the individuals who will maintain a written copy of the pass phrases, such as “Storage Administrator” and “Security Administrator”.

   The remaining parameters have defaults that work in most customer environments.

For information on the dual pass phrases and other parameters, see the *Configuration Guide*.

Note: Unless otherwise noted, references to “parmlib” refer to the CA Tape Encryption parameter library.

Optionally, you can define system protection and data set selection profiles to the CA@BES resource class. Entities within CA@BES are used by the CA Tape Encryption SAF Interface to protect system commands, encryption keys, and utilities. The SAF Interface can be used in place of DFSMS or with DFSMS to select data sets for encryption.

For information about using these security system features, see the *Administration Guide*.

Tailor the LMP Keys

This product is part of the CA License Management Program (C LMP). CA LMP is distributed as part of the CA Common Services for z/OS CAIRIM component and consists of the following:

- CA product
- CA LMP Product Key Certificate with an execution key for each CPU licensed at your site
- Common CA LMP enforcement software

The pack list contains a CA LMP Product Key Certificate that corresponds to the CA Tape Encryption product option that you are running.

To tailor the LMP keys

1. Enter the keys into the PPOPTION data set CA LMP product keys member that has a default name of KEYS.
2. Edit the information as needed.

Chapter 7: Deploying Your Product

This chapter describes the tasks needed to deploy [set the DSI variable value for your book] in your environment.

Note: Skip this chapter if you use CA MSM to deploy [set the DSI variable value for your book].

This section contains the following topics:

Verify Basic Functionality

When CA Tape Encryption is operational the BES primary and mirror databases are secure.

To verify that CA Tape Encryption is operational

1. To start the BES address space, enter the command:

   `S BES.`*`stepname`*

   stepname

   Defines the subsystem name.

   Values: BES1 to BES8

   The BES address space starts and dynamically updates the stepname value into the subsystem name table and uses it as its subsystem name.

2. To start CA Tape Encryption, enter the command:

   `BES`*`n`* `D S`

   n

   Specifies the BES address space. This must be the same number used in step 1.

   The output of the command shows the following:

   - That both CA Tape Encryption and ICSF have been properly installed and activated on your system.
   - That the proper maintenance for CA 1 and CA TLMS has been applied to your system to support CA Tape Encryption.
   - The first time the BES primary database is used, a message is displayed indicating that a new database is being initialized.

3. Enter a cryptographic pass phrase of up to 64 characters.

   The integrity of the BES primary database and the BES mirror database is secured.

Important! Keep a record of the pass phrase stored securely and with restricted access. The pass phrase is required when starting a disaster recovery system or when upgrading to a different central processing unit.

For the CA 1, CA TLMS, and Third Party Tape Management System Options, you can verify the basic functionality of CA Tape Encryption by running job BESIVP in the CTAPJCL data set. The BESIVP job runs IEBGENER in the following three steps to verify encryption and decryption processing:

- Step GENER1 executes program IEBGENER to read a member of the parmlib data set and write it to tape in encrypted format.
- Step GENER2 adds another parmlib member to the tape file created in step GENER1, using MOD processing. The additional data is encrypted using the same encryption algorithm.
- Step LIST reads the tape file created in the first two steps and automatically decrypts it, resulting in a printout of the two PARMLIB members in clear text.

All steps must run with a condition code of 00. If CA Tape Encryption is properly installed, message BES*n*T0001I is issued for each step. If this message is not issued, encryption activity is not being performed, and further analysis is necessary.

The CA Vtape and CA Disk Options can be tested by setting their encryption parameters and performing backstore or a backup/archival to tape.

Refer to the comments in the BESIVP job for details on the customization required. As part of the installation procedure you set up the Symmetric Keys to be used at your site or accepted the default keys shipped with CA Tape Encryption. Prior to running BESIVP, set up a data class that references one of the Symmetric Keys defined in parmlib. The data class you set up must be specified in the first step of BESIVP.

Note: For information about creating the DFSMS data classes to control encryption processing, see the *Administration Guide.*

Check the ACS routines on the target system to insure that they permit the data class to be assigned by the JCL and do not override it with another data class. If you do not see the *BESn*T0001I message, check the job log to see that the expected data class was assigned.

Chapter 8: Managing Business to Business (B2B) Partnerships

This section contains the following topics:

CA Tape Encryption Business-to-Business Processing

CA Tape Encryption allows you to send encrypted tapes to business partners on other z/OS systems or on selected distributed platforms. This is known B2B processing. To decrypt tapes created by CA Tape Encryption, your business partners must do one of the following:

- On z/OS platforms, install and run the CA Tape Encryption base product.
- On Microsoft Windows, Linux, and Sun Solaris platforms, install the Multiplatform Decryption Utility (MDU).

Both the CA Tape Encryption base product and the MDU are available to your business partners free of charge.

What z/OS Business Partners Need to Decrypt B2B Tapes

After you contact your z/OS business partners and agree on the use of CA Tape Encryption, your business partners need to install the free base product, as outlined by the following points:

- Each z/OS partner that wants to process tapes encrypted by CA Tape Encryption should call 1-866-573-3435 and inform the Customer Service Representative that they need to order the free CA Tape Encryption base product.
- The representative will take the necessary information to process and ship the order and provide the required License Managed Product (LMP) key to activate the base product. This license will entitle the z/OS business partner to receive regular maintenance for CA Tape Encryption.

Required Maintenance for z/OS Business Partners

Business partners who install the free CA Tape Encryption base product must plan to keep the product up to date on maintenance using the CA technical support site http://ca.com/support.

What Distributed Business Partners Need to Decrypt B2B Tapes

After you contact your business partners that run distributed systems and agree on the use of CA Tape Encryption, these business partners need to install the Multiplatform Decryption Utility (MDU), as outlined by the following points:

- Business partners who need to process tapes on distributed systems that were encrypted by CA Tape Encryption on the mainframe do not need to order and install the CA Tape Encryption base product.
- These partners should obtain the Multiplatform Decryption Utility (MDU) from the site that creates the encrypted tape.
  - The MDU is delivered as part of the z/OS product install in a ZIP or TAR file format that allows for easy transmission or sharing on a CD-ROM or other media.
  - The MDU files are delivered in a z/OS data set named CAI.CTAPMDU.

Note: For information about the MDU, see the instructions provided in CAI.CTAPMDU member $MDUNDX and the *Multiplatform Decryption Utility User Guide*.

Required Maintenance for Distributed Business Partners

Business partners who install the MDU on their distributed systems must plan to apply maintenance to the MDU. Maintenance is provided in new TAR and ZIP files delivered to the z/OS product. When maintenance is provided, the new TAR or ZIP file must be sent to the distributed systems that run the MDU. This maintenance must be installed using the instructions provided in the *Multiplatform Decryption Utility User Guide.*

To insure that proper maintenance is applied, all PTFs that provide maintenance to the MDU include an SMP/E ACTION HOLD.

How You Identify MDU Versions

The ISPF statistics of the members in the CAI.CTAPMDU data set show the date, time and PTF level of the MDU. The maintenance level of the MDU on your target system can be determined by reviewing the readme file delivered with the MDU utility.

Index

M

P

R

S

T

U