S/390®

Support Element Operations Guide

Version 1.6.1

Multiprise® 3000 Enterprise Server

Level 01a, February 28, 2001
GC38-0607-01

S/390®

Support Element Operations Guide

Version 1.6.1

Level 01a, February 28, 2001
GC38-0607-01

Note!

Before using this information and the product it supports, read the information in “Safety notices” on page xi and Appendix C, “Notices” on page C-1.

Second Edition (June 2000)

This edition, GC38-0607-01, applies to the IBM Support Element Console Application, Version 1.6.1.

This edition replaces GC38-0607-00. A technical change to the text or illustration is indicated by a vertical line to the left of the change.

Contents

Safety

Safety notices

Safety notices are printed throughout this document. **DANGER** notices warn you of conditions or procedures that can result in death or severe personal injury. **CAUTION** notices warn you of conditions or procedures that can cause personal injury that is neither lethal nor extremely hazardous. **Attention** notices warn you of conditions or procedures that can cause damage to machines, equipment, or programs.

There are no **DANGER** notices in this document.

Coupling Facility Channel Laser Safety Information

CAUTION:
The coupling facility channel laser ports are designed and certified for use only with optical fiber and connectors having characteristics specified by IBM. The use of any other connectors or fiber may result in emission of laser power levels capable of producing injury to the eye if directly viewed. Use of non-specified connectors or fiber could violate the class 1 certification.

CAUTION:
Data processing environments can contain equipment transmitting on system links with laser modules operating at greater than class 1 power levels. For this reason, it is advised never to look into the end of an optical fiber cable or open receptacle. The inspection or repair of optical fiber cable assemblies and receptacles should be performed by trained service personnel only.

Laser Compliance

The coupling facility channel modules are certified in the U.S. to conform to the requirements of DHHS 21 CFR Subchapter J for Class 1 laser products. Elsewhere, they are certified to be in compliance with IEC 825 (first edition 1984) and CENELEC HD 482 S1 as a Class 1 laser product. The coupling facility channel modules have also been tested and approved to comply with international Class 1 laser product certifications. Consult the label on each part for laser certification numbers and approval information.

Class 1 laser products are not considered to be hazardous. Internally, the coupling facility channel modules operating on multimode fiber contain a Class 3b laser that is nominally a 5.0 milliwatt source operating in the wavelength region of 780-850 nm. Internally, the coupling facility channel modules operating on single-mode fiber contain a class 3b laser that is nominally a 5.0 milliwatt source operating in the wavelength region of 1270-1340 nanometers. All coupling facility channel modules are designed so that there is never any human access to laser radiation above a Class 1 level during normal operation, user maintenance, or prescribed service conditions.

Preface

This operations guide is for anyone who is responsible for monitoring and operating the following IBM S/390 product, which are referred to in this operations guide as *systems*:

- IBM S/390 Multiprise 3000 Enterprise Server

This operations guide provides information and instructions for users who use a support element while logged on in the following user modes:

- Access administrator
- Advanced operator
- Operator
- System programmer

Note: Many of the same tasks and controls that are available in the user modes listed above are available also in the service representative user mode. This operations guide does not provide information or instructions for using tasks and controls available exclusively in the service representative user mode. Service representatives should refer instead to the service documentation provided with the system.

Support element users should have experience with S/370™ or S/390 system operations and should also be familiar with using:

- Workstations
- Graphical user interfaces
- Printers
- Tapes and tape devices
- Diskettes and diskette devices
- Optical cartridges and optical drives
- Direct access storage devices (DASD)
- Communication devices

For information and instructions for operating devices other than the support element, refer to the documentation provided with the devices.

How to Use this Guide

The information in this guide is available to you as an online document on the Support Element Console as well as this hardcopy book. To view this guide in its online form, open **Books** in the Views area by double-clicking on the **Books** icon with the left mouse button. After the guide has been opened, the Table of Contents is displayed.

When the Table of Contents is first displayed, the highest level topics are displayed in the order that they appear as chapters in the hardcopy book. If any of these topics have lower level topics, a “+” (plus sign) is displayed to the left of the higher level topic. To expand the topic, click once on the “+” and the next level will be displayed. Other options for expanding topics are available by clicking once on the **Options** pull-down window located at the top of the document. Double-click on any topic to view its text.

The Support Element Console is shipped with OS/2® Warp Version 4 installed. If you have not used this operating system before or are not familiar with common terminology used with manipulating the mouse, read the following information before continuing in this guide. The terms defined below are used throughout this guide.

Graphical User Interface

The following section provides you with information on the graphical user interface to help guide you on the support element console. The user interface has the following elements:

Title The title describes the function performed or the objects listed on the window.

Menu Bar The menu bar shows the different categories of actions that can be performed.

Pull-down Menu A pull-down menu appears when you select a category from the menu bar, and shows a list of choices that you can select. You can select choices from the pull-down menu using either the mouse, the keyboard, or the appropriate mnemonic.

You can also go from one pull-down menu to another by using the left (←) and right (→) cursor control keys. To remove the pull-down menu from the window without making a selection from it, press the **Esc** key or *click* the mouse on an area outside of the pull-down menu.

Pop-up Window A pop-up window can display over the window from which a selection was made. It contains more information to complete the task you are doing, or gives an instructional message.

Scroll Bars The scroll bars allow you to display information that has more data than can be displayed on the panel.

Push buttons The push buttons are rectangular areas at the bottom of the window that contain wording. They look like keys on the keyboard, and when selected, perform similar functions.

Using the Mouse

The mouse controls the pointer that appears on the support element console display. When you move the mouse, the pointer moves the corresponding direction on the screen. You can use the mouse to:

- Select objects, menu choices, entry fields, push buttons, and icons
- Move, size, and switch to other windows
- Scroll information.

To select objects or to drag and drop them, you need to learn a few simple techniques of mouse use. First, a few definitions:

Icon A graphical representation of an object, consisting of an image, image background, and a label.

To point with the mouse
Move the mouse until the mouse pointer rests on the desired spot.

To click the mouse button
Press and release the button once.

To double-click the mouse button
Click the button twice in quick succession.

To select an object
Click on an object's icon with the left mouse button to select it for further action.

To swipe Press and hold down the left mouse button on the first object to be selected. Without releasing the left button, move the mouse's pointer over the other objects to be selected.

To open an object
Double-click on an object's icon with the left mouse button to display another level of detailed information about the object.

To drag an object
Place the mouse pointer on the object's icon. Press and hold down the right mouse button. Then, move the mouse (and the icon) to another location.

To drag several objects
After selecting several objects, place the mouse pointer on one of the selected object's icon. Press and hold down the right mouse button. Then, move the mouse (and the icon) to another location.

To drop an object
Release the right mouse button to drop the dragged object in the new location.

Box Selection
Place the mouse pointer above and to the left of the leftmost, top object to be selected. Move the mouse pointer down and to the right with the left mouse button held down. Complete the box selection by releasing the left mouse button.

This guide reflects the licensed internal code for Support Element Console Application, Version 1.6.1. You can tell if your Support Element Console has this version installed by looking at the title bar on the Support Element Console Workplace window.

How to send your comments

Your feedback is important in helping to provide the most accurate and high-quality information. If you have any comments about this book or any other S/390 documentation:

- Send your comments by e-mail to PUBFDBK@VNET.IBM.COM or PUBFDBK@GDLVME. Be sure to include the name of the book, the form number of the book, the version of the book, if applicable, and the specific location of the text you are commenting on (for example, a page number or table number).
- Fill out one of the forms at the back of this book and return it by mail, by fax, or giving it to an IBM representative.

Chapter 1. Introduction

The S/390 Multiprise 3000 Enterprise Server systems includes an I/O and Support Procesor (IOSP) which provides the support element functions, emulated channel, and device support, a user front end, and point of control and the system image for the CPC.

You can also use a Hardware Management Console, if available, for monitoring and operating an S/390 Multiprise 3000 Enterprise Server:

- An optional Hardware Management Console is available as an additional feature for an S/390 Multiprise 3000 Enterprise Server. Connected by a local area network (LAN) to the support element, the optional Hardware Management Console can be used for monitoring and operating the system, and can be located at greater distances from the system than the support element.
- Hardware Management Consoles used to monitor and operate multiple systems in a Parallel System Complex (Parallel Sysplex®) can also be used to monitor and operate an S/390 Multiprise 3000 Enterprise Server.

In either case, if you use a Hardware Management Console to monitor and operate an S/390 Multiprise 3000 Enterprise Server, refer to the *Hardware Management Console Operations Guide*, GC38-0602.

The support element console application

The Support Element Console Application version 1.6.1 is a licensed application that provides the tasks you will use to monitor and operate your system. The application is shipped with each support element.

The version number of the Support Element Console Application is displayed in the title bars of the Support Element Logon window and the Support Element Workplace window. See “The support element console application” for more information about the windows and the application.

Note: You can use the **System Information** task to determine the EC number of any version of the Support Element Console Application. See “Viewing internal code change information” on page 11-15 for instructions for starting the task.

The Support Element Console Application starts automatically whenever the support element is turned on or rebooted.

Starting the application begins the process of initializing it. You should then see the initialization window containing the IBM Logo and copyright information. When the process completes, the logon window is displayed. You must log on the support element console to verify you are authorized to use it.

You are logged on the support element console automatically when you establish a session with the support element from a Hardware Management Console. If you are not using a Hardware Management Console, you can log on the support element console at the support element.

Note: The Logon window contains message icons and a status indicator. A flashing icon is alerting you that a message was logged that may require your

attention. You will need to log on to view the message. The status indicator reflects the current overall status of the Defined CPCs and images.

Logging on at the support element

You can log on the support element console at the support element. Logging on at the support element typically is necessary only when using a support element to monitor and operate an S/390 Multiprise 3000 Enterprise Server.

Use the Support Element Logon window to log on at the support element. Your *access administrator*, or the person who is responsible for controlling access to the support element console, should have assigned you a user identification and password for logging on the console.

Type your user identification and password in the fields provided on the window, then select the **Log on** push button to log on. Use the online **Help** to guide you through completion.

When logon completes, the support element workplace for your user mode is displayed. The workplace is the window where you start tasks for monitoring and operating your system.

If the S/390 Multiprise 3000 Enterprise Server system is connected to a Hardware Management Console, you can establish a support element console session through the **Single Object Operations** task. See “Establishing a support element console session from a Hardware Management Console” on page 1-3.

Your User Mode

Your *user mode* determines which tasks and controls you can use on the support element workplace.

Default userids and passwords are established as part of a base Support Element Console. The Access Administrator **should assign new userids and passwords as soon as the Support Element Console is installed** for each user using the **User Profiles** task under **Console Actions.** The default userids and passwords are:

```
Operator                OPERATOR   PASSWORD
Advanced Operator       ADVANCED   PASSWORD
System Programmer       SYSPROG    PASSWORD
Access Administrator    ACSADMIN   PASSWORD
Service Representative  SERVICE    SERVMODE
```

To log on, type one of the default userid and password combinations, or the userid and password combination assigned to you. Then press **Enter**, or select the **Log on** push button. Once you log on, the Support Element Console Workplace window is displayed.

Not all tasks are available for each user mode. Refer to the description of the specific task you want to access to see what user mode(s) it is available in.

If at any time you do not know or remember what user mode is currently logged on to the Support Element Console:

1. Click on the System Menu icon located in the upper left corner of the workplace to open the system menu.
2. Click on the **Logon details** menu choice.

   The **Logon Details** window displays and shows the current user mode.

Upon logging on the support element console, the support element workplace for your user mode is displayed:

- When you establish a session with the support element from a Hardware Management Console, you are automatically logged on the support element console in the same user mode assigned to you for logging on the Hardware Management Console.
- When you log on at the support element, you are logged on in the user mode assigned to you for logging on the support element console.

Establishing a support element console session from a Hardware Management Console

A Hardware Management Console can be used for monitoring and operating systems with support elements.

Ordinarily, you should use the Hardware Management Console to monitor status and perform tasks for the systems defined to it. Only the Hardware Management Console can be used for monitoring and operating multiple systems; using it is more efficient than using each system's support element console individually.

Using a system's support element console is necessary only for getting information or using tasks that are *not* available from the Hardware Management Console. If using a system's support element console is necessary, use the Hardware Management Console's **Single Object Operations** task to establish a session with the support element console.

To establish a support element console session from a Hardware Management Console:

1. Locate the task.
2. Open the **Task List** from the **Views** area.
3. Open **CPC Recovery** from the **Task List Work Area**.
4. Open **Groups** from the **Views** area.
5. Open the group that contains the object with the support element that you want to connect to.
6. Select one CPC.
7. Drag and drop the selected object on **Single Object Operations** in the **CPC Recovery** tasks area.

The **Single Object Operations Task Confirmation** window displays to allow you to continue or cancel. Use online **Help** to get additional information to complete the task.

You are logged on the support element console when you establish a session with the support element from a Hardware Management Console. When the automatic logon completes, the support element workplace for your user mode is displayed.

The workplace is the window from where you start tasks for monitoring and operating the CPC.

Note: The support element workplace is distinguished from the Hardware Management Console workplace most notably by the title of its window and the background pattern of IBM's S/390 trademark.

Chapter 2. The Support Element Workplace

The *support element workplace* is the window where you start tasks for monitoring and operating your system.

If you have experience using other systems, you will find that the workplace supports functions, facilities, and controls that are similar to those you have used to monitor and operate similar systems. The workplace presents tasks and their targets graphically, as *icons*. Using the workplace to get information and start tasks is often a matter of monitoring and manipulating icons, rather than, for example, typing commands or using menus.

Icons that represent the functions, facilities, and controls you use to monitor and operate the system and console are referred to as *tasks*. A single icon that represents a set of one or more related tasks is referred to as a *task list*.

Icons that represent the physical and logical elements of the system, which are often the targets of tasks, are referred to as *objects*. The console's objects include:

- Central processor complex (CPC)
- Central processors
- Channel paths
- Images (An *image* is a set of CPC resources capable of running a control program or operating system. One or more images is created during a power-on reset of a CPC. When a power-on reset puts the CPC in logically partitioned (LPAR) mode, each logical partition is an image. Otherwise, when a power-on reset puts the CPC in a basic mode, the CPC has a single image.

A single icon that represents a set of one or more objects of the same type is referred to as a *group*.

The workplace is divided into three *areas* to organize its icons. The three areas are your means of locating the icons to get information or start tasks. The three areas are:

Views
: Located along the top left side of the workplace, this area contains icons you can use to change the type of icons displayed in the work area below it.

Work area
: Located below the Views area, this area contains icons in the current view. Depending on the view, the work area contains either groups, objects, tasks in progress, task lists, tasks for monitoring and operating the console, or online books.

Tasks area
: Located along the right side of the workplace, this area displays the current task list that contain tasks for monitoring and operating the system.

Monitoring and Operating the System

There are three general ways to use the workplace for monitoring and operating the system:

- Monitoring summarized system status.
- Getting detailed system status.
- Starting tasks for monitoring and operating the system.

Monitoring summarized system status

Use the Views area to monitor summarized system status by monitoring the background color of the area.

The system includes all console objects that represent physical and logical elements of the system. The status of the system is summarized in one of two ways:

No exceptions
: This is the summarized system status when all objects have acceptable statuses. An *acceptable* status is any object status that is normal, is as expected, or does not require your immediate attention or intervention. That is, an object with an acceptable status is OK as is.

Exceptions
: This is the summarized system status when one or more objects have unacceptable statuses. An *unacceptable* status is any object status that is not normal, is not as expected, or requires your immediate attention when it occurs. That is, an object with an unacceptable status is not OK, and may require your intervention to make it OK again.

An *exception occurs* when the status of an object becomes unacceptable. The object is referred to as an *exception* while its status remains unacceptable.

When an exception occurs, the status of the system also becomes unacceptable. But rather than monitoring the system's status by monitoring whether its individual objects become exceptions, you can recognize when an exception occurs by monitoring the background color of the Views area. The default colors, green and red, are set for indicating no exceptions and exceptions, respectively. The colors are used for the Views area, to indicate the summarized status of the system, as follows:

- When there are no exceptions, the area's background color is green, the color set for indicating there are no exceptions.
- When an exception occurs, the area's background color changes to red, the color set for indicating there are exceptions.
- The area remains red, the color set for indicating there are exceptions, until you open the **Exceptions** view. Upon opening the view, the area's background color returns to green, the color set for indicating there are no exceptions, to indicate there are no *new* exceptions.

  Note: The **Exceptions** view is described in the next section; see “Locating objects with unacceptable status” on page 2-8.

Monitoring system status exclusively

If you intend to use the workplace exclusively for monitoring summarized system status, consider reducing the size of the workplace to emphasize the Views area. For example, you may want to leave the console temporarily unattended, yet be able to check the system status at a glance by checking the color of the Views area.

Consider reducing the size of the workplace also if you intend to use the console to monitor several windows, including the workplace, simultaneously. Reducing the workplace to emphasize the Views area makes space available for displaying other windows. For example, you may want to use the console's 3270 emulator, yet be able to continue monitoring system status.

To reduce the workplace to emphasize the Views area:

1. Locate the sizing controls in the upper right corner of the workplace.

   From left to right, the four sizing controls are: the *autosize* button, the *log off* button, the *minimize* button, and the *maximize* button.

2. Click on the autosize button to automatically reduce the workplace to a size that emphasizes the Views area.

   Click on the autosize button again to restore the workplace to its previous size.

Getting detailed system status

Use Views and the work area to get detailed system status by checking the individual status of the following objects that represent physical or logical elements of the system:

- Central processor complex (CPC)
- Central processors
- Channel paths
- Images

Like the background color of the Views area, the background color of an object's icon indicates whether its status is acceptable or unacceptable. The background color of an object's icon indicates the object's status in one of two ways:

No color
: This indicates the object's status is acceptable. An *acceptable* status is any object status that is normal, is as expected, or does not require your immediate attention or intervention. That is, an object with an acceptable status is OK as is.

Color
: This indicates the object's status is unacceptable. The specific color indicates the object's specific, unacceptable status. An *unacceptable* status is any object status that is not normal, is not as expected, or requires your immediate attention when it occurs. That is, an object with an unacceptable status is not OK, and may require your intervention to make it OK again.

Therefore, checking whether the individual status of an object is acceptable or unacceptable requires locating a group that contains the object, then checking the background color of the object's icon.

Locating groups and objects

Use Views and the work area to locate objects. Objects are divided into groups of objects of the same type. To locate a particular object, you must locate and open the group that contains it. Opening a group displays its objects in the work area.

To open a group:

1. Open **Groups** from Views.
2. Locate the group that contains the type of objects you want to locate in the Groups Work Area.
3. Double-click on the group to open it.

Locating the CPC: One of console's default groups, the **CPC** group, contains the object that represents the central processor complex (CPC).

To locate the CPC:

1. Open **Groups** from Views
2. Locate the group labelled **CPC** in the Groups Work Area.
3. Double-click on the **CPC** group to open it.

Locating the CPC's image: When the central processor complex (CPC) is activated in basic mode, one of console's default groups, the **Images** group, contains the object that represents the CPC's image.

In basic mode, the CPC has a single image. An *image* is a set of CPC resources capable of running a control program or operating system.

To locate the CPC's image:

1. Open **Groups** from Views.
2. Locate the group labelled **Images** in the Groups Work Area.
3. Double-click on the **Images** group to open it.

Locating logical partitions: When the central processor complex (CPC) is activated in logically partitioned (LPAR) mode, one of console's default groups, the **Images** group, contains objects that represent the logical partitions.

In LPAR mode, logical partitions are referred to also as images. An *image* is a set of CPC resources capable of running a control program or operating system.

To locate logical partitions:

1. Open **Groups** from Views
2. Locate the group labelled **Images** in the Groups Work Area.
3. Double-click on the **Images** group to open it.

   This displays the objects that represent logical partitions in the Images Work Area.

Locating physical processors and logical processors: The object that represents the central processor complex (CPC) contains objects that represent its physical processors.

Each object that represents a CPC image contains objects that represent either physical processors or logical processors:

- When the CPC is activated in basic mode, it support a single image. Like the CPC, the CPC image also contains objects that represent the CPC's physical processors.
- When the CPC is activated in logically partitioned (LPAR) mode, each logical partition is an image. Each CPC image contains objects that represent a logical partition's logical processors.

On the support element workplace, both physical processors and logical processors are referred to as *central processors (CPs)*.

To locate physical processors:

1. Open the CPC Work Area.

   For instructions, see “Locating the CPC” on page 2-4.
2. In the CPC Work Area, locate the CPC.
3. Right click on the CPC to open its pop-up menu.
4. Select the **CPs** menu choice.

   This displays the objects that represent the CPs in the work area.

To locate logical processors when the CPC is operating in LPAR mode:

1. Open the Images Work Area.

   For instructions, see “Locating logical partitions” on page 2-4.
2. In the Images Work Area, locate the image that represents the logical partition to which the logical processors are assigned.
3. Right click on the image to open its pop-up menu.
4. Select the **CPs** menu choice.

   This displays the objects that represent the image's logical processors in the work area.

Locating channel paths: The object that represents the central processor complex (CPC) contains objects that represent all channel paths defined in its input/output (I/O) configuration.

To locate all channel paths in the CPC's I/O configuration:

1. Open the CPC Work Area.

   For instructions, see “Locating the CPC” on page 2-4.
2. In the CPC Work Area, locate the CPC.
3. Right click on the CPC to open its pop-up menu.
4. Select the **CHPIDs** menu choice.

   This displays the objects that represent the channel paths in the work area. Each channel path is labelled with its channel path identifier (CHPID).

When the central processor complex (CPC) is activated in logically partitioned (LPAR) mode, in which the CPC's images are its logical partitions, each image contains objects that represent the channel paths assigned to it.

To locate channel paths assigned to a specific logical partition:

1. Open the Images Work Area.

   For instructions, see “Locating logical partitions” on page 2-4.

2. In the Images Work Area, locate the image that represents the logical partition to which the channel paths are assigned.
3. Right click on the image to open its pop-up menu.
4. Select the **CHPIDs** menu choice.

   This displays only the objects that represent the image's channel paths in the work area. Each channel path is labelled with its channel path identifier (CHPID).

Determining the exact status of an object

After locating an object, check the background color of its icon to determine whether its status is acceptable or unacceptable:

- The icon's background has no color when the object's status is acceptable.
- When the object's status is unacceptable, the icon's background displays the color that identifies the unacceptable status.

Note: If you are not certain which unacceptable status is indicated by the background color of the CPC's icon, double-click on it to open the CPC's *details window*.

Background color of the CPC: The background color of the icon of the central processor complex (CPC) indicates whether the statuses of the CPC, its central processors (CPs), and its channel paths are acceptable or unacceptable. While the statuses are acceptable, the background of the CPC icon has no color. Otherwise, the background color of the CPC indicates unacceptable statuses as follows:

- Until CPC power is turned on and a power-on reset is performed, the background color of the CPC indicates an unacceptable CPC status.
- After CPC power is turned on and a power-on reset is performed:
  - The background color of the left side of the CPC indicates an unacceptable CP status.
  - The background color of the right side of the CPC indicates an unacceptable channel path status.

The background color of the CPC's icon also indicates whether its support element received hardware messages from the CPC. When the support element receives a hardware message, the background color of the CPC changes to the color set for indicating a hardware message was received. The default color is blue.

Note: If the status of the CPC, its CPs, or its channel paths is unacceptable, *and* the CPC's support element received hardware messages, then:

- The color of the top half of the CPC's icon indicates the unacceptable status.
- The color of the bottom half of the CPC's icon indicates the support element received hardware messages.

Background color of images: The background color of an image's icon indicates whether the statuses of the image, its central processors (CPs), and its channel paths are acceptable or unacceptable. While the statuses are acceptable, the background of the image icon has no color. Otherwise, the background color of the image indicates unacceptable statuses as follows:

- While the image is not activated, the background color of the image indicates an unacceptable image status.
- After the image is activated:
  - The background color of the left side of the image indicates an unacceptable CP status.
  - The background color of the right side of the image indicates an unacceptable channel path status.

The background color of the image's icon also indicates whether its support element received operating system messages from the image. When the support element receives an operating system message, the background color of the image changes to the color set for indicating an operating system message was received. The default color is cyan.

Note: If the status of the image, its CPs, or its channel paths is unacceptable, *and* the image's support element received operating system messages, then:

- The color of the top half of the image's icon indicates the unacceptable status.
- The color of the bottom half of the image's icon indicates the support element received operating system messages.

Background color of CPs: The background color of the icon of a central processor (CP) indicates whether the status the CP is acceptable or unacceptable. While the status is acceptable, the background of a CP icon has no color. Otherwise, the background color of the CP is the color that indicates its specific unacceptable status.

Background color of channel paths: The background color of the icon of a channel path indicates whether the status the channel path is acceptable or unacceptable. While the status is acceptable, the background of a channel path's icon has no color. Otherwise, the background color of the channel path is the color that indicates its specific unacceptable status.

Opening an object's details window: If you want to determine the exact acceptable status of an object, or if you are not certain which unacceptable status is indicated by the background color of an object's icon, you can open the object's *details window*.

To open an object's details window:

1. Locate the object.

   For instructions, see the topics that follow “Locating groups and objects” on page 2-4.

2. In the object's work area, double-click on the object.

   This opens the object's details window.

3. To determine an object's exact status, check the display fields in the Instance Information box.

The group box may include more than one display field for indicating an object's status. A single display field is labelled **Status**. Multiple display fields are labelled similarly.

Determining conditions causing test status: If the CPC's performance is affected, an object's icon displays **Test**. This indicates a condition exists, such as I/O tracing, PSW I/O event compare, or Address compare are enabled. To determine the exact conditions causing test status:

1. Locate the object.

   For instructions, see the topics that follow "Locating groups and objects" on page 2-4.

2. In the object's work area, double-click on the object.

   This opens the object's details window.

3. To determine the object's exact status, select the Test Mode push button on the details page.

   The Test mode active indicators window displays the condition(s) for tests.

Use the online **help** for more information on the test indicator.

Locating objects with unacceptable status

You can check the status of an object at any time by locating and opening a group that contains it. But rather than locating exceptions this way, you can use Views and the work area to immediately locate all current exceptions.

To locate objects that are exceptions:

1. Open **Exceptions** from Views.

   This displays all objects with unacceptable statuses in the Exceptions Work Area. (Not all logical objects are displayed. For example, Image CPs.)

2. In the Exceptions Work Area, the background color of each object's icon indicates its current status. If you are not certain which status is indicated by the background color of an object's icon, double-click on the object to open its *details* window.

   This window includes detailed information about the object, including a list of the colors used to indicate its statuses.

Recognizing exceptions

After the background color of the Views area returns to green, indicating there are no new exceptions, you can still recognize *current* exceptions by the background colors of the **Exceptions** icon and of each group that contains an exception:

- Upon opening the **Exceptions** view, the background color of the Views area returns to green, but the **Exceptions** icon remains red, the color set for indicating there are exceptions.

  The **Exceptions** icon remains red until the last of *all* current exceptions is returned to an acceptable status.

- When an exception occurs, the background color of each group that contains the exception changes to red, the color set for indicating there are exceptions.

  A group that contains exceptions remains red until *all* of its exceptions are returned to an acceptable status.

  Note: Within a group, the background color of each object that is an exception is the color set to indicate its specific unacceptable status, as described previously in the topics that follow “Determining the exact status of an object” on page 2-6. An exception remains the color of its unacceptable status until it is returned to an acceptable status.

Returning an exception to an acceptable status

After you locate an exception and check its unacceptable status, you can use any appropriate task to return the exception to an acceptable status. The target object of the task can be either:

- The exception from the Exceptions Work Area.
- The same exception from any group that contains it.

Locating the exception in the Exceptions Work Area likely is the quickest way to locate a target for the task.

Note: When activation is the task you intend to use to return an exception to an acceptable status, you should consider the activation profile assigned to the target object. Whenever an object is activated, it is activated according to the information in its assigned activation profile.

The exception in the Exceptions Work Area is automatically assigned the activation profile used in the most recent attempt to activate the object. To activate the exception with a different activation profile, you can either:

- Assign the exception in the Exceptions Work Area the activation profile you want to use.
- Locate an instance of the same exception, in any group that contains it, that is already assigned the activation profile you want to use.

For more information about activation and assigning activation profiles, see “Activating the CPC” on page 3-4 and “Assigning activation profiles to objects” on page 6-49, respectively.

Starting tasks

Use Views, the work area, and the tasks area to start tasks for monitoring and operating the system. Starting a task includes the following general steps:

1. Locating the task.
2. Locating and selecting the task's targets.
3. Starting the task on its targets.

Locating a task

Use Views, the work area, and the tasks area to locate system tasks. System tasks are divided into lists of related tasks. So to locate a particular system task, you must locate and open the task list that contains it. Opening a task list displays its tasks in the tasks area along the right side of the workplace.

To open a task list:

1. Open **Task List** from Views.
2. In the **Task List Work Area**, locate the list that contains the type of system task you want to start.
3. Double-click on the list to open it.

Begin with the task in the upper left corner of the area, and move left to right through each row of task lists. Consider this order a *ring*. To complete the ring, the last task list in the last row is followed by the first task list in the first row. After you become familiar with this order, you may prefer to open a task list by using the controls, referred to as *ring buttons*, located in the lower right corner of the tasks area.

To use ring buttons to open a task list:

- Click on the left ring button to open the next task list in the ring.
- Click on the right ring button to open the previous task list in the ring.

Locating task targets

Objects, which represent the physical and logical elements of the system, are typical targets of tasks. The console's objects include:

- Central processor complex (CPC)
- Central processors
- Channel paths
- Images

Groups of objects can also be the targets of some tasks. Starting a task on a group performs the task on each object in the group.

After locating the task, use Views and the work area to locate the groups or objects you want to use as the task's targets. Instructions for locating groups and objects are provided in previous topics; see the topics that follow “Locating groups and objects” on page 2-4.

Selecting task targets

After locating the groups or objects you want to use as the task's targets, you may have to select them to identify them as targets.

Selecting a single task target: If you intend to start a task on a single target, selecting the target is optional. Instead, you can start the task immediately after locating the target. For instructions, see “Starting a task on its targets” on page 2-12.

Selecting multiple task targets: Unlike starting a task on a single target, starting a task on multiple targets requires selecting the targets first. There are several ways to select multiple targets. You can use whatever way is easiest for you or most appropriate for the task.

To select each target individually:

1. Locate the objects or groups.

   For instructions, see the topics that follow “Locating groups and objects” on page 2-4.

2. Click on each object or group you want to select.

   The background color of their icons becomes gray to indicate they are selected.

Deselect a selected object or group, to undo its selection, if you do not want it to be a task's target. Click on a selected object or group to deselect it.

To select targets by swiping:

1. Locate the objects or groups.

   For instructions, see the topics that follow “Locating groups and objects” on page 2-4.

2. Click and hold the left mouse button on one of the objects or groups you want to select, then move the mouse pointer over each other object or group you want to select.

   The background color of their icons becomes gray to indicate they are selected.

3. Release the mouse button when you are finished making your selections.

Deselect a selected object or group, to undo its selection, if you do not want it to be a task's target. Click on a selected object or group to deselect it.

To box-select the targets:

1. Locate the objects or groups.

   For instructions, see the topics that follow “Locating groups and objects” on page 2-4.

2. Click and hold the left mouse button above and to the left of the leftmost, uppermost object or group you want to select.
3. Move the mouse pointer down and to the right to begin drawing a box from the selected point.
4. Move the mouse to draw the box over the other objects or groups you want to select.

   The background color of their icons becomes gray to indicate they are selected.

5. Release the mouse button when the box encloses all the objects or groups you want to select.

Deselect a selected object or group, to undo its selection, if you do not want it to be a task's target. Click on a selected object or group to deselect it.

To select all targets at once:

1. Locate the objects or groups.

For instructions, see the topics that follow “Locating groups and objects” on page 2-4.

2. Click on the system menu icon located in the upper left corner of the workplace.

   This opens the system menu for the workplace.

3. From the system menu, click on the **Select all** menu choice.

   The background color of their icons becomes gray to indicate they are selected.

Deselect a selected object or group, to undo its selection, if you do not want it to be a task's target. Click on a selected object or group to deselect it. Or you can use the system menu to deselect all selections at once.

To deselect all selections at once:

1. Click on the system menu icon located in the upper left corner of the workplace.
2. From the system menu, click on the **Deselect all** menu choice.

Starting a task on its targets

After locating a task, and locating and selecting its targets, you can start the task on the targets. There are several ways to start tasks. You can use whatever way is easiest for you or most appropriate for the task.

To start a task on a single target:

1. Locate the task.
2. Locate the target object or group.
3. Start the task on the target by any of the following:
   - Dragging and dropping the task on the target.
   - Dragging and dropping the target on the task.
   - Selecting the target and double-clicking on the task.
   - Selecting the target, selecting the task, and pressing **Enter**.

To start a task on multiple targets:

1. Locate the task.
2. Locate and select the target objects or groups.
3. Start the task on the targets by any of the following:
   - Dragging and dropping the task on any one of the selected targets.
   - Dragging and dropping any one of the selected targets on the task.
   - Double-clicking on the task.
   - Selecting the task, and pressing **Enter**.

Minimizing and restoring a task in progress

A task is considered to be in progress, and is referred to as *active*, until it is completed *and* its completion is acknowledged.

Completing a task typically requires using one or more windows and messages to provide information for performing the task or to acknowledge information about its intermediate and final outcomes. A window or message that requires you to provide or acknowledge information remains open until you do so. Ordinarily, the window or message also remains displayed. Some tasks provided for monitoring and operating the system allow you to temporarily set the task aside, while it is still active, by minimizing its open window or message. This is referred to as *minimizing an active task*.

Consider minimizing an active task whenever either:

- The console is busy processing the task and does not require your interaction or attention for several minutes.
- Or you want an unobstructed view of the workplace.

  For example, you may want to monitor its objects or areas for status changes.
- Or you want to use the workplace to do something else, but do not want to complete or cancel the task first.

  For example, you may want to use the console's 3270 emulator, check or change the console's settings, or open one of the console's online books.

To minimize an active task:

1. Click on the system menu icon of the active task's open window or message.

   Note: The system menu icon, if available, is located in the upper left corner of the window or message. If the system menu icon is not available, then the active task cannot be minimized while the current window or message remains open.
2. From the system menu, click on the **Minimize** menu choice.

   This minimizes the window or message, which minimizes the active task. The task is still active, and its current window or message remains open, but it is temporarily not displayed.

   Note: If the **Minimize** menu choice is not available, then the active task cannot be minimized while the current window or message is open.

After you minimize an active task, it will remain minimized until either:

- The console restores the task automatically when it completes processing the task, and displays a window or message with information about the task's final outcome.

  Close the window or message to acknowledge receiving the information and to end the completed task.
- Or you restore the task, at any time, to either complete it, cancel it, or check its progress.

  Use **Views** and the work area to restore a minimized active task.

To restore a minimized active task:

1. Open **Active Tasks** from **Views** area.

   Note: An empty **Active Tasks Work Area** indicates there are no minimized active tasks.

2. In the **Active Tasks Work Area**, locate the minimized active task you want to restore.

3. Double-click on the task to restore it.

   Restoring the task again displays its open window or message. Follow the instructions on the window for completing, cancelling, or continuing the task.

Restoring a minimized open window: The windows and messages displayed during active tasks remain open until you provide or acknowledge information as required to complete the tasks. But not all open windows indicate an active task.

For example, open windows that provide options for starting tasks, changing settings, or viewing information, are *not* considered active tasks. And while you can minimize an open window the same way you minimize an active task, minimized open windows will not be included in the **Active Tasks** view. Instead, you can locate and restore minimized open windows from the console's *window list*.

To restore a minimized open window:

1. Press **Ctrl+Esc**, or:

   a. Click on the system menu icon located in the upper left corner of the workplace.

   b. From the system menu, click on the **Window list** menu choice.

   In either case, this displays the **Window List** window. It lists the titles of all open windows.

2. Locate the title of the minimized open window you want to restore.

3. Double-click on the title to restore the open window.

   Restoring the open window again displays it. Follow the instructions on the window for using it or use its controls to close it.

Completing active tasks and closing open windows before logging off: You cannot log off the console while tasks are active or windows are open. The console will notify you if there are active tasks or open windows when you attempt to log off. You must complete or cancel each active task and close each open window before the console will allow you to log off:

- If an active task is minimized, restore it, then follow the instructions on an active task's open window or message to complete or cancel the task.

  Completing an active task may often be only a matter of acknowledging the completion of the task.

- If an open window is minimized, restore it, then use its controls to close it.

Setting lockout for disruptive tasks on an object

Some of the Support Element Console tasks are considered *disruptive*. Performing a disruptive task on a CPC or CPC image may disrupt its operation. For example, activating a CPC and loading an image are disruptive tasks. You may want to lock an object to prevent accidentally performing disruptive tasks on it and then unlock the object only when you want to perform a disruptive task on it.

Depending on whether the **Lockout disruptive task** setting is set to **Yes** or **No** determines if you can perform a disruptive task on a CPC or CPC image. You can either lock an individual object or a group of objects at one time.

Note: The **Lockout disruptive task** only affects operations from the Support Element Console workplace you are currently working at and its web browser. It does not affect most operations from the Support Element (for example, scheduled operations and CPC operations management commands, etc.), and operations initiated from other sources (for example, from Hardware Management Consoles).

To individually lock a CPC or CPC image:

1. Locate the objects you want want to lock in the Work Area.
2. Double click on the object's icon to open its Detail page.
3. Set the **Lockout disruptive tasks** radio button to **Yes**.
4. Select the **Save** push button to lock the object.

If you want to lock all CPCs or CPC images at one time:

1. Locate the objects you want to lock in the Work Area.
2. Click on the System Menu icon located in the upper left corner of the workplace to open the System menu.
3. Select **Lock all** from the menu. All objects currently in the work area are now locked.

When the object(s) are locked, a small red lock in the upper left hand corner of the icon indicates that the disruptive tasks are locked for that object. If you attempt to perform a disruptive task on a locked object, a window is displayed indicating the object is locked.

If you need to unlock an object or a group of objects, you must unlock each one individually. To do this:

1. Locate the object you want to unlock in the Work Area.
2. Double click on the object's icon to open its Detail page.
3. Set the **Lockout disruptive tasks** radio button to **No**.
4. Select the **Save** push button to unlock the object.
5. Repeat **steps 1 through 4** for every object you want to unlock.

Monitoring and operating the support element console: an overview

Use Views and the work area to start tasks for monitoring and operating the support element console. These tasks are referred to as *console actions* to distinguish them from tasks the console provides for monitoring and operating the system. Unlike the system tasks, the implied target, and only target, of a console action is the support element console itself.

To start a console action:

1. Open **Console Actions** from Views.

   This displays the console actions in the Console Actions Work Area.

2. In the Console Actions Work Area, locate the console action you want to start.
3. Double-click on the console action to start it.

   Starting the console action displays the windows and messages you must use to complete the console action.

See Chapter 15, “Operation of the console” on page 15-1 for specific descriptions of all console actions.

Opening an Online Book

Use Views and the work area to open online books provided with the Support Element Console Application. The books provide information about using the application and support element workplace. The books include:

Coupling Facility Control Code Commands
This publication is available exclusively as an online book. It provides information about commands you can issue from the support element workplace to coupling facility control code.

Coupling Facility Control Code Messages
This publication is available exclusively as an online book. It provides information about messages sent from coupling facility control code to the support element workplace.

Support Element Console Application Programming Interfaces
This online book is publication *Application Programming Interfaces*, SC28-8141. It provides information to customers in developing system management applications that will provide integrated S/390 hardware and software system management solutions using the application programming interfaces (APIs).

Support Element Operations Guide
This online book is publication *Support Element Operations Guide*, which is the publication you are currently using. It provides information about the Support Element Console Application and about using the support element workplace to monitor and operate your system.

System/390® Reference Summary
This online book is a subset of the reference summary. The reference summary is a quick summary reference to the Enterprise System Architecture/390.

To open an online book:

1. Open **Books** from **Views** area..
2. In the **Books Work Area**, locate the book you want to open. and double-click on the book icon. The book remains open until you close it.
3. When you are finished viewing the book, press **F3** to close it.

Getting Online Help

Provides both general and specific information. Any icon can be dragged and dropped on the Help icon for information, or the Help icon can be dragged and dropped on any of the icons in the Views, Tasks, or Work areas of the Support Element Console window.

Help will display the section of this online document that describes the object that the help icon was dropped on. Once that information is displayed, you may go to any other part of the document for other information.

To display **help** for an object or Support Element Console area:

1. Drag and drop the Help icon on the object or the area of the Support Element Console that you want help information for.

The **Help** window displays help information for the object or area of the Support Element Console where you dropped the help icon.

Help is also available for each window that is displayed by selecting the F1 key on the keyboard. Depending on the type of window, the help displayed will either be *field help* or the *general help*. If the window has one or more fields, the help displayed will be for the field where the cursor is located. To display the general help for the window, select **F2** while the field help is displayed. If the window does not have fields, the general help for the window is displayed when F1 was selected.

Most windows will also provide a Help push button which may be selected with the mouse.

Displaying hover help for workplace objects

Online help provides extensive, comprehensive information for the areas and objects on the support element workplace. As you become more familiar with workplace objects, and if you have less frequent need for the amount and depth of information provided by online help, consider using hover help instead. Hover help is a brief description of an object's, contents, usage, or purpose. The help is

displayed in a compact pop-up window that hovers above the object. The help is displayed in a compact pop-up window that hovers above the object. You can set hover help either *on* or *off,* depending on what you want. Initially, hover help is set off.

To set *hover help* on for your workplace:

- Click on the System Menu icon located in the upper left corner of the workplace to open the system menu.
- Click on the **Hover help** menu choice. This places a mark next to it and sets hover help on. If you want to set hover help off, click the menu choice again, the mark disappears, and hover help is set off.

Note: Hover help is not displayed immediately. The cursor must remain placed on a workplace object for several seconds to display the help.

You can work with the objects on the workplace using the mouse to select them. This is known as the *drag and drop technique*. This involves using the mouse to pick up one or more objects, dragging them to a task, and then dropping them. These techniques are examples of what is known as *direct manipulation* and are described in **"Using the Mouse" on page xiv.**

Opening the Workplace Pop-up Menu

This pop-up menu is a shortcut for navigating the workplace. The menu choices in the pop-up are the names of the views in the Views area. An arrow to the right of a menu choice indicates additional choices are available on a *cascaded menu.* A cascaded menu provides additional menu choices and may include additional cascaded menus. Each cascaded menu provides a more direct shortcut for locating and opening icons in a particular view.

To open the pop-up menu, click the right mouse button once on any empty area in the workplace. When the pop-up menu displays, select the view you want to see.

The pop-up menu provides shortcuts for:

- Locating groups and objects
- Opening a CPC or image details windows
- Locating exceptions
- Opening task lists
- Restoring minimized active tasks
- Starting console actions
- Opening online books

To open the workplace pop-up menu:

1. Right click on empty space in any area of the workplace.

Note: You must right click on an *empty* space to display the workplace pop-up menu. It will not be displayed if you right click on an icon or icon label.

Chapter 3. Daily operation of the system

This section describes the tasks from the **Daily** task list used most often on a daily basis for monitoring and operating the system.

The Daily task list is the task list displayed by default whenever you log on the support element console, making daily tasks immediately available for use. For each daily task, this section also provides:

- Information and instructions about preparing to use the task.
- Instructions for starting the task.

Starting the system

If you have experience using other systems, the steps you took to start the system and make it operational may have included:

1. Turning on system power
2. Performing a power-on reset of the system
3. Allocating system resources
4. Initializing logical partitions
5. Allocating logical partition resources
6. Loading a control program or operating system for the system or each logical partition. (This step may be referred to as an *initial microcode load (IML)* on other systems).

Furthermore, the steps you took may have depended on:

- The current operational status of the system.
- The operational capabilities and characteristics you wanted the system to have.

Using the support element workplace, starting the system and making it operational requires only to activate the system.

When you activate the system, you do not need to consider its current status to determine the steps you must take to make it operational. Activating the system, referred to also as *system activation*, automatically determines the system's current status and then performs the steps necessary to make it operational.

Successfully activating the system still requires you to define the operational capabilities and characteristics you want the system to have, but you can set up and save that information in advance, and assign it to the system. Then activating the system automatically uses the assigned information, rather than requiring you to provide it manually during the process.

Activation

Activation is a process that makes an object operational, where the *object* can be a central processor complex (CPC) or an image, and *operational* means either:

- The object is ready to have a control program or operating system loaded.
- The object has loaded and is running a control program or operating system.

Activation makes an object operational by:

- Using predefined information, referred to as an *activation profile*, to set the operational capabilities and characteristics of the object.
- Checking the current status of the object, and then performing only the operations necessary to make it operational.

So using activation is not limited to starting the system. Using activation is recommended *whenever you want to make the CPC or its images operational*.

A *complete activation* activates the CPC and its images completely and in a single step. The result of a complete activation is an operational CPC with images loaded and running operating systems. The current status of the CPC and its images determines which operations are performed during activation to make them operational. Activation may include:

1. Turning CPC power on.
2. Performing a power-on reset, which includes allocating system resources to the CPC.
3. Then either:
   - Loading a single image of the CPC with a control program or operating system.
   - Or activating logical partitions to support multiple images.

     Activating each logical partition includes:

     a. Initializing it.
     b. Allocating system resources to it.
     c. Loading it with a control program or operating system.

Since the status of the CPC and its images determines which operations must be performed during activation to make them operational, one or more operations listed above may *not* be performed during activation. For example:

- Activating the CPC does not perform a power-on reset if the CPC has already been power-on reset and the applicable settings in its assigned activation profile, such as the operating mode and active input/output configuration data set (IOCDS), are already in effect.
- Activating the CPC does not perform any operations if the CPC is already operational and all settings in its assigned activation profile are already in effect.

Notes:

1. To determine which operations were performed during an activation, view the support element's console events. See “Viewing console events” on page 15-1 for instructions.
2. Activation performs a power-on reset and a load only if necessary. If you want to perform a power-on reset or a load unconditionally, you can use tasks in the CPC Recovery task list. But it is recommended that these tasks be used only for error recovery. For more information, see Chapter 5, “Error recovery” on page 5-1.

Activation profiles

The predefined information used to activate an object is referred to as an *activation profile*. There are three types of activation profiles:

- A *reset profile* is used to activate a central processor complex (CPC) and its images.
- An *image profile* is used to activate an image of a CPC previously activated in logically partitioned (LPAR) mode.
- A *load profile* is used to load a previously activated image with a control program or operating system.

You will customize activation profiles to define the information that sets the operational capabilities and characteristics of the objects you want to activate.

Activating with a reset profile

To support your normal, day-to-day system operations, you will activate a central processor complex (CPC) with a reset profile. Activating a CPC with a properly customized reset profile includes initializing its images, if necessary, and can include loading the images. That is, a properly customized reset profile *includes* the load profile or image profiles necessary to perform a complete activation of a CPC and its images.

Activating with other profiles

After activating a central processor complex (CPC) with a reset profile, you can use the other types of activation profiles to establish a different or alternate operational capabilities and characteristics for the CPC's images, but without performing a complete activation of the CPC again. You can:

- Activate an image with a load profile to load a different control program or operating system.
- On a CPC operating in logically partitioned (LPAR) mode, activate an image with its image profile to activate it individually rather than by activating the CPC.

Getting ready for an activation

Preparation is essential to successfully activate a central processor complex (CPC) and its images. To successfully activate a CPC, you'll need:

- A properly customized reset profile assigned to the CPC and customized to meet your unique needs for operating the CPC.
- Access to resources referred to in the reset profile:
  - An input/output configuration data set (IOCDS) for defining the CPC's input/output (I/O) configuration.
  - Operating systems for loading images.

Preparing an activation profile

Customizing and assigning activation profiles are covered in detail later in this operations guide, beginning with the topic: “Getting ready to operate the system: customizing activation profiles” on page 6-1.

Preparing an IOCDS

You must build an IOCDS and it must be stored on a CPC's support element before you can activate the CPC.

An IOCDS is used during a power-on reset to define your I/O configuration to the channel subsystem of the CPC. The I/O configuration is the set of all I/O devices, control units, and channel paths available to the CPC.

You can build an IOCDS by using an input/output configuration program (IOCP):

- An IOCP may be available as a batch program with your operating system.

  For information about using the IOCP, see: *Input/Output Configuration Program User's Guide*, GC38-0401.

- A stand-alone IOCP also is available with the support element.

  For information about using the stand-alone IOCP, see: *Stand-Alone IOCP User's Guide*, GC38-0458.

Preparing to load images

To load an image during the activation of the CPC or logical partition that supports it, you must make an operating system or control program available for loading the image.

An operating system or control program is available for loading an image if it can be loaded by using I/O devices defined in the IOCDS used to activate the CPC. For example, with a properly defined I/O configuration, the operating system or control program could be:

- Read from a DASD.
- Read from a tape device to a DASD, then read from the DASD.
- Read from a tape device directly.

Note: Activating a coupling facility, which loads an image with coupling facility control code (CFCC), does not require using devices in the CPC's I/O configuration. The CFCC is loaded from the CPC's support element.

Activating the CPC

Use the support element workplace to start the task for activating the central processor complex (CPC).

To activate the CPC:

1. You must be logged on the support element in the operator, advanced operator, system programmer, or service representative user mode.
2. You must customize a reset profile and assign it to the CPC. See “Getting ready to operate the system: customizing activation profiles” on page 6-1.
3. The CPC must have access to the input/output configuration data set (IOCDS) and operating systems referred to in the reset profile. See “Getting ready for an activation” on page 3-3.

4. Open the **Task List** from the **Views** area.
5. Open **Daily** from the **Task List Work Area**.

   The Daily task list contains the **Activate** task that you will start.
6. Open **Groups** from the **Views** area.
7. Open the group that contains the CPC to which you assigned the reset profile.

   Note: Activating a CPC can be considered disruptive. If the CPC is locked, unlock it. See "Setting lockout for disruptive tasks on an object" on page 2-15.
8. Drag and drop the CPC on the **Activate** task to start it.
9. Review the information on the Activate Task Confirmation window to verify the object you will activate is the CPC, and the activation profile it will use is the one you want.
10. If the information is correct, select the **Yes** push button to perform the activation.

    The Activate Progress window indicates the progress of the activation, and the outcome.
11. Select **OK** to close the window when the activation completes successfully.

    Otherwise, if the activation does not complete successfully, follow the directions on the window to determine the problem and how to correct it.

After the CPC is activated, you can use the **Activate** task again, if necessary, to selectively activate its images.

Activating an image

Use the support element workplace to start the task for activating an image of the central processor complex (CPC).

An *image* is a set of CPC resources capable of running a control program or operating system. One or more images is created during a power-on reset of a CPC. When a power-on reset puts the CPC in logically partitioned (LPAR) mode, each logical partition is an image. Otherwise, when a power-on reset puts the CPC in a basic mode, the CPC has a single image.

To activate an image:

1. You must be logged on the support element in the operator, advanced operator, system programmer, or service representative user mode.
2. You must activate the CPC, and the activation must complete with at least a successful power-on reset of the CPC.
3. You must customize an activation profile and assign it to the image. See "Getting ready to operate the system: customizing activation profiles" on page 6-1.
4. The system must have access to the operating system referred to in the activation profile. See "Getting ready for an activation" on page 3-3.
5. Open the **Task List** from the **Views** area.

6. Open **Daily** from the **Task List Work Area**.

   The Daily task list contains the **Activate** task that you will start.

7. Open **Groups** from the **Views** area.

8. Open the group that contains the image to which you assigned the activation profile.

   Note: Activating an image can be considered disruptive. If the CPC image is locked, unlock it. See "Setting lockout for disruptive tasks on an object" on page 2-15.

9. Drag and drop the image on the **Activate** task to start it.

10. Review the information on the Activate Task Confirmation window to verify the object you will activate is the image, and the activation profile it will use is the one you want.

11. If the information is correct, select the **Yes** push button to perform the activation.

    This displays the Activate Progress window. The window indicates the progress of the activation, and the outcome.

12. Select **OK** to close the window when the activation completes successfully.

    Otherwise, if the activation does not complete successfully, follow the directions on the window to determine the problem and how to correct it.

Checking hardware messages from the CPC

The central processor complex (CPC) and Support Element Console Application send messages to the support element console to notify you of significant events that involve or affect the use of CPC hardware and licensed internal code. The messages are referred to as *hardware messages*.

Hardware messages may be sent to the support element console at any time. The support element console receives the messages automatically, stores them in a message log, and turns on several console indicators to help you recognize that hardware messages were received.

The support element console can store a maximum of five hundred messages in its hardware message log. If the message log becomes full, the support element console continues to receive and store new messages, but deletes the log's oldest message for each new message that is received. Promptly view, act on, and delete hardware messages to avoid filling the message log and losing messages.

Recognizing when hardware messages were received

While the Support Element Console Application is running, it changes the background color of one or more icons to indicate the support element console received a hardware message from the central processor complex (CPC).

The type and number of icons changed upon receiving a hardware message depends on whether anyone is logged on the console at the time:

- While logged on, the background color of the following icons changes when the support element console receives a hardware message:

  - The background color of the CPC changes to blue, the color set for indicating a hardware message was received.
  - The background color of each group that contains the CPC changes to blue.
  - The background color of the **Hardware Messages** task flashes blue. That is, its background color alternates between blue and the color of the tasks area. This is the task you will use to view the hardware messages.
- While logged off, the background color of the **Hardware Messages** icon on the logon window flashes blue when the support element console receives a hardware message. That is, its background color alternates between blue and the color of the logon window.

  Note: The logon window is titled Support Element Logon. The **Hardware Messages** icon is located in the Message indicators area of the window.

In addition to changing the background colors of icons, the support element console beeps once when it receives a hardware message, regardless of whether anyone is logged on or logged off the console at the time.

The **Hardware Messages** icon, both in the tasks area and on the logon window, continues to flash blue until you acknowledge receiving the new hardware messages by taking action on any one of them. The background color of the CPC and the groups that contain it remains blue until you take action on each new hardware message. Taking action on hardware messages begins with viewing them.

Viewing hardware messages

View hardware messages to remain informed of events that involve or affect the use of the central processor complex (CPC). Upon viewing hardware messages, you can also:

- Get more details for messages to determine what actions to take in response.
- Delete messages you no longer need.

To view hardware messages:

1. Locate the task in the task list on the right side of the workplace. Any task list contains the **Hardware Messages** task that you will start.
2. Open **Groups** from the **Views.** area.
3. Open the **CPC** group from the **Groups Work Area**.

   This opens the CPC Work Area. The area contains the target CPC.
4. Drag and drop the CPC on the **Hardware Messages** task to start it.

   This opens the Hardware Messages notebook. Its page lists the CPC's hardware messages, and it provides push buttons for working with them.

Note: After you open the notebook, use the online **Help** for more information on using it to view and delete hardware messages.

To get more details for messages:

1. Select each message for which you want more details, then select the **Details** push button.

This opens a *details* window, one at a time, for each selected message for which details are available.

2. Read the information and follow the directions on each details window to determine what action to take in response to a message. In many cases, you can use a details window itself to start the action.

Using the support element console as an operating system console

Console integration is a facility of the support element console. An operating system that supports console integration can be customized to allow using the support element console, if necessary, as an operating system console.

Under normal conditions, while other operating system consoles are available, the support element console should *not* be used as an operating system console. That is, the console integration facility is not intended to make the support element console the primary user interface to an operating system.

The console integration facility is intended instead to allow using the support element console as an operating system console only when other operating system consoles are not available. Other operating system consoles are not available, for example, during initialization of the operating system, or when they become unavailable due to outages or failures.

Refer to the publications provided with your operating system for more information about whether it supports console integration, and how to customize it to allow using the support element console as an operating system console.

Checking operating system messages from images

An *image* is a set of central processor complex (CPC) resources capable of running a control program or operating system. An operating system running in an image sends messages to operating system consoles to notify you of significant events that involve or affect the use of the operating system. The messages are referred to as *operating system messages*.

If an operating system running in an image supports console integration and is customized to allow using the support element console as an operating system console, then the support element console can also receive operating system messages.

An operating system may issue any number of messages at any time. The support element receives the messages automatically and stores them in a message log. The support element also turns on several console indicators to help you recognize that priority or held operating system messages were received. A *priority* or held operating system message either requires a response from the console operator or notifies the console operator of a critical condition that requires immediate attention.

The support element can store an average of approximately 200 (depending on the length of each message) messages in its operating system message log per image. If the message log becomes full, the support element continues to receive and store new messages, but deletes one or more of the log's oldest non-held, non-priority messages to make room for each new message. If there are not any non-held, non-priority messages, the oldest non-held priority, held, or priority message will be deleted.

Recognizing when priority or held operating system messages were received

While the Support Element Console Application is running, it changes the background color of one or more icons to indicate the support element received a priority or held operating system message from an image supported by the central processor complex (CPC).

The type and number of icons changed upon receiving a priority or held operating system message depends on whether anyone is logged on the console at the time:

- While logged on, the background colors of the following icons change when the support element receives a priority operating system message:
  - The background color of the image that supports the operating system changes to cyan, the color set for indicating priority or held operating system message was received.
  - The background color of each group that contains the image changes to cyan.
  - The background color of the **Operating System Messages** task flashes cyan. That is, its background color alternates between cyan and the color of the tasks area. This is the task you will use to view the operating system messages.
- While logged off, the background color of the **Operating System Messages** icon on the logon window flashes cyan when the support element receives a priority or held operating system message. That is, its background color alternates between cyan and the color of the logon window.

  Note: The logon window is titled Support Element Logon. The **Operating System Messages** icon is located in the Message indicators area of the window.

The **Operating System Messages** icon, both in the tasks area and on the logon window, continues to flash cyan until you acknowledge receiving the new priority or held operating system messages by viewing them. Likewise, the background colors of the image and the groups that contain it remain cyan until you acknowledge receiving the new priority or held operating system messages by viewing them. While viewing operating system messages, you have the option of responding to them.

Viewing operating system messages

View operating system messages to remain informed of events that involve or affect the use of images supported by the central processor complex (CPC). Upon viewing operating system messages, you can also:

- Send responses to messages.
- Delete messages you no longer need.

To view operating system messages:

1. Locate the task in the task list on the right side of the workplace. Any task list contains the **Operating System Messages** task that you will start.
2. Locate a target: either a group of images or individual images. Using a group of images will display operating system messages from all images in the group, while using individual images will display their messages only.

To locate a group of images:

a. Open **Groups** from the **Views** area.

b. Locate the **Images** group or any group that contains the images for which you want to view operating system messages.

To locate individual images:

a. Open the **Groups** view on the support element workplace.

b. Open the **Images** group from the **Groups Work Area**.

c. Select the individual images for which you want to view operating system messages.

3. Drag and drop the target group or selected images on the **Operating System Messages** task to start it.

   This opens the **Operating System Messages** notebook. Each page lists the operating system messages from each image in the target group or among the selected images. The notebook provides push buttons for responding to messages and for deleting them.

   Use the online **Help** for more information to view, respond to, or delete operating system messages.

   The color of each message indicates its type:

   Black Indicates an informational message that normally does not require a response from the console operator.

   Blue Indicates a held message that requires a response from the console operator.

   Red Indicates a priority message about a critical condition that requires immediate attention.

Responding to an operating system message requires receiving an operating system message first. You can use **Operating System Messages** also to send commands to an operating system, regardless of whether you've received messages from it.

Sending commands to operating systems

You can use a support element console to send commands, at any time, to operating systems running in images supported by the central processor complex (CPC).

To send commands to an operating system:

1. Locate the task in the task list on the right side of the workplace. Any task list contains the **Operating System Messages** task that you will start.
2. Locate a target: either a group of images or individual images. Using a group of images will allow sending commands to each operating system running on images in the group, while using individual images will allow sending commands to their operating systems only.

   To locate a group of images:

   a. Open the **Groups** view on the support element workplace.

b. Locate the **Images** group or any group that contains the images for which you want to send commands to their operating systems.

To locate individual images:

a. Open the **Groups** from the **Views** area.

b. Open the **Images** group from the **Groups Work Area**.

c. Select the individual target images that you want to send commands to their operating systems.

3. Drag and drop the target group or selected images on the **Operating System Messages** task to start it.

   This opens the Operating System Messages notebook. Each page lists the operating system messages, if any, from each image in the target group or among the selected images. The notebook provides a **Send command** push button for sending commands to the operating systems running on the images.

   Use the online **Help** for more information to send commands to an operating system.

   Note: The **Send command** push button is not available if the operating system running on an image does not support receiving commands from the support element console.

Monitoring system activity

Successfully activating the system makes it capable of doing work. The operating systems and applications running on the system determine its workload. Over any period of time, and depending on its workload, the system will spend some of the time doing work and the rest of the time waiting to do work. That is, the system will be either busy or idle, respectively. *System activity* is a measurement of how busy the system is over a period of time. Since system activity is likely to vary over consecutive periods of time, you need to see those consecutive variations in activity to get an accurate idea of how busy the system is.

Your system is the central processor complex (CPC) and the physical and logical resources it uses to do work. The CPC's support element provides a function, referred to as *system activity analysis*, for monitoring system activity by monitoring the activity, or *usage*, of a subset of the CPC's physical and logical resources:

- Central processors (CPs)
- System assist processors (SAPs)
- Channels
- Logical partitions and logical processors

  Note: Logical partitions and logical processors are resources only while the CPC is activated in logically partitioned (LPAR) mode.

But monitoring system activity does not require monitoring the usage of all CPC resources at once. Instead, you can use a *system activity profile* to define the particular resources you want to monitor. Furthermore, for each resource you choose to monitor, you can use the system activity profile to:

- Set conditions for which you want the resource's usage reported or ignored.
- Indicate how you want the resource's usage presented.

A properly customized system activity profile is essential for monitoring meaningful activity and having it presented in an understandable format. After describing system activity analysis in more detail in the next topic, the remaining topics in this section will describe system activity profiles and how to work with them. Then the final topics will describe how to start system activity analysis, and provide some tips about using it.

System activity analysis

System activity analysis is a function of the Support Element Console Application that:

- Monitors and quantifies the activity of a subset of physical and logical resources, or *system resources*, used by the central processor complex (CPC).

  Quantified activity is referred to here as an *activity summary*.
- Uses graphics to present activity summaries of monitored resources.
- Regularly and automatically updates activity summaries with current information.

The system resources monitored during system activity analysis, and how their activity summaries are presented, are determined by the information in a system activity profile.

System activity profiles

A *system activity profile* is a set of information that defines:

- The system resources you want to monitor during system activity analysis.
- How you want activity summaries of the monitored resources presented.

More specifically, the information in a system activity profile:

- Identifies the central processors (CPs), system assist processors (SAPs), logical partitions, logical processors, and channels for which you want to monitor activity.
- Focuses the measurement of processor activity on specific program status word (PSW) keys or on a specific operating state, if applicable.
- Sets *thresholds* for processor and channel activity, to emphasize activity that does not meet a minimum amount of expected use, or exceeds a maximum amount of expected use.
- Indicates the amount and arrangement of information presented in activity summaries, and how often to update the activity summaries with new information from the system resources being monitored.

A set of sample system activity profiles is provided by IBM with the Support Element Console Application. Consider using the sample system activity profiles for system activity analysis until you become familiar with their contents and purpose. Then you can use the sample profiles as templates for customizing your own system activity profiles.

Sample system activity profiles

A set of sample system activity profiles is provided by IBM with the Support Element Console Application. You can use the sample profiles to monitor your system activity. You can use them also as templates for creating new profiles.

The following table shows the name of each sample system activity profile, describes its intended use, and identifies the system activities it is set to display during system activity analysis.

Table 3-1 (Page 1 of 2). Sample system activity profiles

DEFAULT	This profile is useful for monitoring the activity of all physical processors and the busiest channels. It is customized for displaying the individual and average activity of all central processors (CPs), the individual and average activity of all system assist processors (SAPs), and the activity of the 31 most active channels.
CHANHIGH	This profile is useful for monitoring the activity of the busiest channels. It is customized for displaying the activity of the 49 most active channels.
CHANLOW	This profile is useful for monitoring the activity of the least busy channels. It is customized for displaying the activity of the 49 least active channels.
LPARSUMA	This profile is useful for monitoring the activity of up to 10 logical partitions and physical processors. It is customized for displaying the individual activity of all logical partitions, the individual and average activity of all CPs, and the individual and average activity of all SAPs. **Note:** Some systems support activating 15 logical partitions. You can customize this profile, or a copy of it, to display activity for up to 15 logical partitions.
LPARSUMB	This profile is useful for monitoring the activity of up to 10 logical partitions, all physical processors, and the busiest channels. It is customized for displaying the individual activity of all logical partitions, the average activity of all CPs, and the activity of the 37 most active channels. **Note:** Some systems support activating 15 logical partitions. You can customize this profile, or a copy of it, to display activity for up to 15 logical partitions.
PROCESSOR	This profile is useful for monitoring the activity of all physical processors. It is customized for displaying the individual and average activity of all CPs, and the individual and average activity of all SAPs.
PROCLIST	This profile is useful for monitoring the activity of all physical processors and the busiest channels. It is customized for displaying the individual and average activity of all CPs, the individual and average activity of all SAPs, and the activity of the 31 most active channels.
PROCUSAGEBYKEY	This profile is useful for situations, like tuning applications, that require monitoring CP activity while the program status word (PSW) key is set to a specific value. It is customized for displaying the average activity of all CPs while the PSW key is X'0', the average activity of all CPs while the PSW key is X'1', the average activity of all CPs while the PSW key is X'2', and so on for each of the possible values of the PSW key: X'0' through X'F'. The profile is customized also for displaying the average activity of all CPs, regardless of the value of the PSW key.

Table 3-1 (Page 2 of 2). Sample system activity profiles	
VMPROCESSOR	This profile is useful for monitoring the activity of all physical processors while using an operating system, like some versions of VM, that may put CPs in an active wait state. It is customized for displaying the individual and average activity of all CPs (excluding activity in active wait states), and the individual and average activity of all SAPs. For more information, see “Effect of an active wait state on processing activity” on page 3-16.
VMPROCLIST	This profile is useful for monitoring the activity of all physical processors and the busiest channels while using an operating system, like some versions of VM, that may put CPs in an active wait state. It is customized for displaying the individual and average activity of all CPs (excluding activity in active wait states), the individual and average activity of all SAPs, and the activity of the 31 most active channels. For more information, see “Effect of an active wait state on processing activity” on page 3-16.

You can use any sample system activity profiles immediately to start system activity analysis if the profiles suit your needs for monitoring system activity. For instructions, see “Starting system activity analysis.”

Otherwise, if you want to monitor other types of system activity, or if you simply want to see the exact information in a system activity profile, you can use the support element workplace to work with system activity profiles as needed.

Starting system activity analysis

Start system activity analysis of the central processor complex (CPC) from its support element console to monitor the CPC's system activity. System activity analysis monitors system resources and displays activity summaries according to the information in the system activity profiles you choose upon starting it. You can start system activity analysis either with a single profile or with multiple profiles:

- Start analysis with a single profile to monitor one subset of system resources. Only its activity summaries are displayed during the analysis.
- Start analysis with multiple profiles, up to 16 profiles, to monitor multiple subsets of system resources at once. Each subset's activity summaries are displayed, one subset at a time, in a continuous sequence during the analysis. This is referred to as *rolling* system activity analysis.

To start system activity analysis:

1. You must be logged on the support element in the operator, advanced operator, system programmer, or service representative user mode.
2. Open a list of system activity profiles, using either:
   - The same task you use to work with system activity profiles. For instructions, see “Opening a list of system activity profiles” on page 6-62.
   - Or the task provided on the support element workplace specifically for monitoring system activity. See the following instructions.

   To start the specific workplace task for monitoring system activity:

a. Open the **Task List** from the **Views** area.

b. Open **Daily** from the **Task List Work Area**.

   The Daily task list contains the **Activity** task that you will start.

c. Open **Groups** from the **Views** area.

d. Open the **CPC** group from the **Groups Work Area**.

3. Drag and drop the CPC on the **Activity** task to start it.

   Using either task opens the Customize System Activity Profiles List notebook. Its page lists the CPC's system activity profiles, and it provides a push button for starting system activity analysis.

4. Select from the list the system activity profiles you want to use to monitor system activity, then select the **Start system activity** push button.

   If you selected one system activity profile, this starts system activity analysis.

   Otherwise, if you selected more than one profile, this displays the Rolling System Activity Parameters window. Use the window, as follows, to set rates for displaying and updating the multiple profiles' activity summaries during system activity analysis:

   a. In the Roll rate field, type the amount of time for how long you want to display the activity summaries from one profile, before replacing it with the activity summaries from the next profile in the sequence.

   b. In the Refresh rate field, type the amount of time for how often you want activity summaries, while displayed, to be updated with new data from the system.

   c. Select **OK** to set the rates and start system activity analysis.

   In either case, starting system activity analysis displays the System Activity window. The window uses labels to identify the types of activity being monitored, and graphics to indicate the amounts of activity as percentages, from 0% to 100%.

   Use the online **Help** for more information on using the window to monitor system activity.

   Notes:

   a. Open the window's legend for more information about the labels and graphics used to identify and indicate activity:

      1) Select **Actions** from the window's menu bar to display the menu.

      2) Select **Show legend** from the menu to display the window's legend.

   b. To monitor the true processing activity while using an operating system that uses an active wait state, like some versions of VM, start system activity analysis with a system activity profile customized to exclude processing activity during an active wait state. For more information, see “Effect of an active wait state on processing activity” on page 3-16.

   c. Although the System Activity window's range for displaying activity graphically is 0% to 100%, the processing activity of logical partitions that share processors may exceed 100%. For more information, see “Processing activity for logical partitions using shared processors” on page 3-16.

d. You can use the System Activity window to view a detailed snapshot of a shared channel's usage by each logical partition that shares it. For more information, see “Channel activity for logical partitions using shared channels” on page 3-17.

Effect of an active wait state on processing activity

By using an active wait state, an operating system does not yield idle processing resources to the system. This affects how you should monitor processing activity for such systems.

During system activity analysis of all processing activity, central processors (CPs) in an active wait state are considered busy rather than idle. Since the CPs are either actually busy, or in an active wait state that is considered busy, activity summaries of such CPs always indicate 100% usage.

To monitor the true processing activity, you can customize a system activity profile for monitoring processing activity that excludes a CP's activity while it is in an active wait state. Two of the sample system activity profiles, named VMPROCESSOR and VMPROCLIST, are examples of such profiles. They are customized, as follows, for monitoring processing activity while using a VM operating system that uses an active wait state:

- Processing activity includes the individual and average activity of all CPs.
- But excludes CP activity in the supervisor state while the program status word (PSW) key is X'3'. These conditions are true while a CP is in an active wait state.

Refer to the documentation provided with your operating system to determine whether it uses an active wait state, and if so, to determine also the processor state and PSW key value of a CP while it is in an active wait state.

Processing activity for logical partitions using shared processors

A logical partition is assigned logical processors by the activation profile used to activate it. The activation profile also determines whether the logical processors are supported by dedicated processing resources:

- Logical partitions activated *with* dedicated processing resources have exclusive use of a central processor (CP) for each of its assigned logical processors.
- Logical partitions activated *without* dedicated processing resources share the use of non-dedicated CPs. A logical partition's processing weight and its setting for whether the processing weight is capped, which are both set by the activation profile also, determine the logical partition's share of non-dedicated processing resources.

Note: For instructions for locating this information in an activation profile, see “Assigning logical processors” on page 6-27.

If a logical partition's processing weight is not capped, its processing weight is the *minimum* share of non-dedicated processing resources guaranteed to the logical partition when all non-dedicated processing resources are in use. But when non-dedicated processing resources are available, the logical partition can borrow them, if necessary, in excess of the share ordinarily provided by its processing weight.

During system activity analysis, the processing activity of a logical partition that shares non-dedicated processing resources is *normalized*. Normalized processing activity is 100% while the logical partition is using the full share of processing resources provided by its processing weight. If a logical partition's processing weight is not capped, its processing activity *exceeds* 100% whenever the logical partition uses non-dedicated processing resources in excess of the share provided by its processing weight.

During system activity analysis, the System Activity window uses labels to identify the types of activity being monitored, and graphics to indicate the amounts of activity as percentages. Since the window's range for displaying activity graphically is 0% to 100%, actual amounts of normalized processing activity that exceed 100% are not displayed graphically. Instead, labels and graphics are altered, as follows, to identify and indicate normalized processing activity that exceeds 100%:

- The label is altered to displayed the actual percentage of normalized processing activity.
- The graphics are colored differently while normalized processing activity exceeds 100%.
- If the processing activity being monitored includes activity in both the problem state and the supervisor state, the graphics indicate the *ratio* of activity in each state, rather than the actual percentage of activity in each state, while the total normalized processing activity exceeds 100%.

  For example, if the total normalized processing activity is 200%, and the graphics indicate 60% activity in the problem state and 40% activity in the supervisor state, then the actual activity in the problem state is 120% (60% of 200%), and the actual activity in the supervisor state is 80% (40% of 200%).

Note: Open the legend for the System Activity window for more information about the labels and graphics used to identify and indicate processing activity that exceeds 100%:

1. Select **Actions** from the window's menu bar.
2. Select **Show legend** from the menu to display the window's legend.

Channel activity for logical partitions using shared channels

A shared channel can be online or configured online to more than one logical partition at the same time. An input/output configuration data set (IOCDS) defines whether a channel is shared, and which logical partitions can share it. The activation profile used to activate a central processor complex (CPC) in logically partitioned (LPAR) mode determines which IOCDS is used the define the input/output (I/O) configurations of the CPC's logical partitions.

During system activity analysis, the label for a channel activity summary includes an **S** to indicate the channel is shared. The graphics for a shared channel activity summary displays in two portions:

- The first portion of the activity summary displays channel usage by one logical partition: either a specific logical partition or the logical partition for which the channel usage is highest.

  Note: The system activity profile used to start system activity analysis determines which logical partition has its individual channel usage displayed.

- The second portion of the activity summary displays the combined channel usage by all other logical partitions that share it.

While monitoring shared channel activity, you can use the System Activity window to view a detailed snapshot of a shared channel's usage by each logical partition that shares it.

1. Locate the label and graphics that identify and indicate activity on the shared channel.
2. Double-click with mouse button 1 on the shared channel's graphics.

   This displays the System Activity EMIF Details window. It displays a pie chart graphic that shows the channel usage by each logical partition that shares it, and the channel's unused capacity, if any.

   Note: System activity analysis is suspended while you view the details of a shared channel's usage. As such, the window displays a snapshot of the shared channel's usage at the time you requested it. The snapshot will not be refreshed with new information.
3. Select **OK** to close the window and resume system activity analysis.
4. Repeat these steps to view another detailed snapshot of the shared channel's usage, if needed.

Resetting the system or logical partitions

A *reset normal* initializes a system or logical partition by:

- Clearing its pending interruptions.
- Resetting its channel subsystem.
- Resetting its processors.

If you have experience using other systems, a reset normal may have been referred to as a *system-reset-normal*.

A reset normal prepares a system or logical partition for loading it with an operating system. On the support element workplace, *images* support operating systems, so images are your targets for resets. Recall that an image represents either:

- A central processor complex (CPC) activated in basic mode.
- A logical partition, while the CPC is activated in logically partitioned (LPAR) mode.

A reset normal is one of several *recovery tasks* that you can use to attempt to recover from hardware or software errors. A reset normal is often effective but less disruptive than other tasks, which typically makes it the first task attempted to recover from errors when they occur. But follow your local error recovery procedures for determining when to perform a reset normal.

To perform a reset normal:

1. You must be logged on the support element in the operator, advanced operator, system programmer, or service representative user mode.
2. Open the **Task List** from the **Views** area.
3. Open **Daily** from the **Task List Work Area**.

   The Daily task list contains the **Reset Normal** task that you will start.
4. Open **Groups** from the **Views** area.
5. Open the **Images** group, or any group that contains the image.

   Note: Performing a reset normal on an image can be considered disruptive. If the CPC image is locked, unlock it. See "Setting lockout for disruptive tasks on an object" on page 2-15.
6. Drag and drop the image on the **Reset Normal** task to start it.
7. Review the information on the confirmation window to verify the image you will reset.
8. If the information is correct, select the **Perform reset** push button to perform the reset normal.
9. Select **OK** to close the progress window when the reset completes successfully.

   Otherwise, if the reset does not complete successfully, follow the directions on the window, or on any messages that may display, to determine the problem and how to correct it.

Note: For more information about all recovery tasks, including reset normal, see Chapter 5, "Error recovery" on page 5-1.

Chapter 4. Logging Off, Shutting Down, and Powering Off

When you log off the support element console, you close the support element console workplace only. The support element may automatically or manually require you to shut down and reboot the system to update changes you have made. You may need to deactivate the CPC prior to shutting down or rebooting the system to avoid possible data loss.

Logging off the support element

You can use any one of the following to log off the support element console:

- Press **Alt+F4**.
- Use **Log off** from the system menu:
  1. Click on the system menu icon located in the upper left corner of the workplace to open the system menu.
  2. From the system menu, click on the **Log off** menu choice.
- Use the **Log off** console action:
  1. Double-click on **Console Actions** in the Views area to open the **Console Actions Work Area**.
  2. From the work area, double-click on the **Log off** console action.
- Use the **Log off** button in the upper right corner of the workplace.
  1. Locate the sizing controls in the upper right corner of the workplace.
  2. Double-click the **Log off** button which is the second button from the left.

The **Support Element Logon** window is displayed when you log off.

Deactivating the CPC

Deactivation is an orderly process for shutting down and turning off the system.

Deactivating the system includes:

- Ending hardware and software activity.
- Clearing, releasing, and deallocating hardware resources.

You can use the support element workplace to start the task for deactivating the central processor complex (CPC).

Note: Deactivating the CPC ends hardware and software activity by clearing, releasing, and deallocating hardware resources. The system will be put into a “non-operating” state and power remains in the “operating” state.

The target, or *object*, of a deactivation can be a CPC or an image. While the CPC is operating in basic mode, in which it supports a single image, you can use either the CPC or its image as the deactivation target. In either case, the CPC is deactivated.

While the CPC operates in logically partitioned (LPAR) mode, in which one or more logical partitions support multiple images, you can use only the CPC as the deactivation target to deactivate the CPC.

Note: For more information about deactivating individual logical partitions, see “Deactivating an image” on page 4-3.

To deactivate the CPC:

1. You must be logged on the support element in the operator, advanced operator, system programmer, or service representative user mode.
2. Quiesce all operating systems supported by the CPC's images.

   Use the operating system console for the operating system to quiesce it. Refer to the publications provided with an operating system for information about quiescing it.

   Important: If you do not quiesce all operating systems before deactivating the CPC, operating system activity will be abruptly ended during deactivation, resulting in a possible loss of data.
3. Open the **Task List** from the **Views.** area.
4. Open **Daily** from the **Task List Work Area**.

   The Daily task list contains the **Deactivate** task that you will start.
5. Open **Groups** from the **Views.** area.
6. Open a group that contains the CPC.

   Note: Deactivating a CPC can be considered disruptive. If the CPC is locked, unlock it. See “Setting lockout for disruptive tasks on an object” on page 2-15.
7. Drag and drop the CPC on the **Deactivate** task to start it.
8. Review the information on the Deactivate Task Confirmation window to verify the object you will deactivate is the CPC.
9. If the information is correct, select the **Yes** push button to perform the deactivation.

   The Deactivate Progress window indicates the progress of the deactivation, and the outcome.
10. Select **OK** to close the window when the deactivation completes successfully.

    Otherwise, if the deactivation does not complete successfully, follow the directions on the window to determine the problem and how to correct it.

After the CPC is deactivated, it and its images are no longer operational.

Deactivating an image

You can use the support element workplace to start the task for deactivating an image of the central processor complex (CPC).

An *image* is a set of CPC resources capable of running a control program or operating system. One or more images is created during a power-on reset of a CPC. When a power-on reset puts the CPC in logically partitioned (LPAR) mode, each logical partition is an image. Otherwise, when a power-on reset puts the CPC in a basic mode, the CPC has a single image.

While the CPC is operating in basic mode, in which it supports a single image, deactivating its image has the outcome as deactivating the CPC. In either case, the CPC is deactivated.

But while the CPC operates in LPAR mode, in which one or more logical partitions support multiple images, you can use one or more images as deactivation targets to deactivate individual logical partitions.

To deactivate an image:

1. You must be logged on the support element in the operator, advanced operator, system programmer, or service representative user mode.
2. Open the **Task List** from the **Views** area.
3. Open **Daily** from the **Task List Work Area**.

   The Daily task list contains the **Deactivate** task that you will start.
4. Open **Groups** from the **Views** area.
5. Open the group that contains the image you want to deactivate.

   Note: Deactivating an image can be considered disruptive. If the CPC image is locked, unlock it. See “Setting lockout for disruptive tasks on an object” on page 2-15.
6. Drag and drop the image on the **Deactivate** task to start it.
7. Review the information on the Deactivate Task Confirmation window to verify the object you will deactivate is the image.
8. If the information is correct, select the **Yes** push button to perform the deactivation.

   The Deactivate Progress window indicates the progress of the deactivation, and the outcome.
9. Select **OK** to close the window when the deactivation completes successfully.

   Otherwise, if the deactivation does not complete successfully, follow the directions on the window to determine the problem and how to correct it.

After the image is deactivated, the logical partition it supported is no longer operational. The CPC and images previously activated to support other logical partitions remain operational.

Shutting down, rebooting, and powering off

Shutting down and rebooting of support element ends hardware and software activity. The system will be put into a non-operating state. Changing some support element tasks require a system reboot either automatically or manually. The following are some of the support element tasks that require a system reboot.

1. Tasks that automatically reboot the system
   - Change support element name
   - Disruptive patch
   - EC upgrade
2. Tasks requiring manual reboot
   - Domain security password
   - Enable console services
   - Support element settings

Unsecured desktop

If you are logged on the support element with an unsecured desktop and you need to shut down and reboot the system to update changes or power-off the system, you need to:

1. Ensure that all support element application tasks have completed or have been terminated.
2. Open **Console Actions** from the **Views** area.
3. Select **Log Off** from the **Console Actions Work Area**.
4. Select the **Shutdown Console** push button on the Support Element Console Logon window. The Shutdown Console window is displayed.
5. Select the **Yes** push button.
6. Wait at least 90 seconds for all support element hard disk activity to complete.
7. Minimize all windows displayed by clicking on their minimize icons (in the upper right corner of the windows).
8. Click once with the right mouse button on any empty place of the Desktop.
9. Select **Shut down** from the system menu.
10. Select **OK** on any confirmation window displayed.
11. If you receive a ROP Kernel pop-up window, select the **Yes** push button.
12. When a message indicates that shut down is complete, either power off the support element console display and system unit or press **Ctrl**+**Alt**+**Del** to reboot the system.

Secured desktop

If you are logged on the support element with secured desktop and you need to shut down and reboot the system to update changes or power off the system, you need to:

1. Open the **Task List** from the **Views** area.
2. Open **CPC Recovery** from the **Task List Work Area**.

   The CPC Recovery task list contains the **Shut Down** task that you will start.

3. Open **Groups** from the **Views** area.
4. Open a group that contains the CPC.
5. Drag and drop the CPC on the **Shut Down** task to start it.
6. The Shut Down Task Confirmation window displays.

   To shut down and reboot the system:

   - Select **Yes**

   To power-off the system:

   - Select **Yes**. The System is rebooting message displays.
   - Before the blue OS/2 Warp screen displays, turn the red power switch to Off.

If you are logged off the support element and select the Shutdown Console push button on the support element logon window, a window displays to prompt you to logon and select the Shut Down task from CPC Recovery to shut down and reboot.

Chapter 5. Error recovery

This section describes the tasks typically needed to attempt to recover from hardware or software errors.

The CPC Recovery task list contains the tasks, referred to here as *recovery tasks*. The recovery tasks, from least to most disruptive, are:

- Processor operations: stop all and start all
- Resets: normal and clear
- Load
- Power-on reset

If you have experience using other systems, you may find that some recovery tasks are the same as or similar to tasks you have used not only for error recovery on similar systems, but also for starting the system under normal circumstances. But using the support element workplace, you should *activate* the system instead of using recovery tasks for starting the system under normal circumstances. Activating the system, referred to also as *system activation*, automatically determines its status and then performs all of the tasks necessary to make it operational. For more information about activation, see “Starting the system” on page 3-1.

Use recovery tasks only while following your local procedures for error recovery. This section provides instructions for starting the tasks.

Processor operations: start all and stop all

Start all and *stop all* are processor operations you can use, together, to control whether processors can process instructions. If you have experience using other systems, you may have used START and STOP commands or Start and Stop keys to start and stop processors.

On the support element workplace, *images* are supported by physical processors or logical processors. Recall that an image represents either:

- A central processor complex (CPC) activated in basic mode.
- A logical partition, while the CPC is activated in logically partitioned (LPAR) mode.

By using start and stop on *all* processors that support an image, you can control the processing activity of the image, and thereby control the activity of the software running on the image:

- Stop all processors for an image to suspend its processing activity. This effectively suspends the activity of the software running on the image.
- Start all previously stopped processors for an image to resume its processing activity. The activity of the software running on the image also is resumed.

Follow your local error recovery procedures for determining when to stop all processors, what to do afterwards, and when to start all processors again.

Note: If your local error recovery procedures direct you to work with individual processors, use tasks in the CP Toolbox task list. See the topics that follow Chapter 12, “Processor and storage operations” on page 12-1, for more information about tasks for working with individual processors:

- Processor operations: stop and start
- Changing a processor's operation rate.
- Using display/alter.
- Performing a PSW restart.
- Setting conditions for stopping a processor.
- Tracing processor activity.
- Interrupting processor activity.
- Using store status.

Stopping all processors

Follow your local error recovery procedures for determining when to stop all processors. But generally, stopping all processors for an image is effective only when the image and its processors are operating.

To stop all processors for an image:

1. You must be logged on the support element in the advanced operator, system programmer, or service representative user mode.
2. Open the **Task List** from the **Views** area.
3. Open **CPC Recovery** from the **Task List Work Area**.

   The CPC Recovery task list contains the **Stop All** task that you will perform.
4. Open **Groups** from the **Views** area.
5. Open the **Images** group, or any group that contains the image.

   This opens the group's work area. The area contains the target image.

   Note: Stopping an image can be considered disruptive. If the CPC image is locked, unlock it. See “Setting lockout for disruptive tasks on an object” on page 2-15.
6. Drag and drop the image on the **Stop All** task to stop all processors for the image.

   This immediately performs the operation; all processors for the image are stopped.

Starting all processors

Follow your local error recovery procedures for determining when to start all processors. But generally, starting all processors for an image is most effective after you've used the **Stop All** task to stop all processors for the image.

To start all processors for an image:

1. You must be logged on the support element in the advanced operator, system programmer, or service representative user mode.
2. Open the **Task List** from the **Views** area.
3. Open **CPC Recovery** from the **Task List Work Area**.

   The CPC Recovery task list contains the **Start All** task that you will perform.
4. Open **Groups** from the **Views** area.
5. Open the **Images** group, or any group that contains the image.

   This opens the group's work area. The area contains the target image.

   Note: Starting an image can be considered disruptive. If the CPC image is locked, unlock it. See “Setting lockout for disruptive tasks on an object” on page 2-15.
6. Drag and drop the image on the **Start All** task to start all processors for the image.

   This immediately performs the operation; all processors for the image are started and resume operating.

Resets: normal and clear

A reset initializes a system or logical partition by:

- Clearing its pending interruptions.
- Resetting its channel subsystem.
- Resetting its processors.

Such a reset is referred to as a *reset normal*; if you have experience using other systems, a reset normal may have been referred to as a *system-reset-normal*. Like a reset normal, a *reset clear* clears interruptions, resets channels, and reset processors for a system or logical partition, but a reset clear also clears main storage for the system or logical partition. If you have experience using other systems, a reset clear may have been referred to as a *system-reset-clear*.

A reset prepares a system or logical partition for loading it with an operating system. On the support element workplace, *images* support operating systems, so images are your targets for resets. Recall that an image represents either:

- A central processor complex (CPC) activated in basic mode.
- A logical partition, while the CPC is activated in logically partitioned (LPAR) mode.

Follow your local error recovery procedures for determining when to perform a reset normal or reset clear.

Reset normal

To perform a reset normal:

1. First you must be logged on the support element in the advanced operator, system programmer, or service representative user mode.
2. Open the **Task List** from the **View** area.
3. Open **CPC Recovery** from the **Task List Work Area**.

   The CPC Recovery task list contains the **Reset Normal** task that you will start.
4. Open **Groups** from the **Views** area.
5. Open the **Images** group, or any group that contains the image.

   Note: Performing a reset normal on an image can be considered disruptive. If the CPC image is locked, unlock it. See “Setting lockout for disruptive tasks on an object” on page 2-15.
6. Drag and drop the image on the **Reset Normal** task to start it.
7. Review the information on the confirmation window to verify the image you will reset.
8. If the information is correct, select **Yes** to perform the reset normal.

   The progress window indicates the progress of the reset, and the outcome.
9. Select **OK** to close the window when the reset completes successfully.

   Otherwise, if the reset does not complete successfully, follow the directions on the window, or on any messages that may display, to determine the problem and how to correct it.

Reset clear

To perform a reset clear:

1. First you must be logged on the support element in the advanced operator, system programmer, or service representative user mode.
2. Open the **Task List** from the **Views** area.
3. Open **CPC Recovery** in the **Task List Work Area**.

   The CPC Recovery task list contains the **Reset Clear** task that you will start.
4. Open **Groups** from the **Views** area.
5. Open the **Images** group, or any group that contains the image.

Note: Performing a reset clear on an image can be considered disruptive. If the CPC image is locked, unlock it. See “Setting lockout for disruptive tasks on an object” on page 2-15.

6. Drag and drop the image on the **Reset Clear** task to start it.
7. Review the information on the confirmation window to verify the image you will reset.
8. If the information is correct, select **Yes** to perform the reset clear.

   The progress window indicates the progress of the reset, and the outcome.
9. Select **OK** to close the window when the reset completes successfully.

   Otherwise, if the reset does not complete successfully, follow the directions on the window, or on any messages that may display, to determine the problem and how to correct it.

Load

A load resets a system or logical partition, to prepare it for loading an operating system, and then loads the operating system. If you have experience using other systems, a load may have been referred to as an *initial program load* or *IPL*.

On the support element workplace, *images* support operating systems, so images are your targets for loads. Recall that an image represents either:

- A central processor complex (CPC) activated in basic mode.
- A logical partition, while the CPC is activated in logically partitioned (LPAR) mode.

Follow your local error recovery procedures for determining when to perform a load.

To perform a load:

1. You must be logged on the support element in the advanced operator, system programmer, or service representative user mode.
2. Open the **Task List** from the **Views** area.
3. Open **CPC Recovery** from the **Task List Work Area**.

   The CPC Recovery task list contains the **Load** task that you will start.
4. Open **Groups** from the **Views** area.
5. Open the **Images** group, or any group that contains the image.

   Note: Loading an image is considered disruptive. If the CPC image is locked, unlock it. See “Setting lockout for disruptive tasks on an object” on page 2-15.
6. Drag and drop the image on the **Load** task to start it.
7. On the Load window:

   a. Use its controls to identify the operating system you want to load, and to indicate how you want to perform the load.

Note: Move the cursor to any control, use the online **Help** for more information about using the control. Press **F2** to request help for the window.

b. Select **OK** to perform the load using the information you provided.

This displays a confirmation window.

8. Review the information on the confirmation window to verify the image you will load and the information you provided for performing the load. If the information is correct, select the **Yes** push button to perform the load.

   The progress window indicates the progress of the load, and the outcome.

9. Select **OK** to close the window when the load completes successfully.

   Otherwise, if the load does not complete successfully, follow the directions on the window, or on any messages that may display, to determine the problem and how to correct it.

Power-on reset

A power-on reset initializes a system by:

- Initializing all processors.
- Initializing the channel subsystem.
- Allocating storage.
- Loading the hardware system area (HSA) with licensed internal code.
- Establishing the operating mode: either basic mode or logically partitioned (LPAR) mode.
- Defining the input/output (I/O) configuration to the channel subsystem.

If you have experience using other systems, a power-on reset may have been referred to as an *initial microcode load* or *IML*.

On the support element workplace, the central processor complex (CPC) is the system, so the CPC is your target for a power-on reset.

Follow your local error recovery procedures for determining when to perform a power-on reset.

To perform a power-on reset:

1. You must be logged on the support element in the advanced operator, system programmer, or service representative user mode.
2. You must have an input/output configuration data set (IOCDS) available on your support element which defines the I/O configuration for the CPC.
3. Open the **Task List** from the **Views** area.
4. Open **CPC Recovery** from the **Task List Work Area**.

The CPC Recovery task list contains the **Power-on reset** task that you will start.

5. Open **Groups** from the **Views** area.
6. Open the **CPC** group, or any group that contains the CPC.

   Note: Performing a power-on reset to a CPC is considered disruptive. If the CPC is locked, unlock it. See "Setting lockout for disruptive tasks on an object" on page 2-15.
7. Drag and drop the CPC on the **Power-on reset** task to start it.

   The Power-On reset notebook pages provide controls for customizing the information used to perform a power-on reset of the CPC.
8. Use the controls on each page to customize the power-on reset information as needed:
   a. Use the General page to select an operating mode and IOCDS for the CPC.
   b. Use the Storage page to set the storage configuration to establish for the CPC and to set the cache size of its internal disk subsystem, if installed.
   c. Use the Dynamic page to establish the hardware support required to use dynamic input/output (I/O) configuration.
   d. Use the Options page to set the operating environment and enable or disable the power save feature for the CPC.

   Note: Move the cursor to any control on any page, use the Online **Help** for more information about using the control. Press **F2** to request help for the page.
9. Select **Perform power-on reset** to perform the power-on reset using the information you provided in the notebook.
10. Select the **Power-on reset** push button to perform the power-on reset.

    The progress window indicates the progress of the power-on reset, and the outcome.
11. Select **OK** to close the window when the power-on reset completes successfully.

    Otherwise, if the power-on reset does not complete successfully, follow the directions on the window, or on any messages that may display, to determine the problem and how to correct it.

Loading software from a CD-ROM or FTP server

This task allows you to load system software or utility programs from a CD-ROM or from an FTP server.

To load software from a CD-ROM or FTP server:

1. You must be logged on the support element in the system programmer or service representative user mode.
2. Open the **Task List** from the **Views.** area.
3. Open **CPC Recovery** from the **Task List Work Area**.

The CPC Recovery task list contains the **Load from CD-ROM or Server** task that you will start.

4. Open **Groups** from the **Views** area.
5. Open the images groups or any group that contains the image.
6. Drag and drop the image on the **Load from CD-ROM or Server** task to start it.

   The Load from CD-ROM or Server Task Confirmation window displays.
7. Select **Yes** to continue.

   The Load from CD-ROM or Server window displays.
8. Select the source of the software that you want to load from.

   If you select the FTP Source, you must enter the FTP Host computer, your User ID, and your password.

   Note: If you are loading software from an FTP server, an optional account number and file location may be necessary.
9. Select **Continue**

   The Load from CD-ROM or Server - Select the software to load window displays.
10. Select the file or program that you want to load.
11. Select **Continue** to complete the task.

    The progress window indicates the duration and elapsed time of the program loaded.
12. Select **OK** to close the window when the task completes successfully.

Chapter 6. Settings for system operations

This section describes tasks you can use to customize settings that control how the system operates. Some settings affect system operations directly, while other settings are input for other tasks you use to monitor and operate the system.

The **CPC Operational Customization** task list contains the tasks, referred to here as *operational customization tasks*. This section provides instructions for starting the tasks.

Getting ready to operate the system: customizing activation profiles

Customize activation profiles to define the information that sets the operational capabilities and characteristics of the objects you want to activate. There are three types of activation profiles:

- A *reset profile* is used to activate a central processor complex (CPC) and its images.
- An *image profile* is used to activate an image of a CPC previously activated in logically partitioned (LPAR) mode.
- A *load profile* is used to load a previously activated image with a control program or operating system.

Default activation profiles

A set of default activation profiles is provided by IBM with the Support Element Console Application. There is one default profile of each type:

Type	Default profile name
Reset	DEFAULT
Image	DEFAULT
Load	DEFAULTLOAD

The default profiles are not meant to be used to activate your central processor complex (CPC) or its images; the information in them may not be correct for your configuration or needs. Instead, customize the default profiles to meet your needs. Or customize the default profiles to meet your general needs, then use them as templates for creating new profiles that meet your specific needs.

Using the right profiles

You can perform a complete activation of a central processor complex (CPC) and its images by using a properly customized reset profile:

- When a reset profile is customized for activating the CPC in basic mode, in which it supports a single image, the reset profile includes the load profile necessary to load the CPC's image. That is, you can customize the reset and load profiles at once for performing a complete activation of the CPC and its image:
  - Customize the reset profile for activating the CPC in basic mode.

  - Customize the load profile included in it for loading the image during CPC activation.
- When a reset profile is customized for activating the CPC in logically partitioned (LPAR) mode, in which logical partitions support multiple images, the reset profile includes the image profiles necessary to activate and load the images. That is, you can customize reset and image profiles at once for performing a complete activation of the CPC and its images:
  - Customize the reset profile for activating the CPC in LPAR mode.
  - Customize the image profiles included in it for activating and loading one or more images during CPC activation.

In summary:

- You must customize reset profiles for activating the CPC.
- Then while you are customizing a reset profile, you have the option of customizing the load profile or image profiles included in it.
- To use a reset profile to perform a complete activation of the CPC and its images, you must properly customize the load profile or image profiles included in it.

Other options for using profiles

While you are customizing a reset profile, you have the option of customizing the load profile or image profiles included in it. You can also customize load profiles and image profiles individually. In either case, after you use a reset profile to activate the central processor complex (CPC), you can use individual load profiles or image profiles as follows:

- After activating the CPC in basic mode, you can use a load profile to load its image with an operating system.

  Activating the image with a load profile, rather than activating the CPC again with a reset profile, allows loading the image while maintaining the rest of the CPC's current operational capabilities and characteristics. You can load an image this way whether you are loading it for the first time, or loading it again but with a different operating system.
- After activating the CPC in logically partitioned (LPAR) mode, you can use an image profile to activate a logical partition.

  Activating the logical partition with its image profile, rather than activating the CPC again with a reset profile, allows activating only the logical partition, while maintaining current operational capabilities and characteristics of the CPC and other logical partitions. You can activate an image this way whether you are activating it for the first time, or activating it again.
- After activating a logical partition, you can use a load profile to load its image with an operating system.

  Activating the image with a load profile, rather than activating the logical partition again with an image profile, allows loading the image, while maintaining the rest of the logical partition's current operational capabilities and characteristics. You can load an image this way regardless of whether you are loading it for the first time, or loading it again but with a different operating system.

Customizing unique profiles

Customize unique activation profiles for each different way you want to activate the central processor complex (CPC) and its images. You can customize unique activation profiles by giving them unique names. That is, all reset profiles, load profiles, and image profiles you create must have unique names.

Recall that a reset profile includes either a load profile or one or more image profiles. A reset profile includes a load profile or image profile by referencing its unique profile name. While you are customizing a reset profile, you have the option of customizing the load profile or image profiles included in it. You can also customize load profiles and image profiles individually. But regardless of whether you customize them within reset profiles or individually, load profiles and image profiles remain unique.

- **Example 1:** a reset profile named LPARMODE includes image profiles named LP01 and LP02.

  While customizing the LP01 image profile individually, any changes you make also affects the LPARMODE reset profile. While customizing the LP01 image profile included in the LPARMODE reset profile, any changes you make also changes the individual LP01 image profile.

  While customizing the LP02 image profile individually any changes you make also affects the LPARMODE reset profile. While customizing the LP02 image profile included in the LPARMODE reset profile, any changes you make also changes the individual LP02 image profile.

- **Example 2:** a reset profile named FIRSTSHIFT includes a load profile named ESALOAD, and a reset profile named NIGHTSHIFT also includes the load profile named ESALOAD.

  While customizing the ESALOAD load profile individually, any changes you make also affects the FIRSTSHIFT and NIGHTSHIFT reset profiles.

  While customizing the ESALOAD load profile included in either reset profile, any changes you make changes the individual ESALOAD load profile and affects the other reset profile.

Developing an activation strategy

Until you become familiar with the different types of activation profiles and their purposes, you should concentrate on customizing reset profiles, and the load profiles or image profiles included in them, for performing a complete activation of the central processor complex (CPC) and its images. After you become more familiar with activation profiles, developing an activation strategy may help you determine the types of activation profiles you should customize and use to meet your needs.

To fully exploit the advantages of using activation to start your CPC, IBM recommends customizing activation profiles for activating the CPC and its images completely and in a single step. IBM recommends this strategy for establishing the CPC's normal, day-to-day operational capabilities and characteristics because it saves time and requires minimal action by the operator.

But you should develop your own activation strategies to meet your needs. The strategies you develop determine the types of activation profiles you must customize and use.

Complete activation

A *complete activation* activates the central processor complex (CPC) and its images completely and in a single step. The result of a complete activation is an operational CPC with images loaded and running operating systems.

A properly customized reset profile includes the load profile or image profiles necessary to perform a complete activation of the CPC and its images. Using a properly customized reset profile for performing a complete activation is the recommended activation strategy for establishing the CPC's normal, day-to-day operational capabilities and characteristics.

Information and instructions for customizing reset profiles are provided in the topics that follow “Profiles for complete activation.”

Staged activation

A *staged activation* activates the central processor complex (CPC) and its images in steps:

- An initial activation of the CPC and one or more images.
- And any number of subsequent, selective activations of images.

Staged activations are useful for changing the operational capabilities and characteristics of the CPC's images, but without performing a complete activation of the CPC. They allow meeting different processing needs at different times of day or on different days of the week. For example, you may want to use one logical partition as a production system during first shift, and use other logical partitions as batch and test systems on second shift.

You could perform a complete activation of the CPC each time you want to change the operational capabilities and characteristics of its images. But you can get the same results by planning and performing staged activations instead. Staged activations will not require performing a complete activation of the CPC each time you want to change its operational capabilities and characteristics of its images. Instead, you can activate the CPC once, and then activate only its images when you want to change their operational capabilities and characteristics.

A reset profile is required for performing the initial activation of a staged activation. Afterwards, you can use image profiles to selectively activate logical partitions, and load profiles to selectively load images.

Information and instructions for customizing reset profiles, image profiles, and load profiles are provided in the topics that follow “Profiles for staged activations” on page 6-41.

Profiles for complete activation

You can perform a complete activation of a central processor complex (CPC) and its images by using a reset profile.

A complete activation means customizing a reset profile to either:

- Activate the CPC in basic mode and load it with an operating system.

  See “Tips for activating CPCs” on page 6-8 and “Tips for loading operating systems” on page 6-37.

- Or activate the CPC in logically partitioned (LPAR) mode, activate one or more logical partitions, and load them with operating systems.

  See “Tips for activating CPCs” on page 6-8, “Tips for activating logical partitions” on page 6-22, and “Tips for loading operating systems” on page 6-37.

Reset profiles

Customize a reset profile for activating a central processor complex (CPC) and its images.

Opening a reset profile: You can use the support element workplace to start the task for customizing reset profiles for a central processor complex (CPC). Starting a task is referred to also as *opening a reset profile*.

To open a reset profile:

1. You must be logged on the support element in the system programmer user mode, and a reset profile must be assigned as the CPC's activation profile.
2. Open the **Task List** from the **Views** area.
3. Open **CPC Operational Customization** from the **Task List Work Area**.

   The CPC Operational Customization task list contains the **Customize/Delete Activation Profiles** task that you will start.
4. Open **Groups** from the **Views** area.
5. Open the **CPC** group from the **Groups Work Area**.
6. Drag and drop the CPC on the **Customize/Delete Activation Profiles** task to start it.

   When the profile list of profiles is initially displayed, the highlighted profile is the currently assigned profile.
7. Select from the list the name of the reset profile you want to customize.
8. Select the **Customize** push button.

   This opens the selected reset profile. Its information appears on the pages of the notebook.

   After you start the task, select a page and move the cursor to any control, use the online **Help** for more information about the control. Press **F2** to request help for the page.

Checking the CPC's assigned activation profile: You can assign a central processor complex (CPC) either a reset profile or a load profile as its activation profile. Whenever the CPC is activated, it is activated according to the information in its assigned activation profile.

To check and change a CPC's assigned activation profile:

1. Open **Groups** from the **Views** area.
2. Open the **CPC** group from the **Groups Work Area**.

3. Double-click on the CPC.

   This opens a CPC details window of information about the CPC.

4. Select the **Change options** push button.

5. Locate the **Profile name** field from the Change Object Options window.

   It displays the name of the profile currently assigned as the CPC's activation profile.

6. To assign a different profile, locate the desired profile name in the list of profiles field and select it.

   To assign the CPC a reset profile instead, use the window to select and save a reset profile.

Navigating a reset profile notebook: A reset profile includes information for activating a central processor complex (CPC) and its images.

Opening a reset profile displays its information on windows that are organized as pages in a notebook.

If the reset profile activates the CPC with multiple images, which is the case when it activates the CPC in logically partitioned (LPAR) mode, there are page tabs along the right side of the notebook. Each page tab begins a distinct section of the reset profile. The information in each section is used to activate a single object, either the CPC or a logical partition. The name on each page tab identifies the object activated by the information.

If the reset profile activates the CPC with a single image, which is the case when it activates the CPC in a basic mode, there are *no* page tabs along the right side of the notebook. There is only one section of information.

In either case, the pages within a section are identified by page tabs along the bottom of the notebook. The label on each page tab is a general description of the information on the page.

To use page tabs to turn notebook pages directly:

- To turn to a different section of the profile, click on its page tab along the right side of the notebook.
- To turn to a different page within a section, click on its page tab along the bottom of the notebook.

Each page of the notebook also includes paging buttons, a left-pointing button and a right-pointing button, in its lower right corner.

To use paging buttons to turn notebook pages sequentially:

- To turn to the previous page in the notebook, click on the left-pointing button.
- To turn to the next page in the notebook, click on the right-pointing button.

Creating a new reset profile: You are responsible for creating reset profiles that meet your unique needs.

You can use the default reset profile as a template for creating new profiles. After you create a new profile, you can customize it as needed. After you create and

customize your own reset profiles, you can use them as templates for creating more new profiles. You can also modify the default reset profile and use the modified default reset profile as a template.

To create a new reset profile:

1. Open a reset profile.

   For more information, see “Opening a reset profile” on page 6-5.

2. Select the General page.

   The **Profile name** field identifies the reset profile you opened. It will be used as a template for the new reset profile.

3. To use a different reset profile as a template:

4. Select the list button beside the **Profile name** field.

   This opens a list of the names of all the CPC's reset profiles. The reset profile named DEFAULT is the default reset profile provided by IBM.

5. Select from the list the name of the reset profile you want to use as a template.

   This opens the selected reset profile. Its information replaces the previous profile's information on the pages of the notebook.

6. To create a new profile from the template, type a unique name for the new profile in the **Profile name** field.

7. Select the **Save** push button to save the profile with the new name.

   Note: Saving the new profile does not change the reset profile you used as a template.

Assigning a reset profile: After you open a reset profile, you can assign it to the central processor complex (CPC) as its activation profile. Whenever the CPC is activated, it is activated according to the information in its assigned activation profile.

To assign an open reset profile as a CPC's activation profile:

1. After opening and customizing a reset profile, select the General page.

   The **Profile name** field identifies the reset profile that will be assigned to the CPC.

2. Select the **Assign profile** push button to assign the reset profile as the CPC's activation profile.

Saving a reset profile: You must save a reset profile to save the information you customized on its pages.

To save an open reset profile:

1. After opening and customizing a reset profile, select the General page.

   The **Profile name** field identifies the reset profile that will be saved.

2. Select the **Save** push button to save the reset profile and close it.

Tips for activating CPCs

The topics in this section provide tips for customizing a reset profile for activating a central processor complex (CPC).

Supporting basic mode operation: The reset profile you use to activate a central processor complex (CPC) can establish the support required to operate the CPC in basic mode. The reset profile must identify:

- An input/output configuration data set (IOCDS) that supports basic mode.
- A basic mode as the operating mode you want to establish.

An IOCDS is used during a power-on reset to define your input/output (I/O) configuration to the channel subsystem of the CPC. The I/O configuration is the set of all I/O devices, control units, and channel paths available to the CPC.

Performing a power-on reset also establishes the operating mode of the CPC. The operating mode determines whether the CPC can support a single image or multiple images:

- *Logically partitioned (LPAR) mode* supports multiple images.
- All other operating modes, referred to as *basic modes*, support single images.

  ESA/390™ and ESA/390 TPF are examples of basic modes.

To customize a reset profile to support operating the CPC in basic mode:

1. Open a reset profile.

   For more information, see “Opening a reset profile” on page 6-5.
2. Select the General page.

   Move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the General page.
3. Select from the **Input/Output Configuration Data Set** list an IOCDS that supports basic mode.

   Note: The **Type** list column indicates the operating mode supported by each IOCDS. The column displays **ESA/390** to indicate an IOCDS supports basic mode.
4. Select either **ESA/390** or **ESA/390 TPF** from the want to establish.

Supporting LPAR mode operation: The reset profile you use to activate a central processor complex (CPC) can establish the support required to operate the CPC in logically partitioned (LPAR) mode. The reset profile must identify:

- An input/output configuration data set (IOCDS) that supports LPAR mode and the logical partitions you want to activate.
- LPAR mode as the operating mode you want to establish.

An IOCDS is used during a power-on reset to define your input/output (I/O) configuration to the channel subsystem of the CPC. The I/O configuration is the set of all I/O devices, control units, and channel paths available to the CPC.

Performing a power-on reset also establishes the operating mode of the CPC. The operating mode determines whether the CPC can support a single image or multiple images:

- *LPAR mode* supports multiple images.
- All other operating modes, referred to as *basic modes*, support single images.

  ESA/390 and ESA/390 TPF are examples of basic modes.

To customize a reset profile to support operating the CPC in LPAR mode:

1. Open a reset profile.

   For more information, see “Opening a reset profile” on page 6-5.
2. Select the General page.

   Move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the General page.
3. Select from the **Input/Output Configuration Data Set** list an IOCDS that supports LPAR mode and defines the logical partitions you want to activate.

   Notes:

   a. The **Type** list column indicates the operating mode supported by each IOCDS. The column displays **Partition** to indicate an IOCDS supports LPAR mode.

   b. The **Partitions** list column displays the names of logical partitions supported by the IOCDS.
4. Select **Logically partitioned** from the **Mode** list to identify LPAR mode as the operating mode you want to establish.

Selecting an IOCDS: The reset profile you use to activate a central processor complex (CPC) can identify the input/output configuration data set (IOCDS) you want to use. The IOCDS must be compatible with the operating mode you want to establish. That is, the IOCDS you select must support the type of operating mode you select.

An IOCDS is used during a power-on reset to define your input/output (I/O) configuration to the channel subsystem of the CPC. The I/O configuration is the set of all I/O devices, control units, and channel paths available to the CPC.

Performing a power-on reset also establishes the operating mode of the CPC. The operating mode determines whether the CPC can support a single image or multiple images:

- *Logically partitioned (LPAR) mode* supports multiple images.
- All other operating modes, referred to as *basic modes*, support single images.

  ESA/390 and ESA/390 TPF are examples of basic modes.

You can customize the reset profile to use either a specific IOCDS or the active IOCDS (if you intend to use dynamic I/O configuration, for example). Follow the instructions below for using a specific IOCDS; see “Using the active IOCDS” on page 6-10 for more information about using the active IOCDS.

To customize a reset profile to select an IOCDS and operating mode:

1. Open a reset profile.

   For more information, see “Opening a reset profile” on page 6-5.
2. Select the General page.

Move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the General page.

3. Select an IOCDS from the **Input/Output Configuration Data Set** list.
4. Select an operating mode from the **Mode** list that is compatible with the IOCDS you selected.

   Note the type of operating mode supported by the IOCDS you selected. The **Type** list column indicates the operating mode supported by each IOCDS:

IOCDS type	Operating mode
ESA/390	ESA/390 or ESA/390 TPF
Partition	Logically partitioned
Currently *ID*	The operating mode of the IOCDS is not known because the reset profile will use the active IOCDS when activation is performed; the *ID* identifies the current active IOCDS. Select an operating mode from the **Mode** list that is compatible with the IOCDS you *intend* to make active. For more information, see "Using the active IOCDS."

Using the active IOCDS: The reset profile you use to activate a central processor complex (CPC) can be customized for using the active IOCDS rather than a specific IOCDS. The *active IOCDS* is the IOCDS used for the most recent power-on reset. But if you use dynamic I/O configuration, you can change the active IOCDS at any time without performing a power-on reset.

You should customize a reset profile to use the active IOCDS if you intend to use dynamic input/output (I/O) configuration. And at least one of the images activated on the CPC must be loaded with an operating system that supports an application or facility for using dynamic I/O configuration. Dynamic I/O configuration is supported by:

- The Hardware Configuration Definition (HCD) application on some MVS and OS/390® operating systems.
- The dynamic I/O configuration facility of some VM operating systems.

To customize an activation profile to use the active IOCDS:

1. Open a reset profile.

   For more information, see "Opening a reset profile" on page 6-5.
2. Select the General page.

   Move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the General page.
3. Select **Use active IOCDS** from the **Input/Output Configuration Data Set** list.

   When activation is performed using this reset profile:

   - The last active IOCDS is used if the CPC is not operational.
   - The active IOCDS is used if the CPC is already operational *and* if a power-on reset must be performed to make at least one other profile setting take effect. For more information, see "How using the active IOCDS affects CPC activation" on page 6-11.

4. Note the identifier of the IOCDS that is currently active. See **Currently** *ID* displayed in the **Type** list column for the **Use active IOCDS** selection. The *ID* is the IOCDS identifier.

   With dynamic I/O configuration, you can change the active IOCDS anytime prior to using this reset profile to activate the CPC.

5. Select an operating mode from the **Mode** list that is compatible with the IOCDS you've made active or *intend* to make active.

   To determine the type of operating mode supported by the IOCDS, locate it in the **Input/Output Configuration Data Set** list. The **Type** list column indicates the operating mode supported by the IOCDS.

IOCDS type	Operating mode
ESA/390	ESA/390 or ESA/390 TPF
Partition	Logically partitioned

How using the active IOCDS affects CPC activation: When a reset profile is used to activate the central processor complex (CPC), several profile settings take effect when a power-on reset is performed during activation. Such settings are referred to here as *power-on reset settings* and include, for example, the CPC's storage allocations. If the CPC is already operational and the reset profile's power-on reset settings are already in effect when activation is performed using the profile, then a power-on reset is not performed during activation. That is, a power-on reset is performed during CPC activation only if it is necessary to make one or more of the reset profile's power-on reset settings take effect.

The input/output configuration data set (IOCDS) setting is one of the reset profile's power-on reset settings, *unless* it is set to **Use active IOCDS**. Activating the CPC with a reset profile customized for using the active IOCDS affects CPC activation as follows:

- If the CPC is not operational, then a power-on reset is performed and the last active IOCDS is used.
- If the CPC is already operational, then:
  - A power-on reset is performed and the active IOCDS is used only if one or more of the reset profile's other power-on reset settings are not already in effect. For example, a power-on reset is performed if the CPC's current storage allocations are not the same as the storage allocations set in the reset profile.
  - A power-on reset is *not* performed and the active IOCDS is ignored if all of the reset profile's other power-on reset settings are already in effect.

    This may be the case when you use dynamic input/output (I/O) configuration. Using dynamic I/O to change the active IOCDS will not affect whether a power-on reset is performed during CPC activation. Only changing the reset profile's other power-on reset settings will cause a power-on reset to be performed.

Delaying the load while devices power-on: The reset profile you use to activate a central processor complex (CPC) can set a load delay for power sequencing.

Activating a CPC includes initializing its images, and can include loading the

images. The operating systems are loaded from devices in the input/output (I/O) configuration of the CPC.

If the devices are attached to control units that are powered-on by the CPC during activation, operating systems cannot be loaded from the devices until powering-on their control units is complete.

If you know or can estimate the amount of time it takes for control units to be powered-on, you can delay starting the load for that amount of time, up to 100 minutes. The delay may allow the powering-on to complete before the load begins.

To customize a reset profile to delay the load while control units power-on:

1. Open a reset profile.

   For more information, see “Opening a reset profile” on page 6-5.

2. Select the General page.

   Move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the General page.

3. Type the amount of time to delay the load, from 0 to 59 seconds or 1 to 100 minutes, in the **Load delay for power sequencing** fields.

Allocating storage: The reset profile you use to activate a central processor complex (CPC) can allocate its storage.

The storage available to a CPC can be allocated as central storage, expanded storage, or cache size for the CPCs internal disk subsystem, if installed. *Central storage* includes main storage, the hardware system area (HSA). *Expanded storage* is a buffer some operating systems can use for high-speed paging to and from main storage. For LPAR mode, customize storage in each of the logical partitions, see “Allocating storage” on page 6-36.

To customize a reset profile to allocate central and expanded storage for a CPC when in basic mode:

1. Open a reset profile.

   For more information, see “Opening a reset profile” on page 6-5.

2. Select the Storage page.

3. Use the storage spin buttons in the Installed Storage Details group box to allocate central and expanded storage at the same time.

   Notes:

   a. Move the cursor to either spin button, then use the Online **Help** for information about it. While viewing the help, press **F2** to request help for the Storage page.

   b. Using either spin button changes the central storage and expanded storage amounts at the same time; increasing central storage decreases expanded storage, and vice versa.

   c. The minimum central storage is 64 MB. You cannot allocate less than that amount.

d. Not all operating systems can use expanded storage. Allocate 0 MB of expanded storage if the operating system you intend to load cannot use expanded storage.

e. The central and expanded button will not display if you are in LPAR mode.

4. To allocate part of the available storage for the CPC's internal disk subsystem, if installed:

   Use the **Requested cache size** spin button in the Internal Disk Subsystem Details group box to set the amount of central storage to use for the internal subsystem cache.

   Notes:

   a. Move the cursor to the spin button, then use the Online **Help** for more information about it. While viewing the help, press **F2** to request help for the Storage page.

   b. Increasing the amount of central storage used for the CPC's internal disk subsystem decreases the amount of main storage that remains available for its operating systems. After setting the cache size for the internal disk subsystem, check the amount displayed in the **Main storage (available for operating systems)** field to determine how much main storage remains available. Use the **Central storage** spin button again, if necessary, to allocate more central storage and thereby increase the amount available as main storage.

   c. For more information about the internal disk subsystem, see “The Internal Disk Subsystem Feature” on page 10-5.

Supporting dynamic I/O configuration: The reset profile you use to activate a central processor complex (CPC) can establish the hardware support required to use dynamic input/output (I/O) configuration.

Your I/O configuration is the set of all I/O devices, control units, and channel paths you define to your hardware and software.

Performing a power-on reset establishes the *hardware I/O definition*. That is, it defines the I/O configuration to the hardware. Loading the software establishes the *software I/O definition*. That is, it defines the I/O configuration to the software.

Ordinarily, changing the hardware I/O definition requires performing another power-on reset, and changing the software I/O definition requires loading the software again. But if the hardware and software support *dynamic I/O configuration*, you can *dynamically change* their I/O definitions. Changes made dynamically, referred to as *dynamic I/O changes*, take effect immediately. Yet they do *not* require a power-on reset or load to make them take effect.

Hardware support for dynamic I/O: Your hardware is the CPC. Dynamic I/O configuration, or simply *dynamic I/O*, is a facility of the CPC's licensed internal code. The hardware support required for using dynamic I/O can be established during power-on reset of the CPC:

- The IOCDS used during power-on reset must support dynamic I/O. The IOCDS must be either:
  - Built using the Hardware Configuration Definition (HCD) application of an MVS or OS/390 operating system that supports dynamic I/O.

  - Written using the DYN option of the input/output configuration program (IOCP) utility of a VM operating system that supports dynamic I/O.

- Dynamic I/O must be enabled for the CPC. That is, the CPC must allow dynamically changing its I/O definition.

  Note: Only a power-on reset of the CPC, performed directly or during CPC activation, can initially enable dynamic I/O. Afterwards, you can use the support element workplace at any time, if necessary, to change the dynamic I/O setting. For more information, see “Enabling or disabling dynamic I/O without performing a power-on reset” on page 6-15.

- In logically partitioned (LPAR) mode, dynamic I/O must be enabled for a logical partition.
- The CPC's hardware system area (HSA) must be expanded to allow dynamic I/O changes to increase the size of the I/O definition.

To customize a reset profile for hardware support of dynamic I/O:

1. Open a reset profile.

   For more information, see “Opening a reset profile” on page 6-5.

2. Select the General page.

   Move the cursor to any control and use the online **Help** for more information about it. Press **F2** to request help for the General page.

3. Select an IOCDS that supports dynamic I/O from the **Input/Output Configuration Data Set** list.

   Note: The **Allow Dynamic I/O** list column displays **Yes** to indicate an IOCDS supports dynamic I/O.

4. Select the Dynamic page.

   Move the cursor to any control and use the online **Help** for more information about it. Press **F2** to request help for the Dynamic page.

5. Mark the **Allow dynamic changes to the channel subsystem input/output (I/O) definition** check box.

   The check box displays a check mark when you mark it. The check mark indicates you want to enable dynamic I/O for the CPC.

6. In the **Percent of input/output configuration (IOCDS) expansion allowed** field, type a percentage of additional space, from 1 to 999 percent of the space allocated for the initial I/O definition, to reserve in the CPC's HSA for increasing the size of the I/O definition.

   Notes:

   a. You do not need to know the storage amount allocated for the initial I/O definition, only the number of devices in it. The percent increase in devices you plan to add is approximately the same as the percent increase in the size of the I/O definition.

      For example, if the CPC currently has 1,000 I/O devices defined and you anticipate dynamically adding up to 200 more, then you'll need 20% more space for the expanded I/O definition. Type 20 for the percent of expansion.

b. To determine the total number of IOCDS subchannels (devices), shared subchannels, and unshared subchannels in an I/O definition:

- Use the totals in the HCD Device Detail Report.
- Use the totals in the IZP IOCP I/O Device Report.

7. To customize the Dynamic page for LPAR mode:

   Use the controls in the Percent of IOCDS expansion for shared I/O group box to divide the additional HSA space, reserved for expanding the I/O definition, between shared and dedicated I/O devices.

   Note: Select the **Determined by the system** radio button to use the system default percentages to divide the additional HSA space. The system default percentages are based on the ratio of shared I/O devices to dedicated I/O devices in the input/output configuration data set (IOCDS). However, a minimum of 20% and a maximum of 80% will be used for the percentage of shared I/O devices.

8. To customize the reset profile for LPAR mode:

   a. Choose one logical partition for making dynamic I/O changes to the hardware I/O definition. Select the notebook section for that logical partition, then select its Security page.

   b. Mark the **Input/output (I/O) configuration control** check box.

      The check box displays a check mark when you mark it. The check mark indicates you want to enable the logical partition for making dynamic I/O changes to the hardware I/O definition.

   c. Optionally, disable I/O configuration control for the remaining logical partitions. To disable I/O configuration control for a logical partition:

      1) Select the notebook section for the logical partition, then select its Security page.

      2) Unmark the **Input/output (I/O) configuration control** check box.

         The check box becomes empty when you unmark it. An empty check box indicates you want to prevent the logical partition from making dynamic I/O changes to the hardware I/O definition.

Enabling or disabling dynamic I/O without performing a power-on reset: Performing a power-on reset of the central processor complex (CPC), either directly or by activating the CPC, establishes many of its initial operational capabilities and characteristics, including whether dynamic input/output (I/O) configuration is enabled or disabled. Ordinarily, after a power-on reset of the CPC is performed, changing its operational capabilities and characteristics requires performing another power-on reset.

But if a power-on reset of the CPC initially enables dynamic I/O configuration, a task becomes available on the support element workplace for changing the CPC's dynamic I/O setting without performing another power-on reset.

To change the CPC's dynamic I/O setting without performing a power-on reset:

1. You must be logged on the support element in the system programmer or service representative user mode, and the most recent CPC power-on reset must have enabled dynamic I/O.
2. Open the **Task List** from the **Views** area.
3. Open **CPC Operational Customization** from the **Task List Work Area**.

   The CPC Operational Customization list contains the **Enable/Disable Dynamic Channel Subsystem** task that you will start.
4. Open **Groups** from the **Views** area.
5. Open the CPC from the **Groups Work Area**.
6. Drag and drop the CPC on the **Enable/Disable Dynamic Channel Subsystem** task to start it.

   This displays the Customize Dynamic Channel Subsystem window.
7. Use the window's controls, as follows, to enable or disable dynamic I/O for the CPC:
   a. Review the CPC's current setting for dynamic I/O. The selected radio button, either **Enabled** or **Disabled**, indicates the current setting.
   b. While dynamic I/O is enabled, select the **Disabled** radio button to change the setting to disabled.
   c. Or while dynamic I/O is disabled, select the **Enabled** radio button to change the setting to enabled.
   d. Select **OK** to save the setting and close the window.

   Use the online **Help** for more information on using the window to change the CPC's dynamic I/O setting.

Optimizing the performance of an application: You can optimize the performance of an application by selecting an A CP/SAP configuration for the central processor complex (CPC) that best suits the instruction processing requirements.

The physical processor units installed in the CPC are used either as central processors (CPs) or system assist processors (SAPs). The model of your machine determines its default configuration of CPs and SAPs. The SAPs, if any, are used exclusively for input/output (I/O) instruction processing.

If other CP/SAP configurations are available, selecting a configuration that configures one or more CPs as additional SAPs may improve the performance of some types of applications (applications that have greater needs for I/O instruction processing, for example). Selecting a non-default CP/SAP configuration may affect how the CPC can be activated.

Setting the CP/SAP configuration: The reset profile you use to activate a central processor complex (CPC) can establish the CPC's configuration of central processors (CPs) and system assist processors (SAPs).

To customize a reset profile to set the CP/SAP configuration:

1. Open a reset profile.

   For more information, see “Opening a reset profile” on page 6-5.

2. Select the CP/SAP page.

   The page lists the configurations of CPs and SAPs that can be established when the CPC is activated. The CPC's default configuration is listed first, followed by its additional configurations, if any.

3. Select from the list the configuration of CPs and SAPs you want to establish for the CPC upon activating it.

Use the online **help** for more information on customizing the CP/SAP configuration.

Effects of changing the CP/SAP configuration: No additional action is necessary if you intend to activate a CPC in a basic operating mode.

But if you intend to activate a CPC in logically partitioned (LPAR) mode, a reduction in the number of available CPs will reduce the number of logical processors you can assign to logical partitions. Activation of a logical partition will fail if the number of logical processors you attempt to assign exceeds the number of CPs available.

To avoid a logical partition activation failure, verify the number of logical processors assigned to a logical partition by its activation profile does not exceed the number of CPs available. For more information about customizing an activation profile to assign logical processors to a logical partition, see “Assigning logical processors” on page 6-27.

Preserving coupling facility data during power outages: Follow your local procedures for recovering from a power outage that is the result of a utility power failure. But you may be able to lessen the impact of such power outages on coupling facility data by *enabling the power save feature* of the central processor complex (CPC). The setting of the CPC's *power save feature* is one of several conditions that affect whether the CPC can preserve coupling facility data during a utility power failure. To use the power save feature, the following conditions must be true when a utility power failure occurs:

- The current setting of the power save feature is enabled.
- The operating system running in at least one CPC image supports the power save feature.

  Note: Currently, only coupling facility control code (CFCC) supports the power save feature. This condition is met only when the CPC is operating in logically partitioned (LPAR) mode, and one or more of its logical partitions are operating in coupling facility mode.

- An alternate, temporary power source for the CPC is installed and operational. Typical temporary power sources for CPCs include an optional Internal Battery Feature (IBF) or an uninterruptible power supply (UPS).

Logical partitions operating in coupling facility mode are referred to as *coupling facility logical partitions*. The conditions listed above are referred to here as *conditions for using the power save feature*.

Tips for setting the power save feature: The default setting for the power save feature of the central processor complex (CPC) is: disabled. If any of the conditions for using the power save feature cannot be met, let the power save feature remain disabled.

Otherwise, if all conditions for using the power save feature can be met, you may still want to have the power save feature disabled when:

- A back-up or emergency long-term power source is available and used for providing power during a utility power failure.
- *And* if a utility power failure occurs, you want to use the power provided to the CPC by its temporary power source to continue operating the CPC until the emergency power source starts providing power.

If all conditions for using the power save feature can be met, it is recommended you enable the power save feature when:

- A back-up or emergency long-term power source is not available or not used for providing power during a utility power failure.
- *And* during a utility power failure, you want to use the power provided to the CPC by its temporary power source to preserve data for coupling facility logical partitions, rather than using the power to continue operating the CPC.

Consequences of disabling the power save feature: When the power save feature is disabled, a central processor complex (CPC) cannot use the power save feature to preserve data for coupling facility logical partitions.

If a utility power failure occurs, and the power save feature cannot be used, a CPC uses power from its alternate, temporary power source to continue operating.

The CPC uses power from its temporary power source until utility power is restored by the utility or by an equivalent back-up or emergency long-term power source, or until the temporary power source is exhausted.

Consequences of enabling the power save feature: When the power save feature is enabled, and all other conditions for using the power save feature are true, the central processor complex (CPC) can preserve data for coupling facility logical partitions during a utility power failure.

If a utility power failure occurs, and the power save feature is used, then:

- Logical partitions that are not operating in coupling facility mode are reset. This interrupts and ends all operations in progress for those logical partitions.
- A rideout interval begins for each coupling facility logical partition. The coupling facility logical partitions continue operating during the rideout interval.

A *rideout interval* is an amount of time allowed to pass before a coupling facility logical partition is put in a power save state. Setting the same rideout interval for all coupling facility logical partitions is recommended. If the rideout interval is the same for all coupling facility logical partitions, the coupling facility logical partitions and CPC are put in a power save state if the rideout interval ends before utility power is restored. If the rideout interval is not the same for all coupling facility logical partitions, each one is put in the power save state when its rideout interval ends, and the CPC is put in the power save state when the longest rideout interval ends.

The CPC uses only enough power from its alternate, temporary power source to preserve the data for coupling facility logical partitions in the power save state. But coupling facility logical partitions and the CPC are not operational while in the power save state.

The CPC and coupling facility logical partitions remain in the power save state until utility power is restored, or until the CPC's temporary power source is exhausted, whichever occurs first.

Setting the power save feature: The reset profile you use to activate a central processor complex (CPC) can enable or disable the setting for the power save feature of the central processor complex (CPC).

To customize a reset profile for enabling or disabling the CPC's power save feature:

1. Open a reset profile.

   For more information, see "Opening a reset profile" on page 6-5.

2. Select the Options page.

   Move the cursor to any control and use the online **Help** for more information about using it. Press **F2** to request help for the Options page.

3. Locate the **Enable power save feature** check box. Then either:

   - Mark the check box to enable the power save feature. The check box displays a check mark when you mark it.
   - Or unmark the check box to disable the power save feature. The check box becomes empty when you unmark it.

Setting the rideout interval: Use the support element console to set the *rideout interval* for an operating system that supports the power save feature of the central processor complex (CPC).

Note: Currently, only coupling facility control code (CFCC) supports the power save feature. So setting the rideout interval is necessary only when you activate the CPC in logically partitioned (LPAR) mode, and activate one or more of its logical partitions in coupling facility mode.

A rideout interval is an amount of time allowed to pass before a coupling facility logical partition is put in a power save state.

If all the conditions for using the power save feature are true, a rideout interval begins for a coupling facility logical partition when a utility power failure occurs. During this time, the alternate, temporary power source for the CPC provides the power the coupling facility logical partition needs to continue operating.

If utility power is restored before the rideout interval ends, the CPC and coupling facility logical partition continue operating.

If the rideout interval ends before utility power is restored, the coupling facility logical partition is put in the power save state.

The default rideout interval is ten seconds. To change the rideout interval for a coupling facility logical partition, send it a RIDEOUT command. Use the **Operating System Messages** task from the support element workplace to send RIDEOUT and other CFCC commands to a coupling facility logical partition. For more information and instructions for using the task to send commands, see "Sending commands to operating systems" on page 3-10.

Releasing I/O reserves under error conditions: The reset profile you use to activate a central processor complex (CPC) can enable automatically resetting the input/output (I/O) interface under particular error conditions.

In a multiple CPC environment, several objects, which can be CPCs or logical partitions, may share the control units, channel paths, and I/O devices included in their I/O definitions.

The following error conditions may cause shared control units to hold reserves on their devices:

- A machine check places the CPC in a check-stopped state.
- Or the control program places an image of the CPC or a logical partition in a non-restartable wait state.

The reserves are held for the CPC or logical partition affected by the error condition. Holding reserves provides the affected object with exclusive use of devices, preventing them from being used by other objects that share the control units.

To release reserves held by shared control units assigned to an object, you must reset the I/O interface. Although resetting the I/O interface will not recover the object from its error condition, it will make the devices attached to shared control units available to other objects.

To customize a reset profile to enable automatically resetting the I/O interface:

1. Open a reset profile.

   For more information, see “Opening a reset profile” on page 6-5.

2. Select the Options page.

   Move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the Options page.

3. Mark the **Automatic input/output (I/O) interface reset** check box.

   The check box displays a check mark when you mark it. The check mark indicates you want to enable resetting the I/O interface automatically.

Setting a time limit on error recovery: The reset profile you use to activate a central processor complex (CPC) can set whether there is a time limit on error recovery.

The CPC, referred to here as the *system*, uses functions provided by its internal code to automatically handle errors and attempt recovery.

The system uses as much time as necessary to handle errors, unless you set a time limit. When a time limit is set, the system must handle errors and complete its recovery within the time limit, otherwise, the CPC is put in the check-stopped state.

The amount of time you specify determines the type of recovery the system can attempt:

- *Basic recovery*, for resolving hardware and internal code errors, is attempted when the recovery time limit is 2 seconds or greater.

- *Extended recovery*, for resolving hardware and internal code errors that basic recovery is unable to resolve, is attempted after basic recovery when the recovery time limit is 64 seconds or greater.

  Note: Both basic recovery then extended recovery are attempted also if you do not specify a time limit.

IBM recommends setting no time limit. This does not imply the system will recover from all errors, regardless of how much time is spent handling them. But it does allow the system to fully analyze errors and either:

- Recover from the errors.
- Or report errors from which it cannot recover.

To customize a reset profile to set no time limit on system recovery:

1. Open a reset profile.

   For more information, see “Opening a reset profile” on page 6-5.

2. Select the Options page.

   Move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the Options page.

3. Locate the System recovery time group box.
4. Unmark the **Limit system recovery time** check box.

   The check box becomes empty when you unmark it. An empty check box indicates there is no time limit on system recovery.

To customize a reset profile to set a time limit on system recovery:

1. Open a reset profile.

   For more information, see “Opening a reset profile” on page 6-5.

2. Select the Options page.

   Move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the Options page.

3. Locate the System recovery time group box.
4. Mark the **Limit system recovery time** check box.

   The check box displays a check mark when you mark it. The check mark indicates you want to set a time limit on system recovery.

   Marking the check box also makes the **Time limit** field available for you to specify the time limit.

5. Type the time limit for system recovery, from 1 to 999 seconds, in the **Time limit** field.

Setting processor running time: The reset profile you use to activate a central processor complex (CPC) in logically partitioned (LPAR) mode can set whether you or the CPC determines the processor running time.

When the CPC is activated in LPAR mode, the logical processors of logical partitions activated without dedicated processor resources share the remaining processor resources.

Each logical processor is given the same processor running time. *Processor running time* is the amount of continuous time allowed for a logical processor to perform jobs using shared processor resources. Processor running time is referred to also as a *timeslice*.

The processor running time can be dynamically determined by the CPC. That is, the CPC can automatically recalculate the running time whenever the number of active logical processors changes.

You can set the running time to a constant amount. To get optimal use of shared processor resources, IBM recommends letting the CPC dynamically determine the running time.

To customize a reset profile to let the CPC dynamically determine processor running time:

1. Open a reset profile.

   For more information, see “Opening a reset profile” on page 6-5.

2. Select the Options page.

   Move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the Options page.

3. Locate the Processor running time group box.
4. Select the **Dynamically determined by the system** radio button.

To customize a reset profile to set a constant processor running time:

1. Open a reset profile.

   For more information, see “Opening a reset profile” on page 6-5.

2. Select the Options page.

   Move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the Options page.

3. Locate the Processor running time group box.
4. Select the **Determined by the user** radio button.
5. Type the constant running time, from 1 to 100 milliseconds, in the **Running time** field.

Note: After activating the CPC in LPAR mode, you can use the support element workplace to dynamically change its settings for processor running time. See “Logical partition controls” on page 9-3 for more information.

Tips for activating logical partitions

The topics in this section provide tips for customizing an activation profile for activating a logical partition.

The tips are applicable to customizing reset profiles and image profiles unless indicated otherwise.

Activating logical partitions during CPC activation: The reset profile you use to activate a central processor complex (CPC) in logically partitioned (LPAR) mode can also activate one or more logical partitions.

To customize a reset profile to activate logical partitions during CPC activation in LPAR mode:

1. Open a reset profile.

   For more information, see “Opening a reset profile” on page 6-5.

2. If you have not already done so, customize the reset profile to activate the CPC in LPAR mode. For more information, see “Supporting LPAR mode operation” on page 6-8.

3. Select the Partitions page.

   Move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the Partitions page.

4. Review the logical partition name in each **Partition** field.

   The fields are initialized with the names of logical partitions defined in the input/output configuration data set (IOCDS) selected on the General page of the reset profile.

5. Review the numbers in the **Order** fields beside the logical partition names.

   The fields are initialized with the default activation order of the logical partitions. The logical partition with an order of 1 will be activated first, the logical partition with an order of 2 will be activated second, and so on.

6. Optionally, type a new order number in the **Order** field of a logical partition to change its activation order.

   Note: If you intend to operate one of the logical partitions in coupling facility mode, it should be activated first. That is, you should change the activation order of a coupling facility logical partition to 1.

7. Optionally, delete the order number of a logical partition to *not* activate it during activation of the CPC.

   Note: The names of logical partitions that are not activated will not be saved in the profile. That is, if you delete the order number of a logical partition, its name will be discarded.

The reset profile notebook includes a section of additional pages for each logical partition you include in the activation order. Page tabs along the right side of the notebook mark the beginning of each section. The information in each additional section is used to activate a logical partition. The name on each page tab identifies the logical partition activated by the information.

The information used to activate a logical partition, though it is included in a reset profile, is actually the logical partition's image profile.

The name of an image profile is the same as the name of the logical partition it activates. So each logical partition has only one image profile.

Since each reset profile that activates a logical partition includes the logical partition's only image profile, changing the logical partition's information in any activation profile changes the same information in all the other profiles as well. That is, if you customize a reset profile for activating a logical partition, for example, changing the reset profile *also* changes the logical partition's information in its image profile *and* in every other reset profile that activates the same logical partition.

Assigning a logical partition identifier: The activation profile you use to activate a logical partition must assign it a unique logical partition identifier.

The logical partition identifier becomes part of the central processor identifier of each logical processor assigned to the logical partition. The central processor identifier is used by subsystems and control programs to distinguish between logical processors.

To customize an activation profile to assign a logical partition identifier:

1. Open a reset profile or open an image profile.

   For more information, see “Opening a reset profile” on page 6-5 or “Opening a logical partition's image profile” on page 6-43.

2. If you opened a reset profile, select the page tab that displays the name of the logical partition.

3. Select the General page.

   Move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the General page.

4. In the **Partition identifier** field, type the hexadecimal digit to assign as the logical partition identifier.

   Notes:

   a. The partition identifier can be from X'0' to X'F'.

   b. The partition identifier must be unique among the identifiers of other logical partitions activated at the same time. If necessary, verify the partition identifier assigned to this image is unique by checking the **Partition identifier** fields on the General pages of the other logical partitions you intend to activate.

Selecting an operating mode: The activation profile you use to activate a logical partition must identify the operating mode you want to establish.

The operating mode describes the architecture that supports the operating system or control program you intend to load.

S/370, ESA/390, ESA/390 TPF, and coupling facility are examples of operating modes.

To customize an activation profile to select an operating mode:

1. Open a reset profile or open an image profile.

   For more information, see “Opening a reset profile” on page 6-5 or “Opening a logical partition's image profile” on page 6-43.

2. If you opened a reset profile, select the page tab that displays the name of the logical partition.

3. Select the General page.

   Move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the General page.

4. Select the operating mode you want to establish from the **Mode** list.

Activating a coupling facility logical partition: The activation profile you use to activate a logical partition can establish the support required to use it as a coupling facility.

A *coupling facility* is a logical partition that supports data sharing among applications running on other systems or logical partitions. A logical partition operating as a coupling facility is referred to here as a *coupling facility logical partition*.

To customize an activation profile to support and activate a coupling facility logical partition:

1. Open a reset profile or an image profile.

   For more information, see “Opening a reset profile” on page 6-5 or “Opening a logical partition's image profile” on page 6-43.

2. If you opened a reset profile:

   a. To activate the coupling facility logical partition during central processor complex (CPC) activation, customize the reset profile to activate the coupling facility logical partition first.

      For more information, see “Activating logical partitions during CPC activation” on page 6-22.

   b. To customize the information used to activate the coupling facility logical partition, select the page tab that displays the name of the logical partition.

3. Select the General page.

   Move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the General page.

4. Select **Coupling facility** from the **Mode** list.

5. Customize the activation profile to allocate storage to the coupling facility logical partition.

   For more information, see “Allocating central storage” on page 6-36 and “Allocating expanded storage” on page 6-36.

   Notes:

   a. Allocate at least 12 MB of initial central storage to the coupling facility logical partition.

   b. Allocate 0 MB of expanded storage to the coupling facility logical partition.

Supporting coupling facility channel emulation: The activation profile you use to activate a logical partition can establish support for emulating coupling facility channels.

The integrated coupling migration facility (ICMF) provides coupling facility channel emulation, but does not require or use coupling facility channel hardware. This allows emulating a coupled environment on a single central processor complex (CPC) operating in logically partitioned (LPAR) mode. The coupled environment is established between logical partitions that are activated as follows:

- One logical partition is activated in coupling facility mode.
- At least one other logical partition is loaded with a control program, like MVS or OS/390, that supports coupling facility operations.

- The above logical partitions are all enabled to use ICMF.

  Note: Only two logical partitions operating on the same CPC can be activated with the ability to use the ICMF.

An emulated coupled environment can be used to develop and test data sharing applications.

To customize an activation profile to activate a coupling facility with coupling facility channel emulation:

1. Open a reset profile or open an image profile.

   For more information, see “Opening a reset profile” on page 6-5 or “Opening a logical partition's image profile” on page 6-43.

2. If you opened a reset profile, select the page tab that displays the name of the logical partition.
3. Select the General page.

   Move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the General page.

4. Select **Coupling facility** from the **Mode** list.
5. Mark the **Enable integrated coupling migration facility (ICMF)** check box.

   The check box displays a check mark when you mark it. The check mark indicates activation will include establishing support for coupling facility channel emulation.

To customize an activation profile to activate another logical partition with coupling facility channel emulation to complete the emulated coupled environment:

1. Open a reset profile or open an image profile.

   For more information, see “Opening a reset profile” on page 6-5 or “Opening a logical partition's image profile” on page 6-43.

2. If you opened a reset profile, select the page tab that displays the name of the logical partition.
3. Select the General page.

   Move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the General page.

4. Select **ESA/390** or **ESA/390 TPF** from the **Mode** list.
5. Mark the **Enable integrated coupling migration facility (ICMF)** check box.

   The check box displays a check mark when you mark it. The check mark indicates activation will include establishing support for coupling facility channel emulation.

6. Customize the Load page to load an operating system that supports coupling facility operations.

   For more information about loading an operating system, see the topics that follow “Tips for loading operating systems” on page 6-37.

Assigning logical processors: The activation profile you use to activate a logical partition can assign it logical processors.

A logical processor is the processor resource defined to operate in a logical partition as a physical central processor. Logical processors are the processors a control program uses to perform jobs for the logical partition.

To customize an activation profile to assign logical processors to a logical partition:

1. Open a reset profile or open an image profile.

   For more information, see “Opening a reset profile” on page 6-5 or “Opening a logical partition's image profile” on page 6-43.

2. If you opened a reset profile, select the page tab that displays the name of the logical partition.
3. Select the Processor page.

   Move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the Processor page.

4. In the **Number of processors** field, type the number of logical processors to assign to the logical partition.
5. Use the controls in the Logical processor assignment group box to allocate processor resources to logical partitions.

   Note: After activating logical partitions, you can use the support element workplace to dynamically change its settings for sharing processor resources. See “Logical partition controls” on page 9-3 for more information.

Using integrated coupling facility processors: If integrated coupling facility processors are installed in the CPC, you can assign a coupling facility logical partition either central processors, integrated coupling facility processors, or dedicated coupling facility processors and shared central processors.

To customize an activation profile to assign logical processors to a coupling facility logical partition:

1. Open a reset profile or open an image profile.

   For more information, see “Opening a reset profile” on page 6-5 or “Opening a logical partition's image profile” on page 6-43.

2. If you opened a reset profile, select the page tab that displays the name of the logical partition.
3. Select the General page.
4. Select **Coupling Facility** from the **Mode** list.
5. Select the Processor page.
6. Select the type of processors you want assigned to the coupling facility logical partition:

   a. Dedicated central processors
   b. Not dedicated central processors
   c. Dedicated integrated coupling facility processors
   d. Not dedicated integrated coupling facility processors

e. Dedicated integrated coupling facility processors and not dedicated central processors.
f. Dedicated integrated coupling facility processors and not dedicated integrated coupling facility processors.

7. Use the controls available to complete the logical partition assignment for the coupling facility logical partition.

Assign both integrated coupling facility processors and not dedicated central processors to the coupling facility logical partition if you want to enable dynamic coupling facility expansion.

You can enable dynamic coupling facility dispatching for the coupling facility logical partition by:

1. Starting the **Operating System Messages** task on its image.
2. Using the task to send it the coupling facility control code command: DYNDISP ON

Using the Cryptographic Coprocessor feature: The activation profile you use to activate a logical partition can prepare it for running software products that work with the Cryptographic Coprocessor feature. Using the feature's cryptographic facilities and functions requires customizing the logical partition's activation profile to:

- Give it access to at least one cryptographic coprocessor.
- Set whether it can use the public key algorithm (PKA) facility.
- Select the cryptographic domain index (CDX) numbers of its control domains and usage domains.
- Set whether and how it can use cryptographic functions.
- Load it with an operating system, such as OS/390 or MVS/ESA™, that supports using cryptographic functions.

For more information about the Cryptographic Coprocessor feature, see “The Cryptographic Coprocessor feature” on page 10-12.

To customize an activation profile to allow a logical partition to use cryptographic facilities and functions:

1. Open a reset profile or open an image profile.

   For more information, see “Opening a reset profile” on page 6-5 or “Opening a logical partition's image profile” on page 6-43.

2. If you opened a reset profile, select the page tab that displays the name of the logical partition.
3. Select the General page.

   Move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the General page.

4. Select **ESA/390** or **ESA/390 TPF** from the **Mode** list.
5. Select the Processor page.

   Move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the Processor page.

6. The **Cryptographic coprocessors** list identifies each cryptographic coprocessor installed in the CPC. Select from the list the cryptographic coprocessors you want to give the logical partition access to.

   Selecting at least one cryptographic coprocessor inserts the Crypto page in the profile.

7. Select the Crypto page. Use the controls on the Crypto page to indicate whether and how you want the logical partition to use the public key algorithm (PKA) facility and other cryptographic functions and facilities.

   Move the cursor to any control and use the Online **Help** for more information. Press **F2** to request help for the Crypto page.

   Notes:

   a. If you intend to use the Integrated Cryptographic Service Facility (ICSF), see "Using the Integrated Cryptographic Service Facility" for additional instructions for customizing the Crypto page.

   b. If you intend to use a Trusted Key Entry (TKE) workstation to manage cryptographic keys, see "Using the Trusted Key Entry (TKE) feature" on page 6-30 for additional instructions for customizing the Crypto page.

   c. After activating logical partitions customized to use cryptographic coprocessors, you can use the support element workplace to dynamically change the settings of most cryptographic controls set on the Crypto page of their activation profiles. See "Logical partition cryptographic controls" on page 9-5 for more information.

8. Customize the Load page to load an operating system that supports using cryptographic functions and facilities.

   For more information about loading an operating system, see the topics that follow "Tips for loading operating systems" on page 6-37.

Using the Integrated Cryptographic Service Facility (ICSF)*:* The Integrated Cryptographic Service Facility/MVS (ICSF/MVS) is a program product that can use the Cryptographic Coprocessor feature to provide secure, high-speed cryptographic services in the OS/390 environment. If the central processor complex (CPC) is operating in logically partitioned (LPAR) mode, you can use ICSF/MVS cryptographic services for all logical partitions that are customized for using cryptographic coprocessors.

The activation profile you use to activate a logical partition can prepare it for using ICSF/MVS cryptographic services.

To customize an activation profile for a logical partition to use ICSF/MVS cryptographic services:

1. Customize a reset profile or image profile to enable the logical partition to use cryptographic facilities and functions.

   For more information, see "Using the Cryptographic Coprocessor feature" on page 6-28.

2. Select the Crypto page again.

   Move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the Crypto page.

3. If you have not already set the logical partition's usage domain index, set it now:
   a. Select a usage domain index for the logical partition from the **Usage domain index** list. It must be the same as the usage domain index set for the logical partition in the ICSF/MVS installation options data set. It is recommended that the usage domain index be the same number as the logical partition identifier.
   b. From the **Control domain index** list, select the index that is the same as the selected usage domain index.
4. Mark the **Enable public key algorithm (PKA) facility** check box to use the PKA services of ICSF/MVS for the logical partition.
5. Mark the following check boxes to use ICSF basic operations, including clear key entry, for the logical partition:
   - **Enable cryptographic functions**
   - **Enable public key secure cable (PKSC) and integrated cryptographic service facility (ICSF)**

   A check box displays a check mark when you mark it.
6. Mark the **Enable special security mode** check box to enable ICSF special security mode for the logical partition.

Using the Trusted Key Entry (TKE) feature: A Trusted Key Entry (TKE) workstation is an optional feature and part of a customized solution for using the Integrated Cryptographic Service Facility/MVS (ICSF/MVS) to manage cryptographic keys of a central processor complex (CPC) that has the Cryptographic Coprocessor feature installed and configured for using Data Encryption Standard (DES) and Public Key Algorithm (PKA) cryptographic keys. If the CPC is operating in logically partitioned (LPAR) mode, and one or more logical partitions are customized for using cryptographic coprocessors, you can use the TKE workstation to manage DES master keys, PKA master keys, and operational keys for all domains of each cryptographic coprocessor assigned to logical partitions defined to the TKE workstation as TKE hosts. Each logical partition using a domain managed through a TKE workstation connection to a TKE host is referred to here as a TKE target.

The activation profile you use to activate a logical partition can prepare it for being a TKE host or TKE target.

To customize an activation profile for a TKE host logical partition:

1. Customize a reset profile or image profile to enable the logical partition to use cryptographic facilities and functions.

   For more information, see “Using the Cryptographic Coprocessor feature” on page 6-28.
2. Select the Crypto page again.

   Move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the Crypto page.
3. If you have not already set the logical partition's usage domain index, set it now:
   a. Select a usage domain index for the logical partition from the **Usage domain index** list. It must be the same as the usage domain index set for

the logical partition in the ICSF/MVS installation options data set. It is recommended that the usage domain index be the same number as the logical partition identifier.

b. From the **Control domain index** list, select the index that is the same as the selected usage domain index.

4. From the **Control domain index** list, also select each index that is the same as the usage domain index of each TKE target logical partition you want to manage through a TKE workstation connection to this TKE host logical partition.
5. Mark the following check boxes to use a TKE workstation connection to this TKE host logical partition for basic cryptographic key management operations:
   - **Enable cryptographic functions**
   - **Enable public key secure cable (PKSC) and integrated cryptographic service facility (ICSF)**
   - **Enable query signature controls**
   - **Enable query transport controls**

   A check box displays a check mark when you mark it.
6. Mark the **Enable modify authority** check box to use a TKE workstation connection to this TKE host logical partition for loading updated cryptographic keys for domains used by the host's TKE target logical partitions.

   Note: This setting can be enabled for only one active logical partition.
7. To use a TKE workstation to dynamically enable and disable special security mode for the domain used by this logical partition, special security mode must be enabled for the logical partition at the support element and in the ICSF/MVS installation options data set. Mark the **Enable special security mode** check box to enable it at the support element when the logical partition is activated.

To customize an activation profile for a TKE target logical partition:

1. Customize a reset profile or image profile to enable the logical partition to use cryptographic facilities and functions.

   For more information, see “Using the Cryptographic Coprocessor feature” on page 6-28.
2. Select the Crypto page again.

   Move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the Crypto page.
3. If you have not already set the logical partition's usage domain index, set it now:

   a. Select a usage domain index for the logical partition from the **Usage domain index** list. It must be the same as the usage domain index set for the logical partition in the ICSF/MVS installation options data set. It is recommended that the usage domain index be the same number as the logical partition identifier.

   b. From the **Control domain index** list, select the index that is the same as the selected usage domain index.

4. Mark the following check boxes to use a TKE workstation to manage cryptographic keys for this TKE target logical partition:
   - **Enable cryptographic functions**
   - **Enable public key secure cable (PKSC) and integrated cryptographic service facility (ICSF)**

   Mark the **Enable integrated cryptographic facility (ICRF) key entry** check box also to enable using the **Load to queue** pop-up menu choice at a TKE workstation to load master keys, personal identification numbers (PINs), or key encrypting keys (KEKs) for the domain used by this logical partition.

   A check box displays a check mark when you mark it.
5. To use a TKE workstation to dynamically enable and disable special security mode for the domain used by this logical partition, special security mode must be enabled for the logical partition at the support element and in the ICSF/MVS installation options data set. Mark the **Enable special security mode** check box to enable it at the support element when the logical partition is activated.

Using the ADM facility: The activation profile you use to activate a logical partition can establish support for using the asynchronous data mover (ADM) facility, rather than the processor subsystem, to perform a subset of data storage operations.

The ADM facility uses the input/output (I/O) subsystem, rather than the processor subsystem, to move data:

- From central storage to expanded storage.
- From expanded storage to central storage.
- From one central storage location to another.

This frees the processor subsystem to process other instructions.

To customize an activation profile to establish support for using the ADM facility:

1. Open a reset profile or open an image profile.

   For more information, see “Opening a reset profile” on page 6-5 or “Opening a logical partition's image profile” on page 6-43.
2. If you opened a reset profile, select the page tab that displays the name of the logical partition.
3. Select the General page.

   Move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the General page.
4. Select **ESA/390** or **ESA/390 TPF** from the **Mode** list.
5. Select the Processor page.

   Move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the Processor page.
6. Mark the **Enable asynchronous data mover (ADM) facility** check box.

   The check box displays a check mark when you mark it. The check mark indicates activation will include establishing support for using the ADM facility.

7. Customize the Load page to load an operating system that supports using the ADM facility.

   For more information about loading an operating system, see the topics that follow “Tips for loading operating systems” on page 6-37.

Controlling access to performance data: The activation profile you use to activate a logical partition can control whether it has global access to performance data.

Ordinarily, a logical partition has access to only its own performance data. But a logical partition with global access also has access to the performance data of all other logical partitions activated on the same central processor complex (CPC). Performance data includes central processor usage and input/output processor usage by each logical partition.

To customize an activation profile to control global access to performance data:

1. Open a reset profile or open an image profile.

   For more information, see “Opening a reset profile” on page 6-5 or “Opening a logical partition's image profile” on page 6-43.

2. If you opened a reset profile, select the page tab that displays the name of the logical partition.
3. Select the Security page.

   Move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the Security page.

4. Locate the **Global performance data control** check box. Then either:
   - Mark the check box to give the logical partition global access to performance data. The check box displays a check mark when you mark it.
   - Or unmark the check box to give the logical partition access to only its own performance data. The check box becomes empty when you unmark it.

Note: After activating logical partitions, you can use the support element workplace to dynamically change their security settings, including global performance data control. See “Logical partition security” on page 9-1 for more information.

Controlling I/O configuration changes: The activation profile you use to activate a logical partition can control whether it can change the input/output (I/O) configuration of the central processor complex (CPC) on which it is activated.

Allowing a logical partition to change the I/O configuration enables:

- Reading and writing any input/output configuration data set (IOCDS) of the local CPC.
- Writing an IOCDS to a remote CPC.
- Using dynamic I/O configuration.
- Using the OSA Support Facility to view OSA configuration for other logical partitions.

To customize an activation profile to control changing the I/O configuration:

1. Open a reset profile or open an image profile.

   For more information, see “Opening a reset profile” on page 6-5 or “Opening a logical partition's image profile” on page 6-43.

2. If you opened a reset profile, select the page tab that displays the name of the logical partition.

3. Select the Security page.

   Move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the Security page.

4. Locate the **Input/output (I/O) configuration control** check box. Then either:

   - Mark the check box to allow using the logical partition to change the I/O configuration. The check box displays a check mark when you mark it.
   - Or unmark the check box to prevent using the logical partition to change the I/O configuration. The check box becomes empty when you unmark it.

Note: After activating logical partitions, you can use the support element workplace to dynamically change their security settings, including I/O configuration control. See “Logical partition security” on page 9-1 for more information.

Using dynamic I/O configuration: Dynamic input/output (I/O) configuration is supported by:

- The Hardware Configuration Definition (HCD) application on some MVS and OS/390 operating systems.
- The dynamic I/O configuration facility of some VM operating systems.

A logical partition using dynamic I/O configuration can dynamically change the hardware I/O definition in the hardware system area (HSA) of the central processor complex (CPC).

Input/output configuration control must be enabled for the logical partition on which you want to use dynamic I/O configuration. That is, you must mark the **Input/output (I/O) configuration control** check box on the Security page of the activation profile used to activate the logical partition.

Authorizing control of other logical partitions: The activation profile you use to activate a logical partition can control whether it can be used to issue a subset of control program instructions to other logical partitions activated on the same central processor complex (CPC).

Allowing a logical partition to issue instructions to other logical partitions enables:

- Using it to reset or deactivate another logical partition.
- Using the automatic reconfiguration facility (ARF) to backup another logical partition.

To customize an activation profile to authorize control of other logical partitions:

1. Open a reset profile or open an image profile.

   For more information, see “Opening a reset profile” on page 6-5 or “Opening a logical partition's image profile” on page 6-43.

2. If you opened a reset profile, select the page tab that displays the name of the logical partition.
3. Select the Security page.

   Move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the Security page.
4. Locate the **Cross partition authority** check box. Then either:
   - Mark the check box to allow using the logical partition to control other logical partitions. The check box displays a check mark when you mark it.
   - Or unmark the check box to prevent using the logical partition to control other logical partitions. The check box becomes empty when you unmark it.

Note: After activating logical partitions, you can use the support element workplace to dynamically change their security settings, including cross partition authority. See "Logical partition security" on page 9-1 for more information.

Using the automatic reconfiguration facility (ARF): The automatic reconfiguration facility (ARF) is supported by MVS/ESA SP 4.1 and higher. A logical partition using the ARF can serve as a backup for other logical partitions. The backup logical partition can:

- Deactivate a primary logical partition on which a problem has occurred.
- Automatically reconfigure storage previously allocated to the logical partition it deactivates.

Note: See *Processor Resource/Systems Manager™ Planning Guide* for more information about ARF.

Cross partition authority must be enabled for the logical partition on which you want to use the ARF. That is, you must mark the **Cross partition authority** check box on the Security page of the activation profile used to activate the logical partition.

Controlling use of reconfigurable channel paths: The activation profile you use to activate a logical partition can control whether it has exclusive use of its reconfigurable channel paths.

Ordinarily, a logical partition has exclusive use of its reconfigurable channel paths only while they are configured on. If the channel paths are configured off, they can be configured on to another logical partition.

Isolating a logical partition's reconfigurable channel paths reserves them for the logical partition while they are configured off, and prevents them from being configured on to other logical partitions.

To customize an activation profile to control the use of reconfigurable channel paths:

1. Open a reset profile or open an image profile.

   For more information, see "Opening a reset profile" on page 6-5 or "Opening a logical partition's image profile" on page 6-43.
2. If you opened a reset profile, select the page tab that displays the name of the logical partition.

3. Select the Security page.

   Move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the Security page.

4. Locate the **Logical partition isolation** check box. Then either:

   - Mark the check box to isolate the logical partition's offline reconfigurable channels paths. The check box displays a check mark when you mark it.
   - Or unmark the check box to make the logical partition's reconfigurable channels paths available to other logical partitions when the channel paths are configured off. The check box becomes empty when you unmark it.

Note: After activating logical partitions, you can use the support element workplace to dynamically change their security settings, including logical partition isolation. See “Logical partition security” on page 9-1 for more information.

Allocating storage: The activation profile you use to activate a logical partition can allocate its storage.

Allocating central storage: *Central storage* is main storage.

The central storage allocated to a logical partition upon activation is its *initial storage*. You must allocate initial central storage to each logical partition you intend to activate.

To customize an activation profile for allocating central storage to a logical partition:

1. Open a reset profile or open an image profile.

   For more information, see “Opening a reset profile” on page 6-5 or “Opening a logical partition's image profile” on page 6-43.

2. If you opened a reset profile, select the page tab that displays the name of the logical partition.
3. Select the Storage page.

   Move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the Storage page.

4. Use the Central storage group box to allocate the logical partition's central storage and to set its central storage origin.

Allocating expanded storage: *Expanded storage* is a buffer some operating systems can use for high-speed paging to and from main storage.

To customize an activation profile for allocating expanded storage to a logical partition:

1. Open a reset profile or open an image profile.

   For more information, see “Opening a reset profile” on page 6-5 or “Opening a logical partition's image profile” on page 6-43.

2. If you opened a reset profile, select the page tab that displays the name of the logical partition.
3. Select the Storage page.

Move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the Storage page.

4. Use the Expanded storage group box to allocate the logical partitions expanded storage and to set its expanded storage origin.

Tips for loading operating systems

The topics in this section provide tips for customizing an activation profile for loading an image with an operating system.

The tips are applicable to customizing reset profiles, image profiles, and load profiles unless indicated otherwise.

Loading an operating system during activation: The activation profile you use to activate an object can also load its image with an operating system. The object can be either a central processor complex (CPC) activated in basic mode, or a logical partition.

To customize an activation profile to load an operating system during an object's activation:

1. Open an applicable activation profile:
   - Open a reset profile if the object is a CPC.

     For more information, see “Opening a reset profile” on page 6-5.

     Note: The reset profile must be customized to activate the CPC in basic mode. For more information, see “Supporting basic mode operation” on page 6-8.
   - Otherwise, if the object is a logical partition, either open a reset profile or open its image profile.

     For more information, see “Opening a reset profile” on page 6-5 or “Opening a logical partition's image profile” on page 6-43.

     Note: The activation profile must *not* be customized to activate the logical partition as a coupling facility. For more information, see “Selecting an operating mode” on page 6-24.
2. If you opened a reset profile and the object is a logical partition, select the page tab that displays the name of the logical partition.
3. Select the Load page.

   Move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the Load page.
4. Mark the **Load during activation** check box.

   The check box displays a check mark when you mark it. The check mark indicates activation will include loading the object's image with an operating system.
5. Use the other controls on the page to provide information about which operating system to load and how to load it.

Choosing a CPC load type: normal or clear: The activation profile you use to load a central processor complex (CPC) can perform either a normal or clear load.

To customize an activation profile to choose a CPC load type:

1. Open an applicable activation profile:
   - Open a reset profile.

     For more information, see “Opening a reset profile” on page 6-5.

     Note: The reset profile must be customized to activate the CPC in basic mode. For more information, see “Supporting basic mode operation” on page 6-8.
   - Or open a load profile.

     For more information, see “Opening a load profile” on page 6-46.
2. Select the Load page.

   Note: If you opened a load profile, the Load page is the first and only page.

   Move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the Load page.
3. Locate the **Load type** controls. Then either:
   - Select **Normal** to perform a normal load, which performs the load without clearing main storage.

     Note: If you intend to perform the store status function during the load, it must be a normal load.
   - Or select **Clear** to perform a clear load, which clears main storage during the load.

Setting load attributes: The activation profile you use to load an image can set the load address and load parameter used to perform the load. The image can be supported by either a central processor complex (CPC) activated in basic mode, or a logical partition.

The *load address* is the address of the input/output (I/O) device that provides access to the operating system you want to load. The I/O device must be in the I/O configuration that is active when the load is performed. The I/O device may store the operating system or may be used to read the operating system from a storage device.

The *load parameter* is additional information operating systems support to provide you with additional control over the performance or outcome of a load. Check the configuration programming and reference documentation for the operating system to determine the load parameters that are available, and their effect on a load.

To customize an activation profile to set the load address and load parameter:

1. Open an applicable activation profile:
   - Open a reset profile if the object is a CPC.

     For more information, see “Opening a reset profile” on page 6-5.

     Note: The reset profile must be customized to activate the CPC in basic mode. For more information, see “Supporting basic mode operation” on page 6-8.
   - Otherwise, if the object is a logical partition, either open a reset profile or open its image profile.

For more information, see “Opening a reset profile” on page 6-5 or “Opening a logical partition's image profile” on page 6-43.

Note: The activation profile must *not* be customized to activate the logical partition as a coupling facility. For more information, see “Selecting an operating mode” on page 6-24.

- Or open a load profile.

  For more information, see “Opening a load profile” on page 6-46.

2. If you opened a reset profile and the object is a logical partition, select the page tab that displays the name of the logical partition.
3. Select the Load page.

   Note: If you opened a load profile, the Load page is the first and only page.

   Move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the Load page.
4. Type the load address in the **Load address** field.
5. Type the load parameter in the **Load parameter** field.

Using dynamic I/O to set load attributes: The activation profile you use to load an image can enable using dynamic input/output (I/O) configuration, rather than the activation profile, to set the load address and load parameter used to perform the load. The image can be supported by either a central processor complex (CPC) activated in basic mode, or a logical partition.

The image must be activated on a CPC that supports dynamic I/O configuration. And the image, or at least one of the images activated on the CPC, must be loaded with an operating system that supports an application or facility for using dynamic I/O configuration. Dynamic I/O configuration is supported by:

- The Hardware Configuration Definition (HCD) application on some MVS and OS/390 operating systems.
- The dynamic I/O configuration facility of some VM operating systems.

To customize an activation profile to enable using dynamic I/O to set the load address and load parameter:

1. Open an applicable activation profile:
   - Open a reset profile if the object is a CPC.

     For more information, see “Opening a reset profile” on page 6-5.

     Note: The reset profile must be customized to activate the CPC in basic mode. For more information, see “Supporting basic mode operation” on page 6-8.
   - Otherwise, if the object is a logical partition, either open a reset profile or open its image profile.

     For more information, see “Opening a reset profile” on page 6-5 or “Opening a logical partition's image profile” on page 6-43.

     Note: The activation profile must *not* be customized to activate the logical partition as a coupling facility. For more information, see “Selecting an operating mode” on page 6-24.

- Or open a load profile.

  For more information, see “Opening a load profile” on page 6-46.

2. If you opened a reset profile and the object is a logical partition, select the page tab that displays the name of the logical partition.
3. Select the Load page.

   Note: If you opened a load profile, the Load page is the first and only page.

   Move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the Load page.
4. Mark the **Use dynamically changed address** check box.

   The check box displays a check mark when you mark it. The check mark indicates activation will perform each load using the load address set for the image using dynamic I/O configuration.
5. Mark the **Use dynamically changed parameter** check box.

   The check box displays a check mark when you mark it. The check mark indicates activation will perform each load using the load parameter set for the image using dynamic I/O configuration.

Setting a time limit for performing the load: The activation profile you use to load an image sets a time limit for performing the load. The image can be supported by either a central processor complex (CPC) activated in basic mode, or a logical partition.

A time limit, or *time-out value*, is the amount of time allowed for performing the load. The load is cancelled if it cannot be completed within the time limit.

To customize an activation profile to set the time limit for performing the load:

1. Open an applicable activation profile:
   - Open a reset profile if the object is a CPC.

     For more information, see “Opening a reset profile” on page 6-5.

     Note: The reset profile must be customized to activate the CPC in basic mode. For more information, see “Supporting basic mode operation” on page 6-8.
   - Otherwise, if the object is a logical partition, either open a reset profile or open its image profile.

     For more information, see “Opening a reset profile” on page 6-5 or “Opening a logical partition's image profile” on page 6-43.

     Note: The activation profile must *not* be customized to activate the logical partition as a coupling facility. For more information, see “Selecting an operating mode” on page 6-24.
   - Or open a load profile.

     For more information, see “Opening a load profile” on page 6-46.
2. If you opened a reset profile and the object is a logical partition, select the page tab that displays the name of the logical partition.
3. Select the Load page.

Note: If you opened a load profile, the Load page is the first and only page.

Move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the Load page.

4. Type the time limit, from 60 to 600 seconds, in the **Time-out value** field.

Performing store status before a normal load: The activation profile you use to load a central processor complex (CPC) can perform the store status function before performing a normal load.

The store status function stores the current values of the processing unit timer, the clock comparator, the program status word, and the contents of the processor registers in their assigned absolute storage locations.

Note: For this reason, store status can be performed only before a normal load; a clear load would clear main storage during the load, including the information stored by the store status function.

Attention: Do *not* customize an activation profile to perform store status if the profile is customized to load an operating system, like MVS or OS/390, that already automatically performs store status upon being loaded.

To customize an activation profile to perform store status before a normal load:

1. Open an applicable activation profile:
   - Open a reset profile.

     For more information, see “Opening a reset profile” on page 6-5.

     Note: The reset profile must be customized to activate the CPC in basic mode. For more information, see “Supporting basic mode operation” on page 6-8.
   - Or open a load profile.

     For more information, see “Opening a load profile” on page 6-46.
2. Select the Load page.

   Note: If you opened a load profile, the Load page is the first and only page.

   Move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the Load page.
3. Locate the **Load type** controls. Select **Normal** to perform a normal load, which performs the load without clearing main storage.
4. Mark the **Store status** check box.

   The check box displays a check mark when you mark it. The check mark indicates activation will perform the store status function before performing the load.

Profiles for staged activations

You can perform a staged activation of a central processor complex (CPC) and its images by using a reset profile for an initial activation of the CPC, and then using other types of profiles for selective activations of its images.

Typical staged activations include:

- Using a reset profile to initially activate the CPC in basic mode, then using a load profile to load the CPC's image.

  This type of staged activation allows the operator to choose the operating system to load at the time of the load.

- Using a reset profile to initially activate the CPC in basic mode and to load the CPC's image with an operating system. Then, at a later time, using a load profile to load the CPC's image with a different operating system.

  This type of staged activation allows the operator to change the operating system while maintaining the rest of the CPC's current operational capabilities and characteristics.

- Using a reset profile to initially activate the CPC in logically partitioned (LPAR) mode and to activate and load one or more logical partitions. Then, at a later time, using load profiles to load one or more previously activated logical partitions with a different operating system, or using image profiles to activate and load one or more logical partitions not previously activated.

  This type of staged activation allows the operator to change the active logical partitions while maintaining the rest of the CPC's current operational capabilities and characteristics.

Initially activating the CPC

You can perform an initial activation of a central processor complex (CPC) by using a reset profile.

An initial activation means customizing a reset profile to either:

- Activate the CPC in basic mode.

  For more information, see “Supporting basic mode operation” on page 6-8 and the other topics that follow “Tips for activating CPCs” on page 6-8.

- Or activate the CPC in logically partitioned (LPAR) mode.

  For more information, see “Supporting LPAR mode operation” on page 6-8 and the other topics that follow “Tips for activating CPCs” on page 6-8.

Selectively activating logical partitions

You can perform a complete activation of a logical partition, but without again activating the central processor complex (CPC) that supports it, by using its image profile.

Before you can use an image profile to individually activate a logical partition, you must use a reset profile to activate the CPC in logically partitioned (LPAR) mode.

Image profiles

Customize an image profile for activating a logical partition when you want to activate only the logical partition, after the central processor complex (CPC) that supports it is initially activated in logically partitioned (LPAR) mode.

Optionally, you can customize the image profile to also load the logical partition during activation.

Notes:

- Initially activating a CPC in LPAR mode requires customizing and using a reset profile. For more information, see “Supporting LPAR mode

operation” on page 6-8 and the other topics that follow “Tips for activating CPCs” on page 6-8.

- The name of an image profile is the same as the name of the logical partition it activates. Each logical partition has only one image profile.

  Each reset profile that activates a logical partition includes the logical partition's only image profile, so changing the logical partition's information in any activation profile changes the same information in all the other profiles as well. That is, if you customize an image profile for activating a logical partition, for example, changing the image profile *also* changes the logical partition's information in every reset profile that activates the logical partition.

The reset profile notebook includes a section of additional pages for each logical partition you include in the activation order. Page tabs along the right side of the notebook mark the beginning of each section. The information in each additional section is used to activate a logical partition. The name on each page tab identifies the logical partition activated by the information.

The information used to activate a logical partition, though it is included in a reset profile, is actually the logical partition's image profile.

Opening a logical partition's image profile: You can use the support element workplace to start the task for customizing the image profile for a logical partition supported by a central processor complex (CPC) previously activated in logically partitioned (LPAR) mode. Starting the task is referred to also as *opening an image profile*.

To open a logical partition's image profile:

1. You must be logged on the support element in the system programmer user mode.
2. Open the **Task List** from the **Views** area.
3. Open **CPC Operational Customization** from the **Task List Work Area**.

   The CPC Operational Customization task list contains the **Customize/Delete Activation Profiles** task that you will start.
4. Open **Groups** from the **Views** area.
5. Open the **Images** group from the **Groups Work Area**.
6. Locate the image with the same name as the logical partition.
7. Drag and drop the logical partition on the **Customize/Delete Activation Profiles** task to start it.

   This opens the image profile and the list of load profiles you want to customize. When the list is initially displayed, the highlighted profile is the currently assigned profile for the partition.
8. Select from the list the name of the image profile you want to customize.
9. Select the **Customize** push button.

After you start the task, select a page and move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the page.

Checking a logical partition's assigned activation profile: You can assign a logical partition either its image profile or a load profile as its activation profile. Whenever the logical partition is activated, individually rather than with the central processor complex (CPC), it is activated according to the information in its assigned activation profile.

To check or change a logical partition's activation profile:

1. Open **Groups** from the **Views** area.
2. Open the **Images** group from the **Groups Work Area**.
3. Locate the image with the same name as the logical partition.
4. Double-click on the image.
5. Select the **Change options** push button.

   This opens the Change Object Options window.
6. Locate the **Profile name** field.

   It displays the name of the profile currently assigned as the logical partition's activation profile.
7. To assign a different profile, locate the desired profile name in the list of profiles field and select it.

   To assign the logical partition its image profile instead, use the window to select and save the image profile.

Navigating the image profile notebook: An image profile includes information for activating a logical partition.

Opening an image profile displays its information on windows that are organized as pages in a notebook.

The pages are identified by page tabs along the bottom of the notebook. The label on each page tab is a general description of the information on the page.

To use page tabs to turn notebook pages directly:

- To turn to a different page, click on its page tab along the bottom of the notebook.

Each page of the notebook also includes paging buttons, a left-pointing button and a right-pointing button, in its lower right corner.

To use paging buttons to turn notebook pages sequentially:

- To turn to the previous page in the notebook, click on the left-pointing button.
- To turn to the next page in the notebook, click on the right-pointing button.

Creating a new image profile: When a reset profile is customized for activating a logical partition, the reset profile automatically includes the logical partition's image profile. The name of the image profile is the same as the name of the logical partition.

If a reset profile is customized for activating a logical partition for which an image profile does not exist, a new image profile is automatically created for the logical partition.

For more information about customizing a reset profile for activating a logical partition, see “Activating logical partitions during CPC activation” on page 6-22.

Assigning an image profile to a logical partition: An image profile is automatically assigned to the logical partition with the same name. Whenever the logical partition is activated, it is activated according to the information in its assigned activation profile.

Saving an image profile: You must save an image profile to save the information you customized on its pages.

To save an open image profile:

1. After opening and customizing an image profile, select the General page.

   The **Profile name** field identifies the image profile that will be saved.

2. Select the **Save** push button to save the image profile and close it.

Tips for customizing image profiles: The best way to customize an image profile is to go through the image profile notebook, page by page, control by control. As you become familiar with image profiles you should be able to customize them quickly and easily.

Use the online **Help** for more information on the image profile notebook. It provides additional information about each page and its controls.

1. Move the cursor to the control.
2. Press the **F1** key or select the **Help** push button to request help.
3. While viewing the help for the control, press **F2** to request help for its page.

Note: Tips for activating logical partitions apply to customizing reset profiles and image profiles unless indicated otherwise.

Selectively loading images

You can load an image with an operating system, but without performing another complete activation of the central processor complex (CPC) or logical partition that supports it, by using an load profile.

Before you can use a load profile to load an image, you must use a reset profile to activate the CPC, and use the reset profile or an image profile to initialize the image.

Load profiles

Customize a load profile for loading an object when you want to only load the object after it is initially activated. The object can be either a central processor complex (CPC) or a logical partition.

Loading a CPC

Customize a load profile for loading a CPC when you want to only load the CPC again, after it is initially activated in basic mode.

Notes:

- Initially activating a CPC requires customizing the reset profile that activates the CPC in basic mode. For more information, see “Supporting basic mode operation” on page 6-8 and the other topics that follow “Tips for activating CPCs” on page 6-8.
- Customizing a load profile individually also changes the same load profile in each reset profile that includes it.

  Likewise, customizing a load profile while customizing a reset profile that includes it also changes the individual load profile and the same load profile in every other reset profile that includes it.

Loading a logical partition

Customize a load profile for loading a logical partition when you want to only load the logical partition again, after it is initially activated on a CPC activated in logically partitioned (LPAR) mode.

Note: Initially activating a logical partition requires customizing the reset profile that activates the CPC in LPAR mode. For more information, see “Tips for activating CPCs” on page 6-8, and the topics that follow “Tips for activating logical partitions” on page 6-22.

Opening a load profile: You can use the support element workplace to start the task for customizing load profiles for an object. The object can be a central processor complex (CPC) or logical partition. Starting the task is referred to also as *opening a load profile*.

To open a load profile:

1. You must be logged on the support element in the system programmer user mode.
2. Open the **Task List** from the **Views** area.
3. Open **CPC Operational Customization** from the **Task List Work Area**.

   The CPC Operational Customization task list contains the **Customize/Delete Activation Profiles** task that you will start.
4. Open **Groups** from the **Views** area.
5. To locate a CPC, open the **CPC** group from the **Groups Work Area**.
6. Otherwise, to locate a logical partition, open the **Images** group.

   This opens the Images Work Area. The area contains the target logical partition.
7. Drag and drop the target object on the **Customize/Delete Activation Profiles** task to start it.

   This opens the profile list that you want to customize. When the list of profiles is initially displayed, the highlighted profile is the currently assigned profile for the object.

8. Select from the list the name of the load profile you want to customize.
9. Select the **Customize** push button.

   This opens the selected load profile. Its information replaces the previous profile's information on the notebook page.

   After you start the task, move the cursor to any control, and use the online **Help** for more information. Press **F2** to request help for the page.

Checking an object's assigned activation profile: You can assign a central processor complex (CPC) either a reset profile or a load profile as its activation profile. You can assign a logical partition either an image profile or a load profile as its activation profile. Whenever either object is activated, it is activated according to the information in its assigned activation profile.

To check and change an object's activation profile:

1. Open **Groups** from the **Views** area.
2. To locate a CPC, open the **CPC** group from the **Groups Work Area**.
3. Otherwise, to locate a logical partition, open the **Images** group.

   This opens the Images Work Area. The area contains the target logical partition.
4. Double-click on the object.

   This opens a window of information about the object, referred to as its *object details* window.
5. Select the **Change options** push button.

   This opens the Change Object Options window.
6. Locate the **Profile name** field.

   It displays the name of the profile currently assigned as the object's activation profile.
7. To assign a different profile, locate the desired profile name in the list of profiles field and select it.

   To assign the object a load profile instead, use the window to select and save a load profile.

Creating a new load profile: You are responsible for creating load profiles that meet your unique needs.

You can use the default load profile as a template for creating new profiles. After you create a new profile, you can customize it as needed. After you create and customize your own load profiles, you can use them as templates for creating more new profiles.

To create a new load profile:

1. Open a load profile.

   For more information, see “Opening a load profile” on page 6-46.
2. Locate the **Profile name** field.

   The field identifies the load profile you opened. It will be used as a template for the new load profile.

3. To use a different load profile as a template:
   a. Select the list button beside the **Profile name** field.

      This opens a list of the names of all the load profiles. The load profile named DEFAULTLOAD is the default load profile provided by IBM.

   b. Select from the list the name of the load profile you want to use as a template.

      This opens the selected load profile. Its information replaces the previous profile's information on the notebook page.
4. To create a new profile from the template, type a unique name for the new profile in the **Profile name** field.
5. Select the **Save** push button to save the profile with the new name.

   Note: Saving the new profile does not change the load profile you used as a template.

Assigning a load profile: After you open a load profile for an object, either a central processor complex (CPC) or logical partition, you can assign it to the object as its activation profile. Whenever the object is activated, it is activated according to the information in its assigned activation profile.

To assign an open load profile as an object's activation profile:

1. After opening and customizing a load profile, the **Profile name** field identifies the load profile that will be assigned to the object.
2. Select the **Assign profile** push button to assign the load profile as the object's activation profile.

Saving a load profile: You must save a load profile to save the information you customized on its page.

To save an open load profile:

1. After opening and customizing a load profile, the **Profile name** field identifies the load profile that will be saved.
2. Select the **Save** push button to save the load profile and close it.

Tips for customizing load profiles: The best way to customize a load profile is to go through the one-page load profile notebook, control by control. As you become familiar with load profiles you should be able to customize them quickly and easily.

Use the online **Help** for more information on the load profile notebook.

1. Move the cursor to the control.
2. Press the **F1** key or select the **Help** push button to request help.
3. While viewing the help for the control, press **F2** to request help for its page.

Note: Tips for loading operating systems apply to customizing reset profiles, image profiles, and load profiles unless indicated otherwise.

Viewing activation profiles

If you want to only browse activation profiles, rather than customize them, you can instead use the support element workplace to start the task for viewing activation profiles previously customized for a central processor complex (CPC).

To view an activation profile:

1. You must be logged on the support element in the operator, advanced operator, or service representative user mode.
2. Open the **Task List** from the **Views** area.
3. Open **CPC Operational Customization** from the **Task List Work Area**.

   The CPC Operational Customization task list contains the **View Activation Profiles** task that you will start.
4. Open **Groups** from the **Views** area.
5. Open the **CPC** group from the **Groups Work Area**.

   This opens the CPC Work Area. The area contains the target CPC.
6. Drag and drop the CPC on the **Customize/Delete Activation Profiles** task to start it.

   This opens a list of all activation profiles currently customized for activating the CPC and its images.
7. Select from the list the name of the activation profile you want to view, then select the **View** push button.

   This opens the selected activation profile. Its information is displayed on pages of a notebook.

   After you start the task, select a page and move the cursor to any control, then use the online **Help** for more information. Press **F2** to request help for the page.

Assigning activation profiles to objects

Whenever an object on the support element workplace is the target of an activation, it is activated according to the information in its assigned activation profile.

You can assign activation profiles to either the central processor complex (CPC) or images.

To assign an activation profile to an object:

1. Open **Groups** from the **Views** area.
2. Open the group that contains the object you want to assign an activation profile.
3. Double-click on the object.
4. Locate the Instance information group box in the object details window.
5. Locate the **Activation profile** field in the group box.

It displays the name of the profile currently assigned as the object's activation profile.

6. To assign a different activation profile to the object, select the **Change options** push button.
7. Locate the **Profile name** field from the Change Object Options window.

   It displays the name of the profile currently assigned as the object's activation profile.
8. Locate the same name in the **Profile name** column in the list of profiles below the field. Then check the profile's type in the **Type** column.

   Note: The list includes all the activation profiles that can be assigned to the object.
9. To assign the object a different activation profile, select the profile from the list, then select the **Save** push button.

   This sets the selected profile as the object's assigned activation profile, and returns to the object details window.
10. Select the **Save** push button on the object details window to save the settings, including the object's newly assigned activation profile.

Grouping objects for activation

Creating a group, or *grouping*, is a way to assign more than one activation profile to an object, rather than changing the object's assigned activation profile every time you want to activate it differently.

Grouping creates copies of objects on the support element workplace. The objects can be the central processor complex (CPC) or its images. Different groups can contain the same object, such as the CPC, but the object's settings in one group can be customized independently of its settings in other groups. One such setting is the activation profile assigned to the object.

Grouping the CPC for complete activations

You can customize more than one reset profile for performing complete activations of the CPC and its images. For example, you may customize one reset profile for a complete activation of the CPC in basic mode, and another reset profile for a complete activation of the CPC in logically partitioned (LPAR) mode.

To use a reset profile for activating the CPC, you must assign it to the CPC before performing the activation. Afterwards, to use a different reset profile for activating the CPC, you could assign it to the CPC, replacing the previously assigned profile.

Rather than changing the reset profile assigned to a CPC each time you want to use a different one, you can instead create a unique group with the CPC for each reset profile you want to assign to it.

For example, to assign the CPC *both* a reset profile for activating it in basic mode, and a reset profile for activating it in LPAR mode:

1. Create a group with the CPC for activating it in basic mode:
   a. Give the group a meaningful name, like BASICMODE.
   b. Assign the group's CPC the reset profile for activating it in basic mode.

2. Create another group with the CPC for activating it in LPAR mode:
    a. Give the group a meaningful name, like LPARMODE.
    b. Assign the group's CPC the reset profile for activating it in LPAR mode.

Then to activate the CPC with either profile, simply activate the appropriate group.

Grouping the CPC for staged activations

You can customize a reset profile for performing an initial activation of the CPC in basic mode, and customize a load profile for performing a subsequent activation that only loads it. For example, you may:

- Customize the reset profile to activate the CPC and load the operating system used for production.
- Customize the load profile to only load the CPC with the operating system used for performing dumps.

To use the reset profile for activating the CPC, you must assign it to the CPC before performing the activation. Afterwards, to use the load profile for activating the CPC, you could assign it to the CPC, replacing the previously assigned profile.

Rather than changing the activation profile assigned to a CPC each time you want to use a different one, you can instead create a unique group with the CPC for each activation profile you want to assign to it.

For example, to assign the CPC *both* a reset profile for activating it initially, and a load profile for only loading it:

1. Create a group with the CPC for activating it initially:
    a. Give the group a meaningful name, like PRODUCTION.
    b. Assign the group's CPC the reset profile.
2. Create another group with the CPC for only loading it:
    a. Give the group a meaningful name, like LOADFORDUMP.
    b. Assign the group's CPC the load profile.

Then to activate the CPC with either profile, simply activate the appropriate group.

Grouping images for staged activations

You can customize more than one activation profile for performing staged activations of the CPC and its images. For example, you may:

- Customize a reset profile for an initial activation of the CPC in LPAR mode, with support for activating three logical partitions, but initially activating only of one of the logical partitions to support your production environment.
- And customize image profiles for activating the other two logical partitions to support batch processing and testing environments.

Using the reset profile for activating the CPC and one logical partition still automatically assigns *each* logical partition an image profile of the same name as its activation profile. Afterwards, you may want to deactivate the first logical partition, and then activate the other two logical partitions.

To help distinguish between the different purposes of the logical partitions, you can create a unique group with the logical partitions that support each purpose.

For example, to use one logical partition for production, and the other two logical partitions for batch processing and testing:

1. Create a group with the logical partition used for production.

   Give the group a meaningful name, like PRODUCTION.

2. Create another group with the logical partitions used for batch processing and testing.

   Give the group a meaningful name, like BATCHANDTEST.

To establish either environment, simply activate the appropriate group after deactivating the other group.

Note: The logical partitions in either group will be activated according to the information in the image profiles automatically assigned to them by the initial activation of the CPC.

Starting the system automatically after a power outage

Follow your local procedures for recovering from a power outage that is the result of a utility power failure. You may be able to speed recovery from such power outages by *enabling automatic activation* for the central processor complex (CPC). *Automatic activation* is a CPC setting that controls whether the CPC is activated automatically when power is restored following a utility power failure:

- When automatic activation is *enabled*, and a utility power failure occurs, the CPC is activated automatically when utility power is restored. The CPC is activated using the same reset profile used most recently to activate the CPC before the power outage.
- When automatic activation is *disabled*, and a utility power failure occurs, the CPC power remains off when utility power is restored. You can activate the CPC at any time, but manually, after utility power is restored.

The default setting for automatic activation is: disabled.

To enable or disable automatic activation:

1. You must be logged on the support element in the system programmer or service representative user mode.
2. Open the **Task List** from the **Views** area.
3. Open **CPC Operational Customization** from the **Task List Work Area**.

   The CPC Operational Customization task list contains the **Automatic Activation** task that you will start.

4. Open **Groups** from the **Views** area.
5. Open the CPC from the **Groups Work Area**.

6. Drag and drop the CPC on the **Automatic Activation** task to start it.
7. Use the Customize Automatic Activation window's controls to enable or disable automatic activation:
   a. Select the CPC name from the list.
   b. Select **Options** from the menu bar.
   c. While automatic activation is disabled, select **Enable automatic activation** from the menu to change the CPC's setting to enabled.
   d. While automatic activation is enabled, select **Disable automatic activation** from the menu to change the CPC's setting to disabled.
   e. Select **Save** to save the setting and close the window.

   Use the online **Help** for more information on using the window to enable or disable automatic activation.

Automating system operations

System tasks are the tasks you use to monitor and operate the central processor complex (CPC). Ordinarily, you must use the CPC's support element or other applicable console to manually start a task each time you want it performed.

There is a subset of tasks that you can perform automatically instead. The subset includes tasks, referred to here as *operations*, that are typically performed often or on a regular basis. The operations are:

- Making a backup of the support element's critical hard disk information.

  This operation automates the task you perform manually by using the **Backup Critical Data** task.
- Changing licensed internal code:
  - Accepting internal code changes.
  - Installing and activating internal code changes.
  - Retrieving internal code changes from the IBM Service Support System.
  - Removing internal code changes and activating the previous change levels.

  These operations automate some of the tasks you perform manually by using the **Change Internal Code** task.
- Activating the CPC.

  This operation automates the task you perform manually by using the **Activate** task.
- Deactivating the CPC.

  This operation automates the task you perform manually by using the **Deactivate** task.
- Transmitting system availability data to IBM.

  This operation automates one of the tasks you perform manually by using the **Transmit Service Data** task.

You can perform the operations automatically by setting up a schedule of operations for the CPC. This is referred to as *scheduling operations*. Consider scheduling an operation when you want to:

- Start the operation while the support element is unattended.
- Have the support element, rather than an operator, start the operation.
- Delay starting the operation until a later time.
- Perform the operation repetitively.

Note: The **Lockout disruptive task** does *not* affect a scheduled operation.

Scheduling operations

You can use the support element workplace to start the task for scheduling operations for the central processor complex (CPC).

To schedule operations for the CPC:

1. You must be logged on the support element in the system programmer or service representative user mode.
2. Open the **Task List** from the **Views** area.
3. Open **CPC Operational Customization** from the **Task List Work Area**.

   The CPC Operational Customization task list contains the **Scheduled Operations** task that you will start.
4. Open **Groups** from the **Views** area.
5. Open the CPC from the **Groups Work Area**.
6. Drag and drop the CPC on the **Scheduled Operations** task to start it.

   Select a menu from the menu bar, use the keyboard's arrow keys to move the cursor to a menu choice and use the online **Help** for more information about using the menu choice. Press **F2** to request help for the window.
7. To schedule an operation for the CPC, select the **Options** menu from the menu bar, then select **New** from the menu.
8. Use the **Add a Scheduled Operation** window and subsequent windows to select the operation you want to perform, and to set a schedule for performing it automatically.

   Use the online **Help** for any window for more information about using it to schedule the operation.

Setting the CPC time-of-day clock

If you have experience using other systems, you may have used SET CLOCK or a similar operating system command to set the system's time-of-day (TOD) clock during system initialization. Likewise, the support element workplace supports using an operating system command to set the TOD clock of the central processor complex (CPC). Since the CPC TOD clock is synchronized automatically to the

support element TOD clock, consider whether and how often you need to set the CPC TOD clock manually. You may find there is a less frequent need to do so.

Synchronizing the CPC TOD clock and the support element TOD clock

Both the central processor complex (CPC) and its support element have time-of-day (TOD) clocks. The time and date of both TOD clocks should be the same or very nearly the same. For this reason, the TOD clocks are automatically synchronized with each other as follows:

- The CPC TOD clock is synchronized with the support element TOD clock whenever a power-on reset of the CPC is performed.
- The support element TOD clock is synchronized to the CPC TOD clock whenever the CPC TOD clock is changed either manually or automatically:
  - You can use SET CLOCK or a similar operating system command to manually set the CPC TOD clock.
- At 11:00PM on the support element TOD clock, it is synchronized with the CPC TOD clock if:
  - The CPC is operating.
  - The support element TOD clock was *not* set manually since the TOD clocks were last synchronized.

  Otherwise:
  - If the CPC is not operating, the support element TOD clock remains unchanged.
  - If the CPC is operating, but the support element TOD clock was set manually since the TOD clocks were last synchronized, then both TOD clocks remain unchanged and are not synchronized.

Instructions for setting the CPC TOD clock are provided in the next topic. For instructions for setting the support element TOD clock, see “Setting the support element time-of-day clock manually” on page 16-5.

Setting the CPC TOD clock manually

When manually setting the central processor complex (CPC) time-of-day (TOD) clock is necessary, follow your local procedure for manually setting a system's TOD clock, presumably using SET CLOCK or a similar operating system command from an operating system console. During the procedure, when the operating system responds to your command by instructing you to *enable setting the TOD clock*, use the support element console to temporarily enable setting the CPC TOD clock.

Note: The CPC *cannot* be activated in logically partitioned (LPAR) mode.

To enable setting the CPC TOD clock:

1. You must be logged on the support element in the operator, advanced operator, system programmer, or service representative user mode.
2. Open the **Task List** from the **Views** area.

3. Open **CPC Operational Customization** from the **Task List Work Area**.

   The CPC Operational Customization task list contains the **Enable TOD** task that you will start.

4. Open **Groups** from the **Views** area.

5. Open any group that contains the CPC from the **Groups Work Area**.

   Note: Enabling a CPC TOD clock can be considered disruptive. If the CPC is locked, unlock it. See "Setting lockout for disruptive tasks on an object" on page 2-15.

6. Drag and drop the CPC on the **Enable TOD** task to start it.

   This enables setting the CPC TOD clock for several seconds that allows the operating system to continue processing your command for setting the CPC TOD clock. Return to the operating system console to complete the procedure.

Allocating storage

The model of your system determines the minimum, standard, and maximum storage capacity of the central processor complex (CPC).

Installed storage is part of the CPC's hardware configuration; it is provided by one or more storage cards physically installed in the CPC. *Allocated storage* is installed storage that is set aside for a specific purpose:

- The *hardware system area (HSA)* is storage only the CPC can use. It stores the CPC's licensed internal code and input/output (I/O) definition while the CPC is activated.
- *Central storage* includes main storage, the HSA, and internal disk subsystem cache. Operating systems and applications can use main storage; only the CPC can use the HSA and cache.
- *Expanded storage* is a buffer some operating systems can use for high-speed paging to and from main storage.

Storage is allocated to a CPC when it is activated.

When the CPC is activated in logically partitioned (LPAR) mode, much of the storage allocated to the CPC can be allocated to the logical partitions activated on it:

- The central storage allocated to the CPC, but *excluding* the storage used for the CPC HSA, is the central storage initially available to logical partitions.
- The expanded storage allocated to the CPC is the expanded storage initially available to logical partitions.

Like the CPC, storage is allocated to a logical partition when it is activated. To allocate storage to the CPC or a logical partition, you must customize the activation profile you use to activate it.

Customizing activation profiles for allocating storage

Customize the activation profile you use to activate an object, either a central processor complex (CPC) or a logical partition, for allocating storage to it:

- Customize a CPC's reset profile for allocating its central storage and expanded storage.
- Customize a CPC's reset profile for allocating central storage and expanded storage to each logical partition activated during CPC activation in logically partitioned (LPAR) mode.
- For each logical partition defined but *not* activated during CPC activation in LPAR mode, customize the logical partition's image profile for allocating its central storage and expanded storage.

Customizing activation profiles is documented in detail in the following topics:

- For general information about customizing activation profiles, see “Getting ready to operate the system: customizing activation profiles” on page 6-1.
- For information about allocating storage for a CPC, see “Allocating storage” on page 6-12.
- For information about allocating storage for a logical partition, see “Allocating storage” on page 6-36.

After customizing an activation profile for allocating storage to an object, storage is actually allocated only when the activation profile is used to activate the object.

Estimating the size of the hardware system area

Since the size of the hardware system area (HSA) determines the amount of central storage that remains available for general use or for allocating to logical partitions, it is helpful to estimate the HSA size before customizing activation profiles for allocating storage to the central processor complex (CPC) or logical partitions.

Estimates of the HSA size vary according to several conditions, including:

- The CPC model and engineering change (EC) level.
- The operating mode established for the CPC during power-on reset.

  Operating the CPC in logically partitioned (LPAR) mode increases the HSA size more than operating the CPC in a basic mode. The exact increase varies with the number of logical partitions defined.
- The size of the input/output (I/O) configuration used to define the CPC's I/O definition during power-on reset.

  Defining a large I/O configuration increases the HSA size more than defining a small I/O configuration. The exact increase varies with the number of I/O devices, control units, and channel paths defined.
- Whether the CPC supports dynamic I/O configuration.

  Supporting dynamic I/O configuration increases the HSA size more than not supporting it. The exact increase varies with the additional percentage of HSA storage reserved for expansion the I/O definition.

You can use the support element workplace to estimate the HSA size for any combination of these and other conditions.

To estimate the HSA size:

1. Open the **Console Actions** view on the support element workplace.

   The Console Actions Work Area contains the **HSA Estimation Tool** task that you will start.

2. Double-click on the **HSA Estimation Tool** console action to start it.

   The HSA Estimation Tool window provides controls for setting conditions that affect the size of the HSA and for calculating an estimate of the HSA size.

   Use the online **Help** for more information about using it to set conditions and calculate estimates.

Reviewing current storage allocations

You can use the support element workplace to start the task for reviewing the current storage allocations of the central processor complex (CPC) and its logical partitions, if any.

To review the current storage allocations:

1. You must be logged on the support element in the operator, advanced operator, system programmer, or service representative user mode, and the CPC must be activated or power-on reset.
2. Open the **Task List** from the **Views** area.
3. Open **CPC Operational Customization** from the **Task List Work Area**.

   The CPC Operational Customization task list contains the **Storage Information** task that you will start.

4. Open **Groups** from the **Views** area.
5. Open the CPC from the **Groups Work Area**.
6. Drag and drop the CPC on the **Storage Information** task to start it.
   - Page tabs along the bottom of the notebook identify its pages. Select a page tab to display that page.
   - The first page of the notebook displays information about storage installed and allocated for the CPC. Its page tab is labelled: Base system storage allocation.
   - If the CPC is activated in logically partitioned (LPAR) mode, the notebook includes a second page that displays information about storage allocated for logical partitions currently activated on the CPC. Its page tab is labelled: Logical partition storage allocation.

   Use the online **Help** for more information about using the notebook to review the current storage allocations.

Degraded storage mode

Degraded storage mode is the result of a hardware failure that prevents the central processor complex (CPC) from using all of its installed storage. Activating the CPC fails if a hardware failure that affects its storage occurs. Like all hardware failures, the CPC automatically analyzes it, then reports it by issuing a hardware message.

The details of the hardware message will instruct you to customize the CPC's activation profiles to attempt activating the CPC and its images with *half* the amount of its installed storage. Activate the CPC with the newly customized activation profiles. If the activation succeeds, the CPC resumes operating, but with a reduced amount of installed storage. This condition, referred to as *degraded storage mode*, allows the CPC to continue operating until the hardware failure is corrected by you or your service provider.

Recognizing degraded storage mode

The support element workplace indicates whether a CPC is operating in degraded storage mode:

1. Open **Groups** from the **Views** area.
2. Open the CPC from the **Groups Work Area**.
3. Check the CPC name:
   - If the CPC is operating in degraded storage mode, the term **Degraded** is displayed after or below the CPC name.
   - Otherwise, if the CPC is operating in normal storage mode, with all of its installed storage, only the CPC name is displayed.

Determining the degraded storage amount

In degraded storage mode, the amount of installed storage available for allocating central and expanded storage is temporarily reduced. The reduced amount of available storage is referred to here as the *degraded storage amount*.

Upon activating a central processor complex (CPC) in degraded storage mode, the CPC hardware system area (HSA), central storage, and expanded storage are allocated from the degraded storage amount.

To determine the degraded storage amount, use the support element workplace to review the current storage allocations after the CPC recovers in degraded storage mode.

To determine the degraded storage amount:

1. Open the **Task List** from the **Views** area.
2. Open **CPC Operational Customization** from the **Task List Work Area**.

   The CPC Operational Customization task list contains the **Storage Information** task that you will start.
3. Open **Groups** from the **Views** area.

4. Open any group that contains the CPC from the **Groups Work Area**.
5. Drag and drop the CPC on the **Storage Information** task to start it. The notebook displays the current storage allocation of the CPC and its logical partitions, if any.

   Use the online **Help** for more information about using the notebook to review the current storage allocations.
6. Page tabs along the bottom of the notebook identify its pages. Select the page tab labelled Base system storage allocation, if necessary, to display that page.
7. Locate the Installed Storage Details group box on the page.
8. Add the storage amounts displayed in the following fields in the group box:
   - **Central storage**
   - **Expanded storage**

   The sum is the degraded storage amount.

Allocating storage in degraded storage mode

You can change the central or expanded storage allocated to a central processor complex (CPC) while it remains in degraded storage mode. The total storage you allocate to the CPC cannot exceed the degraded storage amount.

You can also activate logical partitions and allocate storage to them while the CPC is in degraded storage mode. The total storage allocated to a logical partition cannot exceed the degraded storage amount. The sum of storage allocations for all activated logical partitions cannot exceed the degraded storage amount.

Allocating CPC storage in degraded storage mode

You can change the central and expanded storage allocated to a CPC operating in degraded storage mode by customizing a reset profile with new storage amounts, then using it to activate the CPC:

1. Since degraded storage mode is a temporary condition, you may want to create a new, temporary reset profile for the CPC, rather than temporarily changing an existing reset profile.

   For more information, see “Creating a new reset profile” on page 6-6.
2. Customize the reset profile to allocate the degraded storage amount as central and expanded storage for the CPC.

   For more information, see “Allocating storage” on page 6-12.
3. Activate the CPC with the profile to make the new storage allocations take effect.

   For more information, see “Activating the CPC” on page 3-4.

Allocating logical partition storage in degraded storage mode

It may be necessary to change the central and expanded storage allocated to a logical partition before you can activate it on a CPC operating in degraded storage mode. Check the activation profile you use to activate the logical partition to verify that its central and expanded storage allocations do not exceed the reduced amounts of central and expanded storage allocated to the CPC. If necessary,

customize the activation profile to change the central and expanded storage allocated to a logical partition.

- Check a CPC's reset profile for the amounts of central storage and expanded storage allocated to each logical partition activated during CPC activation in logically partitioned (LPAR) mode.

  If necessary, customize a reset profile to change the storage allocations of the logical partitions:

  1. Since degraded storage mode is a temporary condition, you may want to create a new, temporary reset profile for the CPC, rather than temporarily changing an existing reset profile.

     For more information, see “Creating a new reset profile” on page 6-6.

  2. Customize the reset profile to allocate central and expanded storage for each logical partition activated by the profile.

     For more information, see “Allocating storage” on page 6-36.

  3. Activate the CPC with the profile to activate the logical partitions and to make the new storage allocations take effect.

     For more information, see “Activating the CPC” on page 3-4.

- For each logical partition defined but *not* activated during CPC activation in LPAR mode, check the logical partition's image profile for the amounts of central storage and expanded storage allocated to it.

  If necessary, customize the image profile to change the storage allocations of the logical partitions:

  1. Customize the image profile to allocate central and expanded storage for each logical partition activated by the profile.

     For more information, see “Allocating storage” on page 6-36.

  2. Activate the logical partition with the profile to make the new storage allocations take effect.

     For more information, see “Activating the CPC” on page 3-4.

Remember, whether you activate logical partitions during or after CPC activation, the sums of central storage and expanded storage allocated to each activated logical partition cannot exceed the reduced amounts of central and expanded storage allocated to the CPC.

Getting ready to monitor the system: customizing system activity profiles

To prepare for using system activity profiles to start system activity analysis, you can use the support element workplace to work with the profiles as needed. Working with system activity profiles includes:

- Viewing a profile
- Customizing a profile
- Creating a new profile
- Deleting a profile

- Preparing to use profiles for monitoring system activity from a Hardware Management Console.

Regardless of what you want to do with system activity profiles, you will begin by opening a list of system activity profiles.

Opening a list of system activity profiles

You can use the support element workplace to begin tasks for working with system activity profiles for a central processor complex (CPC) by opening a list of its profiles.

To open a list of system activity profiles:

1. Open the **Task List** from the **Views** area.
2. Open **CPC Operational Customization** from the **Task List Work Area**.

   The CPC Operational Customization task list contains the **System Activity Profiles** task that you will start.
3. Open **Groups** from the **Views** area.
4. Open the **CPC** group from the **Groups Work Area**.
5. Drag and drop the CPC on the **System Activity Profiles** task to start it.

   This opens the Customize System Activity Profiles List notebook. Its page lists the CPC's system activity profiles, and it provides push buttons for working with them.

   Use the online **Help** for more information about using it to work with system activity profiles.

Viewing a system activity profile

View a system activity profile to determine:

- The particular system resources it is customized to monitor.
- The conditions for which a resource's usage is reported or ignored.
- How a resource's usage is presented.

To view a system activity profile, follow the instructions for customizing a system activity profile, but do not make or save any changes. For instructions, see “Customizing a system activity profile” on page 6-63.

Note: After starting the task for customizing a profile, you can open various windows to get detailed information about the contents of the profile. To avoid changing a profile while you view it, close the first window, titled Customize System Activity Profile, only by selecting its **Cancel** push button. If you did inadvertently change any information in the profile, closing the window in this way will give you an opportunity to discard the changes.

Customizing a system activity profile

Customize a system activity profile to:

- Define the particular system resources you want to monitor.
- Set conditions that you want each resource's usage reported or ignored.
- Indicate how you want each resource's usage presented.

To customize a system activity profile:

1. Open a list of system activity profiles. For instructions, see “Opening a list of system activity profiles” on page 6-62.

   This opens the Customize System Activity Profiles List notebook. Its page lists the CPC's system activity profiles, and it provides push buttons for working with them.

2. Select from the list the system activity profile you want to customize, then select the **Customize** push button.

   This opens the profile. Its information displays on the Customize System Activity Profile window.

3. Generally, use the window's controls to customize the profile information.

   Move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the window.

4. Review the window's list of activity lines, labelled **Line**, **Component**, and **Description**, to determine which system resources the profile is currently customized to monitor.

   Change one or more activity lines to:

   - Define the particular system resources you want to monitor.
   - Set conditions that you want each resource's usage reported or ignored.
   - Indicate how you want each resource's usage presented.

5. To change an activity line, use the list, the controls labelled **Modify line options**, and the **OK** push button as follows:

   a. From **Modify line options**, select the radio button labelled **Change line**.

   b. From the list of activity lines, select the line you want to change.

   c. Select **OK** to open the Change Line window.

   d. Locate the list labelled **New component for this line**. It lists radio buttons that describe the particular system resources you can monitor.

      Move the cursor to any radio button and use the online **Help** for more information. Press **F2** to request help for the window.

   e. Select the radio button that describes the particular system resource you want to monitor, then select **OK**.

      This opens an additional window, referred to as an *options* window, for the resource you selected to monitor.

   f. Use the controls on the options window to set conditions for which you want the resource's usage reported or ignored, and to indicate how you want the resource's usage presented.

Move the cursor to any control and use the online **Help** for more information. Press **F2** to request help for the window.

g. Select **OK** to set the options and complete customizing the activity line.

This returns you to the Customize System Activity Profile window, and updates its list of activity lines with your changes.

Repeat these steps as needed to customize up to 50 lines of activity.

Note: The activity lines you change are not saved until you save the entire system activity profile. Save the profile, after you finish customizing it, by selecting **Save** on the Customize System Activity Profile window.

6. In addition to changing activity lines, you can use the other line options on the Customize System Activity Profile window at any time to edit and arrange the list of activity lines as needed. Use the list, the controls labelled **Modify line options**, and the **OK** push button as follows:

   a. From **Modify line options**, select the radio button that describes how you want to modify the activity lines. For example, if you want to delete a line from the list, select **Delete line**.

   Use the online **Help** after you select a radio button for more information.

   b. From the list of activity lines, select the line you want to modify with the option you selected.

   c. Select **OK** to use the selected option to modify the selected line.

7. When you finish changing and arranging activity lines, you are ready to finish customizing the system activity profile and save it. Use the Customize System Activity Profile window as follows:

   a. Optionally, type in the **Description** field a brief description of the types of activity the profile can be used to monitor.

   Note: Providing a profile description is recommended. Whenever a list of system activity profiles is opened, either to work with the profiles or to start system activity analysis, profile names *and* descriptions are listed to help you distinguish between the different profiles and their purposes.

   b. Review the value in the **Refresh rate** field. When system activity analysis is started using a single profile, the profile's refresh rate is the number of seconds set for how often the activity summaries are updated with new information from the system.

   Optionally, type a different value, from 3 to 20 seconds, in the field.

   c. Select the **Save** push button to save the system activity profile and close it.

Creating a new system activity profile

You are responsible for creating system activity profiles that meet your unique needs for monitoring system activity.

You can use any default system activity profile as a template for creating new profiles. After you create a new profile, you can customize it as needed. After you create and customize your own system activity profiles, you can use them as templates for creating more new profiles.

To create a new system activity profile:

1. Open a list of system activity profiles. For instructions, see “Opening a list of system activity profiles” on page 6-62.

   This opens the Customize System Activity Profiles List notebook. Its page lists the CPC's system activity profiles, and it provides push buttons for working with them.

2. Select from the list the system activity profile you want to use as a template for the new profile, then select the **Customize** push button.

   This opens the profile. Its information displays on the Customize System Activity Profile window. The **Profile name** field identifies the system activity profile you opened. It will be used as a template for the new system activity profile.

3. To create a new profile from the template, type a new, unique name for the new profile in the **Profile name** field.

4. Customize any other information in the profile as needed. For instructions, see “Customizing a system activity profile” on page 6-63.

5. Select the **Save** push button to save the profile with the new name and any other information you customized.

   Note: Saving the new profile does not change the system activity profile you used as a template.

Preparing to monitor system activity from a Hardware Management Console

A Hardware Management Console typically is used to operate and monitor multiple central processor complexes (CPCs). If you use a Hardware Management Console to operate and monitor your CPC, in addition to its support element console, then you can use the Hardware Management Console to monitor the CPC's system activity.

Unlike starting system activity analysis from the CPC's support element console, for which you choose the system activity profiles you want to use at that time, starting system activity analysis from a Hardware Management Console uses profiles assigned to the CPC for that purpose. The system activity profiles assigned to the CPC are referred to as its *active* profiles.

The active profile initially assigned to the CPC is the default system activity profile named DEFAULT. But you can assign the CPC other active profiles as needed, to choose in advance the system activity you want to monitor from a Hardware Management Console.

To assign profiles for monitoring system activity from a Hardware Management Console:

1. Open a list of system activity profiles. For instructions, see “Opening a list of system activity profiles” on page 6-62.

   This opens the Customize System Activity Profiles List notebook. Its page lists the CPC's system activity profiles, and it provides push buttons for working with them.

2. Review the information in the list column labelled **Status** to determine which profiles are currently assigned to the CPC for monitoring system activity from a Hardware Management Console.

Note: The column displays **Active for HWMCA** to indicate the profile is assigned to the CPC for monitoring its activity from a Hardware Management Console. Otherwise, the column displays **Not active for HWMCA**. You may have to scroll the column to see the entire status.

3. Select from the list the system activity profiles you want to use for monitoring system activity from a Hardware Management Console.

   Note: Select all profiles you want to assign as the CPC's active profiles, *including profiles that are already active*.

4. Deselect the active profiles, if any, that you no longer want to use for monitoring system activity from a Hardware Management Console.

5. Select the **Change status** push button to assign the selected profiles as the CPC's active profiles.

   This sets the status of each selected profile to **Active for HWMCA**. Afterwards, starting system activity analysis from a Hardware Management Console will use the active profiles.

   Note: If system activity analysis of the CPC is already in progress on a Hardware Management Console, it will begin using the CPC's newly assigned active profiles shortly after their status is changed.

Chapter 7. Settings for remote connections and communications

This section describes the tasks from the **CPC Remote Customization** task list you can use to customize settings that control whether, how, and for what purposes connections are established and communications are conducted between remote systems and the support element of the central processor complex (CPC).

The CPC Remote Customization task list contains the tasks, referred to here as *remote customization tasks*. This section provides instructions for starting the tasks.

Connecting and communicating with a remote service support system

Remote service is two-way communication between the support element of a central processor complex (CPC) and a remote, automated *service support system* provided and maintained by the CPC's service provider. For example, when IBM is the CPC's service provider, IBM provides and maintains the remote, automated IBM Service Support System.

Note: If you are familiar with IBM service, you may have heard the IBM Service Support System referred to as RETAIN®.

The CPC's *remote service settings* control whether and how its support element uses remote service. When the CPC's remote service settings are customized for using remote service, the CPC's support element uses a feature called the *remote support facility (RSF)* to establish a remote connection through its *phone server* to your service provider's service support system. Whenever a connection is established during a support element operation, it can send information to the service support system or receive information from it.

Using remote service is optional, but has the following benefits:

- You can let the support element automatically report problems and get service through the service support system.
- You can use the service support system as a source for retrieving internal code changes.
- You can use the service support system as a destination for transmitting service data.

The remaining topics in this section describe these benefits in more detail and provide instructions for getting them by customizing the CPC's remote service settings.

Getting ready to report problems and get service

The support element automatically and continuously monitors itself and the central processor complex (CPC) for problems. If the support element detects a problem, it uses a knowledge-based expert system called *Problem Analysis* to automatically:

- Analyze the problem, attempt to determine its cause, and determine whether service is required to correct the problem.

- Issue a hardware message to notify you of the problem. Information provided with the message includes a detailed description of the problem and instructions for correcting it or calling for service.
- Send problem information for optical errors to a designated console, if available, for additional analysis.

If service is required to correct the problem, it is your responsibility to contact your service provider, report the problem, and request service to correct it. You can do this manually by calling your service provider on the telephone and using the information provided with the hardware message to describe the problem.

But if your service provider has an automated service support system for receiving and processing problem reports and service requests, you can report problems and request service automatically by customizing the support element's remote service settings as follows:

- *Enable* remote service to allow the support element to establish remote connections through its *phone server* to your service provider's service support system.
- *Enable* automatic service calling to allow the support element to automatically report problems and get service through the remote connection to the service support system.

If the support element detects a problem while remote service and automatic service calling are enabled, the support element uses its phone server to transmit the problem report and service request to the service support system, which receives and processes them according to the service policies of your service provider. For example, when your service provider is IBM, the IBM Service Support System analyzes your problem report, then forwards it accordingly:

- When the cause of the problem is known, the IBM Service Support System forwards the problem report to a service representative, who is then sent to your location with the instructions, parts list, and other information necessary to correct the problem.
- When the cause of the problem is not yet known, the IBM Service Support System forwards the problem report to an IBM Support Center for further analysis.

To customize the support element for automatically reporting problems and getting service, see “Customizing remote service settings” on page 7-4 for instructions for enabling remote service *and* automatic service calling.

For more information about the support element's phone server and optical error analysis, respectively, see:

- “Providing modem services to the support element” on page 16-8.
- “Performing Problem Analysis of optical errors” on page 16-9.

Getting ready to retrieve internal code changes

Licensed internal code, referred to also as *internal code*, controls many of the operations available on a central processor complex (CPC) and its support element. IBM provides *internal code changes* to change the internal code of a CPC or its support element. Changing the internal code may be necessary to add new functions, improve existing functions, or correct problems.

IBM provides internal code changes by delivering them on an optical cartridge or diskette, and by making them available on the IBM Service Support System. Although the same internal code changes are available from each source, the most direct source is the IBM Service Support System. But you can use the IBM Service Support System as a source only by customizing, in advance, the CPC's remote service settings to *enable* remote service.

While remote service is enabled, the IBM Service Support System is *another* source for manually retrieving internal code changes; that is, optical cartridges and diskettes remain eligible sources. But if you intend to *schedule an operation* for retrieving internal code changes regularly and automatically, the IBM Service Support System is the only eligible source. So you must enable remote service before scheduling an operation for retrieving internal code changes.

To use the IBM Service Support System as a source for retrieving internal code changes, either manually or during a scheduled operation, see “Customizing remote service settings” on page 7-4 for instructions for enabling remote service.

Getting ready to transmit service data

Service data is a set of system information, such as program and event traces and storage dumps, collected by the support element of the central processor complex (CPC). When IBM is the service provider for your system, service data assists IBM in servicing it.

You can send service data to IBM either by copying it to an optical cartridge or diskette for delivery to IBM, or by transmitting it to IBM through a remote connection to the IBM Service Support System. Although the same service data is sent to IBM through each destination, the most direct destination is the IBM Service Support System. But you can use the IBM Service Support System as a destination only by customizing, in advance, the CPC's remote service settings to *enable* remote service.

While remote service is enabled, the IBM Service Support System is *another* destination for manually transmitting service data; that is, optical cartridges and diskettes remain eligible destinations. But if you intend to *schedule an operation* for transmitting service data regularly and automatically, the IBM Service Support System is the only eligible destination. So you must enable remote service before scheduling an operation for transmitting service data.

To use the IBM Service Support System as a destination for transmitting service data, either manually or during a scheduled operation, see “Customizing remote service settings” on page 7-4 for instructions for enabling remote service.

Customizing remote service settings

You can use the support element workplace to customize the remote service settings of the central processor complex (CPC). The settings control whether and how the CPC's support element uses the remote support facility (RSF) to establish a remote connection through its phone server to your service provider's service support system. Whenever a connection is established during a support element operation, it can send information to the service support system or receive information from it.

To customize remote service settings:

1. You must be logged on the support element in the system programmer or service representative user mode.
2. Open the **Task List** from the **Views** area.
3. Open **CPC Remote Customization** from the **Task List Work Area**.

   The CPC Remote Customization task list contains the **Remote Service** task that you will start.
4. Open **Groups** from the **Views** area.
5. Open the **CPC** group from the **Group Work Area**.
6. Drag and drop the CPC on the **Remote Service** task to start it.
7. Use the Customize Remote Service window to set the CPC's remote service settings.

   Use the online **Help** for more information about using the window to customize the settings.
8. To enable remote service:
   a. Mark the **Enable remote service** check box.

      The check box displays a check mark when you mark it. The check mark indicates you want to enable remote service, which allows the CPC's support element to establish remote connections to your service provider's remote service support system.

   b. Use the fields in the Product Service Support System group box to identify the telephone numbers with which the support element can establish a connection to the service support system.

   c. Use the fields in the Peripheral Product Service Support System group box to identify the telephone numbers with which the support element can establish a connection to the service support system, if available, managed by the service provider for the CPC's peripheral products.

   Move the cursor to any control and request help for more information about using the control. Press **F2** to request help for the window.
9. To enable automatic service calling, mark the **Authorize automatic service call reporting** check box.

   The check box displays a check mark when you mark it. The check mark indicates you want to enable automatic service calling, which allows the CPC's

support element to automatically report problems and get service through its remote connection to the service support system.

Move the cursor to the check box and request help for more information about using it. Press **F2** to request help for the window.

10. Select **Save** to save the settings and close the window.

Transmitting alerts to a SNA Problem Management focal point

Problem Management is a network management discipline for centralizing the management of problems that occur on systems in a systems network architecture (SNA) network. Rather than managing problems on the network's systems only locally, each system that supports Problem Management generates an SNA generic *alert* whenever it detects a problem, and transmits the alert to a system designated as the network's Problem Management *focal point* or *central site*. The focal point, rather than the system on which the problem occurred, handles the problem according to the site's problem management procedures. But typically, the focal point handles each problem completely, from problem determination and diagnosis, through recovery and resolution, to tracking and control.

If the central processor complex (CPC) is in a network of systems that includes a Problem Management focal point, you can use the support element workplace to customize the CPC's *Problem Management settings* to support generating and transmitting alerts to the focal point.

To customize Problem Management settings:

1. You must be logged on the support element in the system programmer or service representative user mode.
2. Open the **Task List** from the **Views** area.
3. Open **CPC Remote Customization** from the **Task List Work Area**.

   The CPC Remote Customization task list contains the **Problem Management** task that you will start.
4. Open **Groups** from the **Views** area.
5. Open the **CPC** from the **Groups Work Area**.
6. Drag and drop the CPC on the **Problem Management** task to start it.
7. Use the Customize Problem Management window to set the CPC's Problem Management settings.

   Use the online **Help** for more information about using the window to customize the settings.
8. To enable generating and transmitting alerts:
   a. Mark the **Enable alert generation** check box.

      The check box displays a check mark when you mark it. The check mark indicates you want to enable generating and transmitting alerts, which

allows the CPC's support element to establish remote connections to your Problem Management focal point.

b. Use the fields in the Focal Point Addressing group box to identify the local area network (LAN) address or telephone numbers with which the support element can establish a connection to the Problem Management focal point.

Move the cursor to any control and request help for more information about using the control. Press **F2** to request help for the window.

9. Select **Save** to save the settings and close the window.

Operating the system from a SNA Operations Management focal point

Operations Management is a network management discipline for centralizing the operation and administration of systems in a systems network architecture (SNA) network. Rather than operating the network's systems only locally, each system that supports Operations Management is authorized to be operated also from a system designated as the network's Operations Management *focal point* or *central site*. Operating a system from the focal point is conducted by sending commands to the system. Monitoring a system from the focal point is conducted by sending queries and receiving alerts from the system. For more information about Operations Management, see *Managing Your Processors*, GC38-0452.

If the central processor complex (CPC) is in a network of systems that includes an Operations Management focal point, you can use the support element workplace to customize the CPC's *Operations Management settings* to support being operated from the focal point. That is, customize the Operations Management settings to authorize the CPC for receiving requests from the focal point and for transmitting reports to it.

To customize Operations Management settings:

1. You must be logged on the support element in the system programmer or service representative user mode.
2. Open the **Task List** from the **Views** area.
3. Open **CPC Remote Customization** from the **Task List Work Area**.

   The CPC Remote Customization task list contains the **Operations Management** task that you will start.
4. Open **Groups** from the **Views** area.
5. Open the **CPC** group from the **Groups Work Area**.
6. Drag and drop the CPC on the **Operations Management** task to start it.
7. Use the Customize Operations Management window to set the CPC's Operations Management settings.

   Use the online **Help** for more information about using the window to customize the settings.
8. To enable receiving requests and transmitting reports:

   a. Mark the **Enable Operations Management** check box.

      The check box displays a check mark when you mark it. The check mark indicates you want to enable receiving requests and transmitting reports,

which allows the CPC's support element to establish remote connections to your Operations Management focal point.

b. Use the fields in the Focal Point Addressing group box to identify the local area network (LAN) address or telephone numbers with which the support element can establish a connection to the Operations Management focal point.

Move the cursor to any control and request help for more information about using the control. Press **F2** to request help for the window.

9. Select **Save** to save the settings and close the window.

Operating the system from a remote console

A *remote console* is a facility that allows operation of a support element console and its central processor complex (CPC) from a remote location. See Appendix A, “Remote Operations” on page A-1 for:

- More information about remote console operations.
- Instructions for customizing a support element console to support operating it and its CPC from remote consoles.
- Instructions for installing and customizing remote consoles.

Assisting service providers with contacting your company

Typically, if the service support system cannot determine the cause of the problem, it forwards the problem report and service request to a support center for further analysis by service personnel. The analysis may require a service representative to contact your company, preferably the person responsible for the CPC at the site where the CPC is located. So problem reports and service requests transmitted from the CPC's support element to the service support system also include such information.

You can use the support element workplace to customize information, referred to here as *account information*, that the CPC's service providers can use to contact your company and the person responsible for the CPC.

To customize account information:

1. You must be logged on the support element in the system programmer or service representative user mode.
2. Open the **Task List** from the **Views** area.
3. Open **CPC Remote Customization** from the **Task List Work Area**.

   The CPC Remote Customization task list contains the **Account Information** task that you will start.
4. Open **Groups** from the **Views** area.
5. Drag and drop the CPC on the **Account Information** task to start it.

6. Use the first page of the Customize Account Information notebook, the Company page, to customize the account information.

   Use the online **Help** for more information about using the page to customize the information.

7. Select **Save** to save the information and close the notebook.

Setting modem parameters for specialized dialing

To successfully dial the telephone numbers of remote systems, the phone server's modem requires additional, specialized dialing parameters:

Dial string prefix
A string of information that controls how the phone server's modem dials telephone numbers for the support element.

The default dial string prefix is CRN, which indicates no calling station identifier.

Calling station identifier
For a support element customized to be its own phone server, the calling station identifier is the complete telephone number of the support element's modem. Typically it is needed only while using the CRI dial string prefix.

The CRI dial string prefix and a calling station identifier are required in some countries.

See “Providing modem services to the support element” on page 16-8, if necessary, to determine whether the support element is its own phone server or uses a Hardware Management Console as a phone server. Then you can use the support element workplace to customize the specialized dialing parameters the phone server's modem uses to dial telephone numbers for the support element.

To customize dialing parameters for the phone server's modem:

1. You must be logged on the support element in the system programmer or service representative user mode.
2. Open the **Task List** from the **Views** area.
3. Open **CPC Remote Customization** from the **Task List Work Area**.

   The CPC Remote Customization task list contains the **Customize Automatic Dialing** task that you will start.

4. Open **Groups** from the **Views** area.
5. Open the **CPC** group from the **Groups Work Area**.
6. Drag and drop the CPC on the **Customize Automatic Dialing** task to start it.
7. Use the Customize Automatic Dialing window to customize the dialing parameters for the phone server's modem:
   - Use the **Dial string prefix** field to customize the dial string prefix the phone server's modem uses to dial telephone numbers for a support element.

- If the dial string prefix requires using a calling station identifier, use the **Calling station identifier** field to customize the telephone number of a support element's modem, if the support element is customized to be its own phone server.

  Note: Only Hardware Management Consoles can be phone servers for integrated support elements. If the support element's dial string prefix requires using a calling station identifier, and a Hardware Management Console is the support element's phone server, then the Hardware Management Console's calling station identifier is used instead.

Use the online **Help** for more information about using the window to customize the parameters.

8. Select **Save** to save the information and close the window.

Chapter 8. System testing, problem determination, and service

This section describes tasks from the **Service** task list you can use to test, report problems, and get service for the central processor complex (CPC).

Enabling service status

You can enable this task to allow a service representative to perform service tasks on the CPC or support element. Many of the CPC service tasks require that the CPC is first placed in service status. Repair and verify, for example, cannot be run on a CPC until that CPC is placed in service status.

The background of the support element workplace also displays **Service** (rather than S/390) while service status is enabled.

Service status also prevents messages indicating the loss of communication to the support element from displaying while the support element is powered off or during licensed internal code load.

To enable or disable service status:

1. Open the **Task List** from the **Views** area.
2. Open **Service** from the **Task List Work Area**.

   The Service task list contains the **Service Status** task that you will start.
3. Open **Groups** from the **Views** area.
4. Open the **CPC** group from the **Groups Work Area**.
5. Drag and drop the CPC on the **Service Status** task to start it.

   This displays the **Service Status** window.
6. Set service status to enable or disable.

Use the online **Help** for more information about using the window to set service status.

Testing the CPC hardware

Checkout tests are test programs typically run by service representatives to test the central processor complex (CPC) hardware and determine whether it is operating correctly.

Running checkout tests will require all CPC resources. That is, you will not be able to run other control programs or operating systems of the CPC while checkout tests are running.

Checkout tests are fully automated. Once you start them, they require no input or interaction until they are completed. Checkout tests begin with a power-on reset of the CPC in the S/390 operating mode and with the diagnostic (D0) input/output configuration data set (IOCDS), followed by loading and running the test programs.

Note: The power-on reset cancels all operations in progress on the CPC, and loading the checkout tests replaces the CPC's current control program or operating system. When the checkout tests are completed, activate the CPC to perform a power-on reset and load the previous control program or operating system.

Checkout tests include testing the CPC's processors and storage, and running internal wrap tests on its channels.

Note: Other hardware in the CPC's input/output (I/O) configuration, such as drivers, receivers, interface cables, control units, and I/O devices, are *not* tested.

To start checkout tests:

1. Open the **Task List** from the **Views** area.
2. Open **Service** from the **Task List Work Area**.

   The Service task list contains the **Checkout Tests** task that you will start.
3. Open **Groups** from the **Views** area.
4. Open the **CPC** group from the **Groups Work Area**.

   Note: Starting checkout tests on a CPC can be considered disruptive. If the CPC is locked, unlock it. See “Setting lockout for disruptive tasks on an object” on page 2-15.
5. Drag and drop the CPC on the **Checkout Tests** task to start it.

   This displays the Checkout Tests window.
6. Select the **Run test** push button from the **Checkout Tests** window to start the checkout tests.

   When checkout tests are completed, the results are displayed. The results provide information about errors that were detected or problems that occurred, if any, during testing.

Reporting problems and getting service

The support element automatically and continuously monitors itself and the central processor complex (CPC) for problems. If the support element detects a problem, it uses a knowledge-based expert system called *Problem Analysis* to automatically:

- Analyze the problem, attempt to determine its cause, and determine whether service is required to correct the problem.
- Issue a hardware message to notify you of the problem. Information provided with the message includes a detailed description of the problem and instructions for correcting it or calling for service.

If service is required to correct the problem, it is your responsibility to contact your service provider, report the problem, and request service to correct it. You can do this manually by calling your service provider on the telephone and using the information provided with the hardware message to describe the problem.

But if your service provider has an automated service support system for receiving and processing problem reports and service requests, you can report problems and request service automatically by customizing the support element's remote service settings.

Settings for reporting problems and getting service automatically

If your service provider has an automated service support system for receiving and processing problem reports and service requests, you can report problems and request service automatically by customizing the support element's remote service settings as follows:

- *Enable* remote service to allow the support element to establish remote connections to your service provider's service support system.
- *Enable* automatic service calling to allow the support element to automatically report problems and get service through its remote connection to the service support system.

To customize the support element for automatically reporting problems and getting service, see “Customizing remote service settings” on page 7-4 for instructions for enabling remote service *and* automatic service calling.

Using hardware messages to report problems and get service

The central processor complex (CPC) and Support Element Console Application send messages to the support element to notify you of significant events that involve or affect the use of CPC hardware and licensed internal code. The messages are referred to as *hardware messages*. Promptly view hardware messages as the support element receives them to determine their source and subject. See “Recognizing when hardware messages were received” on page 3-6 for more information about the support element's hardware message indicators.

Problem Analysis issues hardware messages to notify you of problems detected by the support element. A hardware message issued by Problem Analysis typically is a brief, general description of a problem with hardware or licensed internal code. But information provided with the message includes a detailed description of the problem and instructions for either correcting the problem or reporting the problem and getting service.

Problem Analysis issues the hardware messages regardless of whether the support element's remote service settings are customized for automatically reporting problems and getting service. The remote service settings determine only how problem reports and service requests are transmitted:

- If remote service and automatic service calling are enabled, and if Problem Analysis determines service is required to correct a problem, it automatically transmits a problem report and service request to your service provider.
- Otherwise, if remote service or automatic service calling is not enabled, you must use the hardware message issued by Problem Analysis to report the problem and get service.

To use a hardware message to report a problem and get service:

1. Locate the task in the task list on the right side of the workplace. Any task list contains the **Hardware Messages** that you will start.
2. Open **Groups** from the **Views** area.
3. Open the **CPC** group from the **Groups Work Area**.
4. Drag and drop the CPC on the **Hardware Messages** task to start it.

   This opens the Hardware Messages notebook. Its page lists the CPC's hardware messages, and it provides push buttons for working with them.

   Use the online **Help** for more information to view and delete hardware messages.
5. Select the message that describes the problem for which you want more details, then select the **Details** push button.

   For hardware messages issued by Problem Analysis, this opens a Problem Analysis window that displays the message details.
6. Read the information and follow the directions on the Problem Analysis window to determine what action to take in response to the message.
7. If service is required to correct a problem, a Problem Analysis window includes a **Request service** push button. Select the push button to report the problem to your service provider and to request service. The support element's remote service settings determine how the service request is made:
   - If remote service is enabled, requesting service transmits a problem report and service request to your service provider's automated service support system.
   - Otherwise, if remote service is not enabled, requesting service displays a window that provides all the information you need to call your service provider on the telephone, describe the problem, and request service.

Starting Problem Analysis manually for suspected problems

The support element starts Problem Analysis automatically only upon detecting a problem. But while the support element provides very comprehensive error detection, if it does not detect a problem you suspect is affecting the central processor complex (CPC) or support element, you can use the support element workplace to start Problem Analysis manually.

To start Problem Analysis manually:

1. Open the **Task List** from the **Views** area.
2. Open **Service** from the **Task List Work Area**.

   The Service task list contains the **Perform Problem Analysis** task that you will start.
3. Open **Groups** from the **Views** area.
4. Open any group that contains the CPC from the **Groups Work Area**.
5. Drag and drop the CPC on the **Perform Problem Analysis** task to start it.

6. Use the Perform Problem Analysis window to start Problem Analysis manually.

   Problem Analysis will issue a hardware message to notify you if it identifies a problem.

Reporting and getting service manually for suspected problems

Problem Analysis provides the means for reporting a problem and requesting service only if it identifies the problem and determines service is required to correct the problem. But while Problem Analysis provides very comprehensive problem identification and determination, if it does not identify or does not determine service is required for a problem you suspect is affecting the central processor complex (CPC) or support element, you can use the support element workplace to report the problem and request service anyway, independently of the results of Problem Analysis.

To report a problem and request service independently of Problem Analysis:

1. Open the **Task List** from the **Views** area.
2. Open **Service** from the **Task List Work Area**.

   The Service task list contains the **Report a Problem** task that you will start.
3. Open **Groups** from the **Views** area.
4. Open the **CPC** group from the **Groups Work Area**.
5. Drag and drop the CPC on the **Report a Problem** task to start it.
6. Use the Report a Problem window to:

   a. Test if problem reporting is working, or

   b. Describe the problem and request service to correct it.

   Use the online **Help** for more information about using the window to report the problem and request service.

Sending service data to IBM

Service data is a set of system information, such as program and event traces and storage dumps, collected by the support element of the central processor complex (CPC). When IBM is your service provider for the CPC, service data assists IBM in servicing it.

Sending service data to IBM is necessary only when service data is requested by IBM, usually through either your service representative or IBM Support Center. Typically, IBM will request service data after a problem is reported if analyzing the service data is necessary to determine the cause of the problem.

You can send service data to IBM either by copying it to an optical cartridge or diskette for delivery to IBM, or by transmitting it to IBM through a remote connection to the IBM Service Support System.

Note: Although the same service data is sent to IBM through each destination, the most direct destination is the IBM Service Support System. But you can use the IBM Service Support System as a destination only by customizing,

in advance, the CPC's remote service settings to *enable* remote service. See “Customizing remote service settings” on page 7-4 for instructions for enabling remote service.

To send service data to IBM:

1. Open the **Task List** from the **Views** area.
2. Open **Service** from the **Task List Work Area**.

   The Service task list contains the **Transmit Service Data** task that you will start.
3. Open **Groups** from the **Views** area.
4. Open the **CPC** group from the **Groups Work Area**.
5. Drag and drop the CPC on the **Transmit Service Data** task to start it.
6. Use the Transmit Service Data window, as directed by your service representative or IBM Support Center, to select the service data requested by IBM.

   Use the online **Help** for more information about using the window to select service data and send it to IBM.

Dumping data in LPAR or coupling facility mode

Most service data is collected and stored automatically by the support element of the central processor complex (CPC). This includes logical partition dump data and coupling facility logical partition dump data.

Logical partition dump data is control area information that is automatically collected and stored if logical partition errors are detected while the CPC is operating in logically partitioned (LPAR) mode. Collecting and storing information is often referred to as *dumping data*.

Likewise, *coupling facility logical partition dump data* is control area information that is automatically collected and stored if coupling facility logical partition errors are detected while a logical partition is operating in coupling facility mode.

Like other types of service data, logical partition dump data and coupling facility logical partition dump data assist IBM in servicing the CPC. And like other types of service data, sending dump data to IBM is necessary only when dump data is requested by IBM.

But if the dump data requested by IBM is not available, or if it is available but was not dumped recently, you can manually dump the data first, then send it and any other requested service data to IBM.

Note: If you are not certain whether dump data is already stored on the support element, or whether it was dumped recently, you can use the **Delete LPAR Dump Data** task to check. Starting the task displays a window lists the types of dump data, if any, already stored on the support element, and displays the time and date the data was dumped. See “Deleting dump data” on page 8-7 for instructions for starting the task. After you've checked

the type, time, and date of previously dumped data, you will be able to cancel the task *without* deleting the previously dumped data.

To manually dump data in LPAR or coupling facility mode:

1. To dump logical partition dump data, the CPC must be activated in LPAR mode.
2. To dump coupling facility logical partition dump data, the CPC must be activated in LPAR mode, and a logical partition must be activated in coupling facility mode.
3. You must be logged on the support element in the advanced operator, system programmer, or service representative user mode.
4. Open the **Task List** from the **Views** area.
5. Open **Service** from the **Task List Work Area**.

   The Service task list contains the **Dump LPAR Data** task that you will start.
6. To dump logical partition dump data, locate the CPC:
   a. Open **Groups** from the **Views** area.
   b. Open the **CPC** group from the **Groups Work Area**.

      This open the CPC Work Area. The area contains the target CPC.
7. To dump coupling facility logical partition dump data, locate the coupling facility logical partition.
   a. Open **Groups** from the **Views** area.
   b. Open the **Images** group from the **Groups Work Area**.

      This open the Images Work Area. The area contains the target coupling facility logical partition.
8. Drag and drop the target object on the **Dump LPAR Data** task to start it.

   This opens the dump window for the target object.

   Note: If a message notifies you that dump data is already stored on the support element, you must delete it before you can manually perform another dump. For more information and instructions, see “Deleting dump data.”
9. Use the window's controls to select the type of dump you want to perform, then select the **OK** push button to start the dump.

Deleting dump data

Dump data remains stored on the support element until it is either:

- Replaced by new dump data during an automatic dump.
- Deleted manually.

Ordinarily, you will not need to delete dump data manually. Deleting dump data is necessary only if the dump data prevents you from manually dumping new data:

- If a logical partition data dump is already stored on the support element, you must delete it before you can manually dump new logical partition data.
- If two coupling facility logical partition data dumps are already stored on the support element, you must delete at least one of them before you can manually dump new coupling facility logical partition data.

Note: Starting the task for manually deleting dump data is useful also to check the types of dump data, if any, already stored on the support element, and to check the time and date the data was dumped. But after you've checked the type, time, and date of previously dumped data, cancel the task to end it *without* deleting the previously dumped data.

To manually delete dump data:

1. You must be logged on the support element in the advanced operator, system programmer, or service representative user mode.
2. Open the **Task List** from the **Views** area.
3. Open **Service** from the **Task List Work Area**.

   The Service list contains the **Delete LPAR Dump Data** task that you will start.
4. Open **Groups** from the **Views** area.
5. Open the **CPC** group from the **Groups Work Area**.
6. Drag and drop the CPC on the **Delete LPAR Dump Data** task to start it.
7. Use the window's controls to select the types of dump data you want to delete, then select the **Delete** push button to delete them.

   Otherwise, if you only wanted to check the type, time, and date of previously dumped data, select the **Cancel** push button to end the task *without* deleting the previously dumped data.

Dumping Emulated I/O Data

Emulated I/O subsystem data is automatically collected to determine when something goes wrong with the emulated I/O subsystem. IBM can use this information to determine the problem.

If the dump data requested by IBM is lost or not available, or if it is available but was not dumped recently, you can manually dump data first, then send it and any other requested service data to IBM. This task manually creates a dump of the emulated I/O subsystem data, including control blocks and device manager data.

To manually dump emulated I/O data:

1. You must be logged on the support element in the advanced operator, system programmer, or service representative user mode.

2. Open the **Task List** from the **Views** area.
3. Open **Service** from the **Task List Work Area**.

   The Service task list contains the **Dump Emulated I/O Data** task that you will start.
4. Open **Groups** from the **Views** area.
5. Open the **CPC** group from the **Groups Work Area**.

   This opens the CPC Work Area. The area contains the target CPC.
6. Drag and drop the target object on the **Dump Emulated I/O Data** task to start it.

   This opens the dump window for the target object.

   Note: If a message notifies you that dump data is already stored on the support element, you must delete it before you can manually perform another dump. For more information and instructions, see "Deleting Emulated I/O Dump Data."
7. Use the window's controls to select the type of dump you want to perform, then select the **OK** push button to start the dump.

Deleting Emulated I/O Dump Data

Emulated I/O dump data remains stored on the support element until it is either:

- Replaced by new dump data during an automatic dump.
- Deleted manually.

Note: Starting the task for manually deleting dump data is useful also to check the types of dump data, if any, already stored on the support element, and to check the time and date the data was dumped. But after you've checked the type, time, and date of previously dumped data, cancel the task to end it *without* deleting the previously dumped data.

To manually delete emulated I/O dump data:

1. You must be logged on the support element in the advanced operator, system programmer, or service representative user mode.
2. Open the **Task List** from the **Views** area.
3. Open **Service** from the **Task List Work Area**.

   The Service list contains the **Delete Emulated I/O Dump Data** task that you will start.
4. Open **Groups** from the **Views** area.
5. Open the **CPC** group from the **Groups Work Area**.
6. Drag and drop the CPC on the **Delete Emulated I/O Data** task to start it.
7. Use the window's controls to select the types of dump emulated I/O data you want to delete, then select the **Delete** push button to delete them.

Otherwise, if you only wanted to check the type, time, and date of previously dumped data, select the **Cancel** push button to end the task *without* deleting the previously dumped data.

Keeping records of problems and service

The support element automatically keeps records of problem reports and service requests. Each record, referred to simply as a *problem*, includes detailed information about the problem, and indicates whether the service required to correct the problem is still pending or already completed.

A problem is *opened* when either:

- Problem Analysis determines service is required to correct a problem detected by the support element.
- A console operator uses the **Report a Problem** task to report a suspected problem not detected by the support element.

Collectively, the problem and service information is referred to as the *service history* of the central processor complex (CPC).

Viewing the CPC's service history

You can use the support element workplace to display the service history of the central processor complex (CPC).

To view the CPC's service history:

1. Open the **Task List** from the **Views** area.
2. Open **Service** from the **Task List Work Area** area.

   The Service task list contains the **Service History** task that you will start.
3. Open **Groups** from the **Views** area.
4. Open the **CPC** group from the **Groups Work Area**.

   This open the CPC Work Area. The area contains the target CPC.
5. Drag and drop the CPC on the **Service History** task to start it.

   Use the online **Help** for more information about the problem and service information on it.

Chapter 9. LPAR mode operations

This section describes the tasks from the **CPC Operational Customization** task list for operating logical partitions.

Changing how logical partitions operate: alternatives to activation

The operational capabilities and characteristics of the central processor complex (CPC) and its logical partitions are established by the activation profiles used to activate them. Ordinarily, after the CPC is activated, changing its operational capabilities and characteristics requires opening and customizing a reset profile, and then using the profile to activate the CPC again. Likewise, after the CPC is activated in logically partitioned (LPAR) mode, changing the operational capabilities and characteristics of its logical partitions requires opening and customizing their image profiles, and then using the profiles to activate the logical partitions.

But the following tasks on the support element workplace allow changing some of the operational capabilities and characteristics of the CPC and logical partitions *without* opening their activation profiles or activating them:

Change LPAR Security
Use this task to review or change the settings that determine the extent of interaction between logical partitions that can be activated on the CPC.

Change LPAR Controls
Use this task to review or change the settings that determine how processor resources are assigned to, used by, and managed for logical partitions that can be activated on the CPC.

Change LPAR Cryptographic Controls
Use this task to review or change the settings that determine how logical partitions use the cryptographic functions of the Cryptographic Coprocessor feature.

Logical partition security

The settings that determine the extent of interaction between logical partitions that can be activated on the central processor complex (CPC) are referred to here as *security settings*.

A logical partition's security settings are:

Performance data control
This setting controls whether a logical partition has global access to performance data.

Input/output configuration control
This setting controls whether a logical partition can change the input/output (I/O) configuration of the CPC on which it is activated.

Cross partition authority
This setting controls whether a logical partition can issue a subset of control program instructions to other logical partitions activated on the same CPC.

Logical partition isolation
This setting controls whether a logical partition has exclusive use of its reconfigurable channel paths.

A logical partition's initial security settings are established by the activation profile used to activate the logical partition. See the following topics for more information about customizing activation profiles for establishing a logical partition's initial security settings:

- "Getting ready to operate the system: customizing activation profiles" on page 6-1
- Tips for activating logical partitions:
  - "Controlling access to performance data" on page 6-33
  - "Controlling I/O configuration changes" on page 6-33
  - "Authorizing control of other logical partitions" on page 6-34
  - "Controlling use of reconfigurable channel paths" on page 6-35

Changing logical partition security

You can use the support element workplace to start the task for reviewing or changing the security settings of logical partitions that can be activated on the central processor complex (CPC).

To review or change logical partition security settings:

1. You must be logged on the support element in the system programmer user mode, and the CPC must be activated in logically partitioned (LPAR) mode.
2. Open the **Task List** from the **Views** area.
3. Open **CPC Operational Customization** from the **Task List Work Area**.

   The CPC Operational Customization task list contains the **Change LPAR Security** task that you will start.
4. Open **Groups** from the **Views** area.
5. Locate the **CPC** group from the **Groups Work Area**.

   Note: Changing logical partition security settings on a CPC can be considered disruptive. If the CPC is locked, unlock it. See "Setting lockout for disruptive tasks on an object" on page 2-15.
6. Drag and drop the CPC on the **Change LPAR Security** task to start it.

   This displays the Change Logical Partition Security window. The window lists the logical partitions that can be activated on the CPC and displays check boxes that indicate their current security settings:

   - Performance data control
   - Input/output configuration control
   - Cross partition security
   - Logical partition isolation

Move the cursor to any check box and use the Online **Help** for more information about what its current setting means. Press **F2** to request help for the window.

7. Use the check boxes to change the logical partition's security settings, then select a push button to indicate what you want to do with the new settings.

   Move the cursor to any check box or push button and use the Online **Help** for more information about using it to change security settings. Press **F2** to request help for the window.

   Tips for supporting specific applications:

   - Dynamic I/O configuration: Although more than one logical partition can run an application that supports dynamic I/O configuration, you should allow using only one logical partition to dynamically change the I/O configuration. The I/O configuration control setting of the logical partition you choose must display a check mark. The I/O configuration control setting of all other logical partitions should be blank.
   - Automatic reconfiguration facility (ARF): To use a logical partition for running an application that supports the ARF, its cross partition authority setting must display a check mark.

Logical partition controls

The settings that determine how processor resources are assigned to, used by, and managed for logical partitions that can be activated on the central processor complex (CPC) are referred to here as *control settings*. More specifically, control settings determine:

- Whether logical partitions are assigned dedicated or shared processor resources.
- How each logical partition activated with shared processor resources shares them with other logical partitions activated with shared processor resources.
- How the CPC manages logical partitions' use of shared processor resources.

Both the CPC and its logical partitions have control settings. A logical partition's control settings apply to it only. The CPC's control settings apply to all of its logical partitions. The control settings are:

Logical processor assignment
: These logical partition settings control how many logical processors are assigned to the logical partition, and how they are assigned as either dedicated or shared processor resources.

Processor running time
: These CPC settings control how its logical partition's processor running time is determined. The processor running time, referred to also as a timeslice, is the amount of continuous time allowed for each logical partition's logical processors to perform jobs on shared central processors.

The initial control settings of the CPC and each logical partition are established by the activation profiles used to activate them. See the following topics for more information about customizing activation profiles for establishing initial control settings:

- “Getting ready to operate the system: customizing activation profiles” on page 6-1
- “Assigning logical processors” on page 6-27
- “Setting processor running time” on page 6-21

Changing logical partition controls

You can use the support element workplace to start the task for reviewing or changing the control settings of the central processor complex (CPC) and the logical partitions that can be activated on it.

To review or change control settings:

1. You must be logged on the support element in the system programmer user mode, and the CPC must be activated in logically partitioned (LPAR) mode.
2. Open the **Task List** from the **Views** area.
3. Open **CPC Operational Customization** from the **Task List Work Area**.

   The CPC Operational Customization task list contains the **Change LPAR Controls** task that you will start.
4. Open **Groups** from the **Views** area.
5. Locate any group that contains the CPC from the **Groups Work Area**.

   Note: Changing logical partition control settings on a CPC can be considered disruptive. If the CPC is locked, unlock it. See “Setting lockout for disruptive tasks on an object” on page 2-15.
6. Drag and drop the CPC on the **Change LPAR Controls** task to start it.

   This displays the Change Logical Partition Controls window. The window lists the logical partitions that can be activated on the CPC and displays check boxes, entry fields, and other controls that indicate their current control settings:

   - Each logical partition's settings for logical processor assignment, including the number of logical processors assigned to each logical partition, and how they are assigned as either dedicated or shared processor resources.
   - The CPC's settings for processor running time.

   Move the cursor to any control and use the online **Help** for more information about what its current setting means. Press **F2** to request help for the window.
7. Use the controls to change the control settings of the logical partitions or the CPC, then select a push button to indicate what you want to do with the new settings.

   Move the cursor to any control or push button and use the Online **Help** for more information about using it to change control settings. Press **F2** to request help for the window.
8. Use the controls to change:

   - One or more logical partition's settings for how logical processors are assigned as either dedicated or shared processor resources.

- The CPC's settings for processor running time.

Then select a push button to indicate what you want to do with the new settings.

Move the cursor to any control or push button and use the Online **Help** for more information about using it to change control settings. Press **F2** to request help for the window.

Logical partition cryptographic controls

The settings that determine how logical partitions use the cryptographic functions of the Cryptographic Coprocessor feature are referred to here as *cryptographic controls*.

A logical partition's cryptographic controls are:

Cryptographic coprocessor assignment
This setting controls which cryptographic coprocessors, if any, are assigned to the logical partition.

Cryptographic domain index (CDX) numbers
These settings identify the control domains and usage domains the logical partition can use.

Public key algorithm (PKA) facility setting
This setting controls whether the logical partition can use the public key algorithm (PKA) facility of its assigned cryptographic coprocessors.

Cryptographic function settings
These settings control whether and how the logical partition can use the cryptographic functions of its assigned cryptographic coprocessors.

A logical partition's initial cryptographic controls are established by the activation profile used to activate the logical partition. See the following topics for more information about customizing activation profiles for establishing a logical partition's initial cryptographic controls:

- “Getting ready to operate the system: customizing activation profiles” on page 6-1
- “Using the Cryptographic Coprocessor feature” on page 6-28

For more information about the Cryptographic Coprocessor feature, see “The Cryptographic Coprocessor feature” on page 10-12.

Changing logical partition cryptographic controls

You can use the support element workplace to start the task for reviewing or changing the cryptographic controls of logical partitions that can be activated on the central processor complex (CPC).

Note: Cryptographic coprocessor assignment CDX numbers cannot be changed dynamically, but you can use this task to review each logical partition's current settings.

To review or change cryptographic settings:

1. The Cryptographic Coprocessor feature must be installed.
2. The CPC must be activated in logically partitioned (LPAR) mode.
3. At least one activated logical partition must have at least one cryptographic coprocessor assigned to it.
4. You must be logged on the support element in the system programmer user mode.
5. Open the **Task List** from the **Views** area.
6. Open **CPC Operational Customization** from the **Task List Work Area**.

   The CPC Operational Customization task list contains the task that you will start. **Change LPAR Cryptographic Controls**.
7. Open **Groups** from the **Views** area.
8. Locate any group that contains the CPC from the **Groups Work Area**.

   Note: Changing cryptographic controls on a CPC can be considered disruptive. If the CPC is locked, unlock it. See “Setting lockout for disruptive tasks on an object” on page 2-15.
9. Drag and drop the CPC on the **Change LPAR Cryptographic Controls** task to start it.

   This displays the Change LPAR Cryptographic Controls notebook. The notebook includes a page for each logical partition that can be activated on the CPC. Each page displays check boxes that indicate the logical partition's current cryptographic controls.

   Move the cursor to any check box and use the online **Help** for more information about what its current setting means. Press **F2** to request help for the window.
10. Use the check boxes to change the logical partition's cryptographic controls, then select a push button to indicate what you want to do with the new settings.

    Move the cursor to any check box or push button and use the Online **Help** for more information about using it to change cryptographic controls. Press **F2** to request help for the window.

    Notes:

    a. If you are using the Integrated Cryptographic Service Facility (ICSF), see “Using the Integrated Cryptographic Service Facility” for additional tips for dynamically changing cryptographic controls.

    b. If you are using a Trusted Key Entry (TKE) workstation to manage cryptographic keys, see “Using the Trusted Key Entry (TKE) feature” on page 9-7 for additional tips for dynamically changing cryptographic controls.

Using the Integrated Cryptographic Service Facility (ICSF)***:*** The Integrated Cryptographic Service Facility/MVS (ICSF/MVS) is a program product that can use the Cryptographic Coprocessor feature to provide secure, high-speed cryptographic services in the OS/390 environment. If the central processor complex (CPC) is operating in logically partitioned (LPAR) mode, you can use ICSF/MVS cryptographic services for all logical partitions that are customized for using cryptographic coprocessors.

The cryptographic controls set for a logical partition determine whether it can use ICSF/MVS cryptographic services:

- Mark the **Enable public key algorithm (PKA) facility** check box to use the PKA services of ICSF/MVS for the logical partition.
- Mark the following check boxes to use ICSF basic operations, including clear key entry, for the logical partition:
  - **Enable cryptographic functions**
  - **Enable public key secure cable (PKSC) and integrated cryptographic service facility (ICSF)**

  A check box displays a check mark when you mark it.
- Mark the **Enable special security mode** check box to enable ICSF special security mode for the logical partition.

Using the Trusted Key Entry (TKE) feature: A Trusted Key Entry (TKE) workstation is an optional feature and part of a customized solution for using the Integrated Cryptographic Service Facility/MVS (ICSF/MVS) to manage cryptographic keys of a central processor complex (CPC) that has the Cryptographic Coprocessor feature installed and configured for using Data Encryption Standard (DES) and Public Key Algorithm (PKA) cryptographic keys. If the CPC is operating in logically partitioned (LPAR) mode, and one or more logical partitions are customized for using cryptographic coprocessors, you can use the TKE workstation to manage DES master keys, PKA master keys, and operational keys for all domains of each cryptographic coprocessor assigned to logical partitions defined to the TKE workstation as TKE hosts. Each logical partition using a domain managed through a TKE workstation connection to a TKE host is referred to here as a TKE target.

The cryptographic controls set for a logical partition determine whether it can be a TKE host or TKE target:

- For a TKE host logical partition:
  - Mark the following check boxes to use a TKE workstation connection to the TKE host logical partition for basic cryptographic key management operations:
    - **Enable cryptographic functions**
    - **Enable public key secure cable (PKSC) and integrated cryptographic service facility (ICSF)**
    - **Enable query signature controls**
    - **Enable query transport controls**

    A check box displays a check mark when you mark it.
  - Mark the **Enable modify authority** check box to use a TKE workstation connection to the TKE host logical partition for loading updated cryptographic keys for domains used by the host's TKE target logical partitions.

    Note: This setting can be enabled for only one active logical partition.
  - To use a TKE workstation to dynamically enable and disable special security mode for the domain used by the logical partition, special security mode must be enabled for the logical partition at the support element and

in the ICSF/MVS installation options data set. Mark the **Enable special security mode** check box to enable it at the support element.

- For a TKE target logical partition:
  - Mark the following check boxes to use a TKE workstation to manage cryptographic keys for the TKE target logical partition:
    - **Enable cryptographic functions**
    - **Enable public key secure cable (PKSC) and integrated cryptographic service facility (ICSF)**

    Mark the **Enable integrated cryptographic facility (ICRF) key entry** check box also to enable using the **Load to queue** pop-up menu choice at a TKE workstation to load master keys, personal identification numbers (PINs), or key encrypting keys (KEKs) for the domain used by the logical partition.

    A check box displays a check mark when you mark it.
  - To use a TKE workstation to dynamically enable and disable special security mode for the domain used by the logical partition, special security mode must be enabled for the logical partition at the support element and in the ICSF/MVS installation options data set. Mark the **Enable special security mode** check box to enable it at the support element.

Testing applications for the Year 2000

You can use the CPC's test sysplex for testing applications with the date and time kept by the Sysplex Test Datesource. For example, you can test applications for the year 2000 by setting the Sysplex Test Datesource to start at a year 2000 date and time.

While the CPC is operating in LPAR mode, you can set up a test sysplex of logical partitions that are synchronized with the Sysplex Test Datesource rather than the CPC's normal time reference. The Sysplex Test Datesource keeps time like a real TOD clock for the logical partitions in the test sysplex. The Change Logical Partition Sysplex Test Datesource window list indicates whether logical partitions are currently synchronized to the Sysplex Test Datesource. The logical partition synchronization settings are:

Partition Name
Displays the name of each logical partition defined in the active input/output configuration data set (IOCDS).

Currently Synchronized to Sysplex Test Datesource
Indicates whether logical partitions are currently synchronized to the Sysplex Test Datesource. *Yes* indicates the logical partition is synchronized to the Sysplex Test Datesource. *No* indicates the logical partition is not synchronized to the Sysplex Test Datesource, but is synchronized to the CPC's normal time reference. *Not activated* indicates the logical partition is not activated.

Synchronize to Sysplex Test Datesource on next activation of Partition
Use the check boxes in this column to set which logical partitions you want synchronized to the Sysplex Test Datesource the next time they are activated. A check mark indicates the logical partition will be synchronized to the sysplex Test Datesource the next time it is activated. An empty check box indicates

the logical partition will not be synchronized to the Sysplex Test Datesource the next time it is activated. It will be synchronized instead to the CPC's normal time reference.

The window also displays the Sysplex Datesource Starting Values. Use the **Date** and **Time** fields to type the date and time you want to set for the Sysplex Test Datesource. The fields initially display the date and time previously saved as starting values for the Sysplex Test Datesource. If there are no previously saved starting values, the default date and time (01/01/2000 00:00:00) is displayed instead. You can change the starting values to any date and time in the range from 01/01/1900 00:00:00 to 12/31/2040 23:59:59.

After setting the starting values for the Sysplex Test Datesource, it starts keeping time when you activate the first logical partition you want in the test sysplex. When you activate any other logical partitions you want in the sysplex, they are synchronized to the *current* date and time rather than its starting values. The Sysplex Test Datesource stops keeping time when all logical partitions in the test sysplex are deactivated. The current date and time of the Sysplex Test Datesource is not saved when it stops keeping time.

Note: If you have multiple CPCs, you can set up a test sysplex for each CPC, but a CPC's test sysplex *cannot* include logical partitions activated on other CPCs.

Setting the test sysplex before activation in LPAR mode:

If the CPC is activated in basic mode or if it is not activated, use the **Customize/Delete Activation Profiles** task to set which logical partitions you want synchronized to the Sysplex Test Datesource. Then, use the **Change Logical Partition Sysplex Test Datesource** task to set the starting date and time.

To customize the image profiles for the Sysplex Test Datesource:

1. You must be logged on the support element console in the system programmer user mode.
2. Open an activation profile customized for activating a CPC in LPAR mode.
3. Select the logical partition pages that you want in the test sysplex.
4. Select the **Participate in the Sysplex test datesource group** radio button in the Clock type assignment box in each partition page that you want in the test sysplex.
5. Select the **Save** push button.
6. Drag and drop the CPC on the **Change Logical Partition Sysplex Test Datesource**.

   This starts the task and displays the Change Logical Partition Sysplex Test Datesource window.
7. Set the starting date and time for the Sysplex Test Datesource.
8. Select the **Save** push button.
9. Activate the CPC in LPAR mode.
10. Activate the logical partitions you want synchronized to the new Sysplex Test Datesource.

    Use online **Help** to guide you through completion of this task.

Each logical partition's setting is saved in its image profile. New settings take effect the next time you activate the logical partition.

Setting the test sysplex after activation in LPAR mode:

If the CPC is already activated in LPAR mode and no logical partitions are currently synchronized to the Sysplex Test Datesource, then use the Change Logical Partition Sysplex Test Datesource window to:

- Set what logical partitions you want synchronized to the Sysplex Test Datesource.
- Set the starting date and time for the Sysplex Test Datesource.
- Save the settings.

1. To locate the task:
   a. You must be logged on the support element console in the system programmer user mode, and the CPC must be activated in LPAR mode.
   b. Open the **Task List** view on the support element workplace.
   c. Open **CPC Operational Customization**.
   d. Locate the **Change LPAR Sysplex Test Datesource** task.
2. To locate the CPC target:
   a. Open the **Groups** view on the support element workplace.
   b. Locate the CPC.
   c. Drag and drop the CPC on the **Change Logical Partition Sysplex Test Datesource**. This starts the task and displays the Change Logical Partition Sysplex Test Datesource window.
3. Check which logical partitions you want synchronized to the Sysplex Test Datesource.
4. Set the starting date and time for the Sysplex Test Datesource.
5. Select the **Save** push button.
6. Activate the logical partitions you want synchronized to the new Sysplex Test Datesource.

   Use online **Help** to guide you through completion of this task.

Each logical partition's setting is saved in its image profile. New settings take effect the next time you activate the logical partition.

Adding logical partitions to the test sysplex

If the logical partition is active, to add logical partitions to the test sysplex:

1. Deactivate the logical partitions from the normal time reference.
2. Drag and drop the CPC on the **Change Logical Partition Sysplex Test Datesource**.
3. Check which logical partitions you want added to Sysplex Test Datesource.
4. Select the **Save** push button.
5. Activate the logical partitions.

Removing logical partitions from the test sysplex

If the partition is active, to remove logical partitions from the test sysplex:

1. Deactivate the logical partitions to remove them from the test sysplex.

To activate the logical partitions and synchronize them to the CPC's normal time reference:

1. Drag and drop the CPC on the **Change Logical Partition Sysplex Test Datesource**.
2. Uncheck which logical partitions you do *not* want synchronized to the Sysplex Test Datesource.
3. Select the **Save** push button.
4. Activate the logical partitions.

   Each logical partition's setting is saved in its image profile. New settings take effect the next time you activate the logical partition.

Setting a new date and time for the test sysplex

To set a new date and time for the test sysplex:

1. Drag and drop the CPC on the **Change Logical Partition Sysplex Test Datesource**.
2. Set the new starting date and time for the Sysplex Test Datesource.
3. Select the **Save** push button.
4. Activate the logical partitions you want synchronized to the new Sysplex Test Datesource.
5. Deactivate all logical partitions that are currently synchronized to the current Sysplex Test Datesource.

Chapter 10. CPC configuration management

This section describes tasks from the **CPC Configuration** task list and some elements of the physical and logical configuration of the central processor complex (CPC). It also describes task you can use to get or change information that describes or defines the CPC configuration.

The CPC Configuration task list contains the tasks, referred to here as *CPC configuration tasks*. This section provides instructions for starting the tasks.

Getting information about the hardware configuration

Hardware configuration information stored on the support element of the central processor complex (CPC) is information about the CPC's frame and parts in the frame. Information about the frame includes the machine type, model number, and serial number of the frame's machine, and the CPC's location in the frame. The information for each part in the frame includes its:

- Location
- Custom card identifier (CCIN)
- Description
- Part number
- Serial number
- Engineering change (EC) number

You can use the support element workplace to display the hardware configuration information.

To view the hardware configuration:

1. You must be logged on the support element in the system programmer or service representative user mode.
2. Open the **Task List** from the **Views** area.
3. Open **CPC Configuration** from the **Task List Work Area**.

   The CPC Configuration task list contains the **View Hardware Configuration** task that you will start.
4. Open **Groups** from the **Views** area.
5. Open any group that contains the CPC from the **Groups Work Area**.
6. Drag and drop the CPC on the **View Hardware Configuration** task to start it.

   Information is displayed about the CPC's frame and lists the location, CCIN, and a description of each part in the frame.

   Use the online **Help** for more information about the display fields and list.

7. To display the part number, serial number, and EC number for a specific part, select the part from the list, then select the **Details** push button.

   This displays the selected part's detailed information on the Part Details window.

The I/O configuration

The input/output (I/O) configuration of the central processor complex (CPC) is the set of all I/O devices, control units, and channel paths available to the CPC. During each power-on reset of the CPC, an input/output configuration data set (IOCDS) is used to define the I/O configuration to the channel subsystem.

You must build an IOCDS and store it on the CPC's support element before you can use it during power-on reset to define the CPC's I/O configuration. You can build an IOCDS by using an input/output configuration program (IOCP):

- An IOCP may be available as a batch program with your operating system.

  For information about using the IOCP, see: *Input/Output Configuration Program User's Guide*, GC38-0401.

- A stand-alone IOCP also is available with the support element.

  For information about using the stand-alone IOCP, see: *Stand-Alone IOCP User's Guide*, GC38-0458.

Defining the I/O configuration using the stand-alone IOCP

You can use the support element workplace to start the stand-alone input/output configuration program (IOCP) available with the support element of the central processor complex (CPC).

To start the stand-alone IOCP:

1. You must be logged on the support element in the system programmer or service representative user mode.
2. Open the **Task List** from the **Views** area.
3. Open **CPC Configuration** from the **Task List Work Area**.

   The CPC Configuration task list contains the **Input/output (I/O) Configuration**. task that you will start.

4. Open **Groups** from the **Views** area.
5. Open the **CPC** group from the **Group Work Area**.
6. Drag and drop the CPC on the **Input/output (I/O) Configuration** task to start it.
7. Use the controls on the Input/Output Configuration window to use the stand-alone IOCP. It list the input/output configuration data sets (IOCDSs) currently stored on the CPC's support element.

Determining which CHPIDs are assigned to which channels

You can use the support element workplace to determine the type and location of channels in the hardware configuration of the central processor complex (CPC) and which channel path identifiers (CHPIDs) in the CPC's input/output (I/O) configuration are assigned to the channels.

To view the hardware configuration:

1. You must be logged on the support element in the system programmer or service representative user mode.
2. Open the **Task List** from the **Views** area.
3. Open **CPC Configuration** from the **Task List Work Area**.

   The CPC Configuration task list contains the **Hardware Configuration Details** task that you will start.
4. Open **Groups** from the **Views** area.
5. Open any group that contains the CPC from the **Groups Work Area**.
6. Drag and drop the CPC on the **Hardware Configuration Details** task to start it.

   The tree view of the System window displays a tree of icons that represent the following elements of the CPC's hardware and I/O configurations:

   - The CPC
   - The cages installed in the CPC
   - The CHPIDs assigned to channels installed in the cages.
7. Use the controls on the System window to open other views of the CPC's hardware and I/O configurations, and to get detailed information about them.

   Use the online **Help** for more information about opening other views and getting detailed information about the CPC's hardware and I/O configurations.

Hardware configuration upgrades and model conversions

Some central processor complex (CPC) configuration tasks support performing system upgrades and model conversions. Follow your normal order process for ordering an upgrade or model conversion for your system. Then use the CPC configuration tasks described in this section as needed during the order process and only at the direction of your IBM Support Center or IBM Product Engineering.

Vital Product Data

Vital Product Data (VPD) is information that describes the hardware configuration of a central processor complex (CPC). The VPD for a CPC:

- Identifies its frame and location in the frame, and itemizes its installed parts, engineering changes (ECs), and licensed internal code.
- Is stored on the CPC's support element.

- Is updated whenever the CPC configuration changes.

IBM uses VPD to process orders for upgrades and model conversions. Complete machine VPD must be transmitted to IBM immediately prior to ordering an upgrade or model conversion. But VPD should also be transmitted to IBM whenever a machine configuration changes.

Transmitting Vital Product Data to IBM

You can use the support element workplace to transmit Vital Product Data (VPD) to IBM.

You can transmit VPD to IBM either by copying it to a diskette for delivery to IBM, or by transmitting it to IBM through a remote connection to the IBM Service Support System.

Note: Although the same service data is sent to IBM through each destination, the most direct destination is the IBM Service Support System. But you can use the IBM Service Support System as a destination only by customizing, in advance, the CPC's remote service settings to *enable* remote service. See “Customizing remote service settings” on page 7-4 for instructions for enabling remote service.

To transmit VPD to IBM:

1. You must be logged on the support element in the system programmer or service representative user mode.
2. Open the **Task List** from the **Views** area.
3. Open **CPC Configuration** from the **Task List Work Area**.

   The CPC Configuration task list contains the **Transmit Vital Product Data** task that you will start.
4. Open **Groups** from the **Views** area.
5. Open the **CPC** group from the **Groups Work Area**.
6. Drag and drop the CPC on the **Transmit Vital Product Data** task to start it.

   The Transmit Vital Product Data to IBM lists the destinations that you can transmit VPD to IBM.
7. Select a destination from the Transmit Vital Product Data to IBM window, then select **OK** to use the selected destination for transmitting VPD to IBM.

   This displays one or more additional windows, depending on the destination you selected.
8. Follow the instructions on each subsequent window to complete the task.

   Use the online **Help** for more information for the controls on any window to use them to transmit VPD to IBM. Press **F2** to request help for the window.

The Internal Disk Subsystem Feature

The S/390 Multiprise 3000 Enterprise Server supports the internal disk subsystem feature. An *internal subsystem* emulates an external subsystem, but its hardware is located inside the same frame as the central processor complex (CPC).

A facility of the support element workplace provides tasks for monitoring, operating, and customizing the CPC's internal subsystems. The next topic provides instructions for opening the facility. It is followed by topics that describe the specific types of internal subsystems available and provide specific instructions for using the internal subsystem facility to work with them.

A service representative will perform all the tasks necessary to install the internal disk subsystem feature. Installing the internal disk subsystem includes:

- Installing the hardware.
- Using the support element workplace to configure the internal disk subsystem.

  Note: For more information and instructions for configuring the internal disk subsystem, see the *Internal Disk Subsystem User's Guide*, SA22-1025.

Working with internal subsystems

You can use the support element workplace to open a facility for monitoring, operating, and customizing the internal subsystems of the central processor complex (CPC).

To open the internal subsystem facility:

1. Open the **Task List** from the **Views** area.
2. Open **CPC Configuration** from the **Task List Work Area**.

   The CPC Configuration task list contains the **Internal Disk Subsystem Configuration** task that you will start.
3. Open **Groups** from the **Views** area.
4. Open the **CPC** group from the **Groups Work Area**.
5. Drag and drop the CPC on the **Internal Disk Subsystem Configuration** task to start it.

   The Internal Subsystem Configuration window lists the tasks available for working with the CPC's internal subsystems.
6. Select a task to choose the work you want to do.

   Move the cursor to any task and use the online **Help** for more information about it. Press **F2** to request help for the window.

CPC resources used by the internal disk subsystem

The operations performed by the internal disk subsystem are supported in part by the processing and storage resources of the central processor complex (CPC). The following CPC resources, allocated when a power-on reset of the CPC is performed, are used by the internal disk subsystem:

- Internal disk subsystem cache

  The *internal disk subsystem cache* is organized as a special S/390 storage area. It is used exclusively by the internal disk subsystem for intermediate storage of data. The amount of space allocated as internal subsystem cache decreases the amount of physical storage that is available for other types of storage, such as central storage, or expanded storage.

- Internal disk subsystem control blocks

  Internal disk subsystem control blocks, required for emulating external control units and devices, are allocated in the CPC's central storage (HSA) area.

- System assist processors (SAPs)

  Internal disk licensed internal code emulating external disk control units and devices executes on the Multiprise 3000 Enterprise Server's SAP.

Allocating the internal subsystem cache: The *internal subsystem cache* of the central processor complex (CPC) is a portion of the CPC's system storage that is reserved for the exclusive use of its internal subsystems for intermediate storage of data. The cache is allocated when a power-on reset of the CPC is performed.

Activating the CPC is the normal procedure for performing a power-on reset. You can customize the reset profile used to activate the CPC to set the internal subsystem cache size. The Storage page of a reset profile provides controls for setting the cache size. See “Allocating storage” on page 6-12 for more information about customizing the Storage page of a reset profile.

You can perform a power-on reset of the CPC without activating it, but it should be done only as an error recovery procedure. You can customize the information used to perform the power-on reset to set the internal subsystem cache size. The Storage page of the Power-on Reset notebook provides controls for setting the cache size. See “Power-on reset” on page 5-6 for more information about performing a power-on reset as an error recovery procedure.

After performing a power-on reset of the CPC, you can review its current storage allocations, including the internal subsystem cache size, by using the **Storage Information** task from the CPC Operational Customization task list. For additional information and instructions for starting the task, see “Reviewing current storage allocations” on page 6-58.

Configuring system assist processors: The physical processing units installed in the central processor complex (CPC) are configured either as central processors (CPs) or system assist processors (SAPs).

The S/390 Multiprise 3000 Enterprise Server has one SAP and one or more CPs. For instructions for setting the CPC's operating environment, see “Setting the CP/SAP configuration” on page 6-16.

Configuration of the internal disk subsystem

Upon completing the installation and configuration of the internal disk subsystem, performing a power-on reset of the central processor complex (CPC) will make the internal disk control units available.

You can prepare a logical storage subsystem (LSS) for storing data by:

1. Configuring this LSS. This creates from one spare drive and from one to three device arrays in that LSS, based on the number of HDDs that are installed in the associated HDD enclosure.
2. Adding logical volumes to these device arrays and formatting the corresponding storage areas on these device arrays.

Working with logical storage subsystems

You can use the internal disk subsystem configuration facility of the support element workplace to start the task for monitoring, operating, and configuring the internal disk logical storage subsystems, the corresponding internal disk control units, and the logical volumes within these logical storage subsystems.

To work with a logical storage subsystem:

1. Open the internal disk subsystem configuration facility. For instructions, see “Working with internal subsystems” on page 10-5.
2. Select **Logical Storage Subsystems** from the Components list.

   The Logical Storage Subsystems window is displayed.
3. Select a particular logical storage subsystem, identified by the Multiprise 3000 Enterprise Server in which this subsystem is installed.

   Note: The Internal Disk icon on the support element workplace is only available if a storage adapter for the internal disk subsystem is installed.
4. The Arrays and HDDs per LSS window is displayed. The window displays the arrays that pertain to this LSS in the upper section, and all HDDs that pertain to this subsystem that are not associated with a particular array.

   The number of arrays and HDDs that are displayed depends on what is physically installed and whether the LSS has been configured or not.

   If a certain number of HDDs has been installed in this subsystem, but no configuring of the LSS has been done, you should see:

   - No array in the upper section, and
   - All the HDDs you have installed in the lower section.

   If you have installed a number of HDDs that represents a valid configuration, and successfully configured the LSS, you should see:

   - From one to three arrays in the upper section, and
   - One HDD in the lower section.

     This is the spare HDD that will be used to replace an HDD in one of the arrays shown above in case of an HDD failure.

   If you have installed a number of HDDs that represents a valid configuration, successfully configured the LSS, and then added more HDDs in order to upgrade your configuration, you should see:

   - One or two arrays in the upper section, and

- Several HDDs in the lower section.

Configuring a logical storage subsystem

After installing HDDs in an HDD enclosure that was empty so far, you must first configure the LSS associated with this box to create device arrays and a spare drive.

1. Open the internal disk subsystem configuration facility. For instructions, see "Working with internal subsystems" on page 10-5.
2. Select **Logical Storage Subsystems** from the Components list.
3. Select the LSS for the Multiprise 3000 Enterprise Server that you want to configure.

For more information on configuring a logical storage subsystem, see the *Internal Disk Subsystem User's Guide*, SA22-1025.

Upgrading a Logical Storage Subsystem

After installing additional HDDs in an HDD enclosure that contained one or two device arrays, you must first upgrade the LSS associated with this enclosure to create one or two additional device arrays.

1. Open the internal disk subsystem configuration facility. For instructions, see "Working with internal subsystems" on page 10-5.
2. Select **Logical Storage Subsystems** from the Components list.

   The Logical Storage Subsystems window is displayed.
3. Select the LSS for the Multiprise 3000 Enterprise Server that you want to configure.

For more information on upgrading a logical storage subsystem, see the *Internal Disk Subsystem User's Guide*, SA22-1025.

Creating logical volumes

The logical volumes that can be mapped to an internal disk device array can emulate the volumes of an IBM 3380 or IBM 3390 storage device.

1. Open the internal disk subsystem configuration facility. For instructions, see "Working with internal subsystems" on page 10-5.
2. Select **Logical Storage Subsystems** from the Components list.

   The Logical Storage Subsystems window is displayed.
3. Select the device array that you want to create logical volumes.

   A window will display the logical volumes that already exist on this array. If you open the *details view*, you get the unit address, the type and model, the approximate size, and the current operating state of each logical volume.
4. Select the **Add** button to define and create new logical volumes.

   This displays a window where you can select the number and types of logical volumes you want to create.

For more information on creating logical volumes, see the *Internal Disk Subsystem User's Guide*, SA22-1025.

Assigning unit addresses (UAs) to logical volumes: When logical volumes are created, a unit address has to be assigned to each of these logical volumes. These unit addresses have to be unique per control unit image. This means, the unit addresses unused on the device arrays that belong to a single control unit must not be in conflict. You do not have to specify the unit addresses to be assigned to the logical volumes you create. The internal disk subsystem will assign them if they are not entered.

For information on rules used to define the unit addresses for logical volumes when they are created, see the *Internal Disk Subsystem User's Guide*, SA22-1025.

Determining the unit addresses of logical volumes

After you have created new logical volumes, you have to add these unit addresses to the IOCDS in order to be able to work with these logical volumes. In order to do this, you have to determine the unit addresses that are assigned to your logical volumes.

To find the unit addresses assigned to the logical volumes on a particular device array:

1. Open the internal disk subsystem configuration facility. For instructions, see "Working with internal subsystems" on page 10-5.
2. Select **Logical Storage Subsystems** from the Components list.

   The Logical Storage Subsystems window is displayed.
3. Select a particular logical storage subsystem, identified by the Multiprise 3000 Enterprise Server in which this subsystem is installed.
4. Select the device array that the logical volumes are mapped.

   A window will display the logical volumes that exist on the array sorted by their unit address, together with the type and model, the approximate size, and the current operating state of each logical volume.

Deleting logical volumes

The internal disk subsystem configuration facility allows you to array again. You may want to do so in order to change the logical volumes mapping, for instance to replace a big logical volume (e.g., 3390-9), by several smaller ones.

Deleting selected logical volumes can be done while other logical volumes on that same array are still online.

Notes:

1. Deleting a logical volume means that all data that currently resides on this logical volume will be lost.
2. Before deleting a logical volume, you should first vary off this logical volume from your operating system.

In order to delete selected logical volumes (after you have varied them offline from your operating system console):

1. Open the internal disk subsystem configuration facility. For instructions, see "Working with internal subsystems" on page 10-5.
2. Select **Logical Storage Subsystems** from the Components list.

The Logical Storage Subsystems window is displayed.

3. Select the device array that you want to delete logical volumes.

   A window will display the logical volumes that exist on this array, together with the unit address, their type and model, the approximate size, and the current operating state of each logical volume.

4. Select the logical volume(s) you want to delete.
5. Select the **Delete** button.

Note: You can delete logical volumes that are in the formatting or format requested state (i.e., volumes that you just requested to create and which the formatting operation is still in process or hasn't even started yet. This allows you to stop a formatting operation in case you have inadvertently denied the wrong set or number of logical volume types and models, without first waiting for the entire formatting operation to complete.).

Internal disk subsystem upgrades

A service representative will perform all the tasks necessary to upgrade the internal disk subsystem configuration. Upgrading an internal disk subsystem configuration includes moving existing hardware, if necessary, and installing new hardware to support the new configuration.

The internal tape drive

The S/390 Multiprise 3000 Enterprise Server supports the internal tape drive.

Working with internal tape units: You can use the internal subsystem facility of the support element workplace to start the task for monitoring, operating, and customizing internal tape units.

To work with internal tape units:

1. You must be logged on the support element in the system programmer or service representative user mode.
2. Open the internal subsystem facility. For instructions, see “Working with internal subsystems” on page 10-5.

   This displays the Internal Subsystem Configuration window. It lists the tasks available for working with the CPC's internal subsystems.

3. Select **Display internal tape units** from the list of internal subsystem configuration tasks.

   This displays the Internal Tape Adapters window. It lists the internal tape adapters.

4. From the list of internal tape adapters, select the internal tape adapter that you want to work with.
5. Select **Display/Alter Internal Tape Devices** from the **Customize** menu. This displays the Internal Tape Devices window.
6. Use the list and menu choices to choose the tape devices you want to work on, and to choose the work you want to do.

   Move the cursor to the list or any menu choice and request help for more information about it. Press **F2** to request help for the window.

The Emulated I/O Subsystem

The emulated I/O function is a standard feature of the S/390 Multiprise 3000 Enterprise Server. This feature provides I/O device emulation for LAN adapters, communications adapters, DASD, and tape devices that may be plugged into the CPC cage. This emulation code runs on the same integrated PC that also runs on the support element.

The support element provides emulated I/O configuration panels, which allows you to define devices and associate them with PC resources such as LAN cards, communications cards, SCSI devices, and files on the support element hard drives. In this definition process, the unit address of each emulated device is assigned. Each device also has an associated control unit. That control unit type is inferred from the device type during emulation I/O configuration.

Note: If you have a secured desktop, then only 3270 devices can be configured using the AWS3274 device manager control unit. There is a limit of two local 3270 sessions on the desktop or from the SE application. In order to configure and manage emulated I/O communications devices (AWSICA, LCS3172, LAN3172, LAN3274, WAN3172), the System Programmer must have access to an open desktop that allows the execution of emulated I/O OS/2 utility commands at an OS/2 prompt. In order to be able to configure and manage any other emulated I/O devices, the System Operator must be configured for an open desktop. See “Customizing your user profiles for access” on page 14-2 for information on enabling the secured Desktop.

The emulated I/O subsystem uses resources available on your S/390 Multiprise 3000 Enterprise Server to emulate the devices available on larger S/390 systems. Device mapping is performed by a utility program called Emulation I/O Configurator. The Configurator is menu-driven. Changes to system configuration are made by changing the values in data menus. Using the Configurator, you can define the particular S/390 device to emulated I/O device mapping you require and create a DEVMAP file based on this mapping. This function is performed by the UPDATE SYSTEM DEVICES menu of the Configurator. This menu provides DASD allocation/deletion capabilities on a S/390 real device address basis. You can use this menu to:

- Add devices at particular S/390 addresses
- Allocate DASD volumes
- Change OS/2 file names assigned to DASD devices
- Delete devices from DEVMAP
- Temporarily exclude devices from DEVMAP
- Specify parameters for device managers.

For more information on configuring the emulated I/O subsystem, see the *Emulated Input/Output Subsystem User's Guide and Reference*, GC38-0410.

To start the Configurator:

1. You must be logged on the support element in the system programmer mode.

2. Open the **Task List** from the **Views** area.
3. Open **CPC Configuration** from the **Task List Work Area**.

   The CPC Configuration task list contains the **Emulated I/O Configuration** task that you will start
4. Open **Groups** from the **Views** area.
5. Open any group that contains the CPC from the **Groups Work Area**.
6. Drag and drop the CPC on the **Emulated I/O Configuration** task to start it.

   The CONFIGURATION DEVMAPS menu is displayed in the Emulated I/O Configuration window.
7. The menu displays the location and names of the four emulated I/O device maps that are associated with the four IOCDS files in the system.

   The Active Device Map is displayed. This is the Device Map that was used for the last Power-On Reset(POR) that was performed. The active DEVMAP is a copy of one of the DEVMAPs listed below it. At system POR, the copy is made based on which IOCDS (A0 through A3) has been assigned for POR. The Active DEVMAP can only be viewed, not changed. If it is selected on this menu, it allows you to activate and deactivate emulated I/O tracing for the devices shown.
8. Place the cursor under the DEVMAP you want to edit or view, press Enter.

   To edit the original copy of the Active DEVMAP, read the Note displayed below the filenames box.
9. Place the cursor under the corresponding DEVMAP, press Enter

   Any of the DEVMAPS in yellow can be edited, but you must run POR for any of the changes to take affect. The DEVMAP that corresponds to the IOCDS selected during POR becomes the Active Device Map upon successful completion of POR.

The Cryptographic Coprocessor feature

The Cryptographic Coprocessor feature is secure, integrated hardware that performs high-speed cryptographic functions.

The functions provided by the Cryptographic Coprocessor feature comply with the IBM's Common Cryptographic Architecture (CCA). The feature's functions include:

- Data Encryption Standard (DES) and Commercial Data Masking Facility (CDMF) data encryption algorithms
- Rivest-Shamir-Adelman (RSA) and Digital Signature Standard (DSS) public key algorithms (PKAs)
- MAC, MDC-2, MDC-4, and SHA-1 hashing algorithms
- Pseudo-random number (PRN) generator
- Support for the Trusted Key Entry (TKE) feature

The Cryptographic Coprocessor feature works with the IBM Resource Access Control Facility (RACF®) and Integrated Cryptographic Service Facility (ICSF), or equivalent software products, in an MVS/ESA or OS/390 environment to provide data privacy, data integrity, cryptographic key installation and generation, electronic

cryptographic key distribution, and personal identification number (PIN) processing. The Cryptographic Coprocessor feature can be used also with the IBM Processor Resource/System Manager (PR/SM™) to establish a logically partitioned (LPAR) environment in which multiple logical partitions can use cryptographic functions.

Cryptographic Coprocessor feature installation

The Cryptographic Coprocessor feature is available as an optional feature for the S/390 Multiprise 3000 Enterprise Server. A service representative will perform all the tasks necessary to install the feature. The S/390 Multiprise 3000 Enterprise Server includes one cryptographic coprocessor.

In either case, you can check the CPs Work Area of the support element workplace to determine whether cryptographic coprocessors are installed. A unique icon is displayed for CPs that have a cryptographic coprocessor attached:

- The icon for CPs *without* an attached cryptographic coprocessor displays only a chip labelled 390.
- The icon for CPs *with* an attached cryptographic coprocessor displays the chip labelled 390 and a smaller, attached chip that represents the cryptographic coprocessor.

Getting ready to use the Cryptographic Coprocessor feature

Using the cryptographic functions of the Cryptographic Coprocessor feature requires configuring and enabling the cryptographic coprocessors, and loading cryptographic coprocessor configurations during system activation. To perform these and other tasks, you can use the support element workplace to open a facility for working with cryptographic coprocessors.

Working with the cryptographic coprocessors

You can use the support element workplace to work with the cryptographic coprocessors installed in the central processor complex (CPC).

To work with cryptographic coprocessors:

1. You must be logged on the support element in the system programmer or service representative user mode.
2. The Cryptographic Coprocessor feature must be installed, and the CPC must be powered-on.
3. Open the **Task List** from the **Views** area.
4. Open **CPC Configuration** from the **Task List Work Area**.

   The CPC Configuration task list contains the **Cryptographic Coprocessor Configuration** task that you will start
5. Open **Groups** from the **Views** area.
6. Open any group that contains the CPC from the **Groups Work Area**.
7. Drag and drop the CPC on the **Cryptographic Coprocessor Configuration** task to start it.

   The Cryptographic Coprocessor Configuration window lists the cryptographic coprocessors installed in the CPC, and provides push buttons for working with them.

Configuring and enabling cryptographic coprocessors

Cryptographic coprocessors are shipped with their cryptographic functions disabled. The cryptographic functions remain disabled and cannot be used until the cryptographic coprocessors are configured and enabled. To configure and enable cryptographic coprocessors, you must get their unique configuration data from IBM.

Cryptographic coprocessor configuration data is provided separately by IBM Manufacturing according to United States federal export regulations. Configuration data determines the level of cryptographic functions a cryptographic coprocessor can provide. The following configurations are available:

CDMF with Exportable PKA
: This configuration enables the CDMF and allows 512-bit PKA key lengths. It is available outside the United States and Canada to countries and companies that are *not* subject to US export embargo.

DES with Exportable PKA
: This configuration allows 56-bit DES and 512-bit PKA key lengths. It is available outside the United States and Canada to financial institutions owned by US or Canadian companies and to companies with at least 51% US or Canadian ownership.

DES with Exportable PKA & TKE
: This configuration allows 56-bit DES and 512-bit PKA key lengths, and supports the optional Trusted Key Entry (TKE) feature. It is available outside the United States and Canada to financial institutions owned by US or Canadian companies and to companies with at least 51% US or Canadian ownership.

DES with PKA (US/CANADA)
: This configuration allows 56-bit DES and 1024-bit PKA key lengths. It is available within the United States and Canada only.

DES with PKA & TKE (US/CANADA)
: This configuration allows 56-bit DES and 1024-bit PKA key lengths, and supports the optional Trusted Key Entry (TKE) feature. It is available within the United States and Canada only.

To configure and enable a cryptographic coprocessor, you must *import* its unique configuration data from the cryptographic coprocessor enablement diskette provided by IBM. You can use the support element workplace to import the configuration data for a cryptographic coprocessor.

Before importing cryptographic coprocessor configuration data:

1. You must have the enablement diskette provided by IBM for configuring and enabling your system's unique cryptographic coprocessors.
2. You must be logged on the support element in the system programmer or service representative user mode.

To import cryptographic coprocessor configuration data:

1. Start the task for working with cryptographic coprocessors. For instructions, see “Working with the cryptographic coprocessors” on page 10-13.

   The Cryptographic Coprocessor Configuration window lists the cryptographic coprocessors installed in the CPC, and provides push buttons for working with them.

2. Follow these steps for each cryptographic coprocessor for which you want to import configuration data:
   a. Select the cryptographic coprocessor from the list, then select the **Import** push button.

      This displays a message that identifies the selected cryptographic coprocessor.

   b. Insert the enablement diskette for the selected cryptographic coprocessor in the console's diskette drive.

   c. Select the **Import** push button.

      This displays a message that identifies the cryptographic coprocessor configuration that will be imported.

   d. Select the **Import** push button.

      A message is displayed to indicate the results of the import.

Configuring and enabling a cryptographic coprocessor enables loading the configuration data during system activation.

Loading cryptographic coprocessor configuration data

To initialize a cryptographic coprocessor, you must load its previously imported configuration data during activation of the central processor complex (CPC).

You can use the support element workplace to customize whether and how you want configuration data loaded for a cryptographic coprocessor during CPC activation.

Before customizing settings for loading cryptographic coprocessor configuration data:

1. You must have configured and enabled the cryptographic coprocessor. That is, you must have imported the cryptographic coprocessor's configuration data.
2. You must be logged on the support element in the system programmer or service representative user mode.

To customize settings for loading cryptographic coprocessor configuration data:

1. Start the task for working with cryptographic coprocessors. For instructions, see “Working with the cryptographic coprocessors” on page 10-13.

   This displays the Cryptographic Coprocessor Configuration window. The window lists the cryptographic coprocessors installed in the CPC, and provides push buttons for working with them.

2. Follow these steps for each cryptographic coprocessor for which you want to customize settings for loading cryptographic coprocessor configuration data:
   a. Select the cryptographic coprocessor from the list, then select the **Select for next activation** push button.

      This displays the Select Cryptographic Coprocessor Configuration for Next Activation window.

   b. Review the window's current settings for loading configuration data during CPC activation:

- The **Next Configuration** field identifies and describes the configuration data, if any, that is set to be loaded during activation.
- If configuration data is set to be loaded during activation, then the radio buttons in the Activation Control group box indicate how the configuration data is loaded:
  - If the **Force cryptographic coprocessor zeroization and initialize on next activation** radio button is selected, then the cryptographic coprocessor is zeroized then initialized during CPC activation, regardless of its status at that time.
  - Or if the **Auto-initialize** radio button is selected, then the cryptographic coprocessor is loaded with its configuration data during CPC activation only if it is not already initialized.

  Note: If no configuration is set to be loaded during activation, then the Activation Control group box is grayed-out.

c. **Additional instructions** for loading configuration data during activation if no configuration data is currently set to be loaded:

   1) Select the list button beside the **Next Configuration** field.

      This opens a list of the configuration data available for the selected cryptographic coprocessor.

   2) Select from the list the configuration data you want the cryptographic coprocessor to load during the next activation.

      This closes the list and displays the Activation Control group box.

   3) Select a radio button in the Activation Control group box to indicate how you want the configuration data to be loaded.

      Note: Auto-initialization is the default setting, so the **Auto-initialize** radio button is selected initially. If you change the setting by selecting **Force cryptographic coprocessor zeroization and initialize on next activation** instead, it affects only the next CPC activation. After the cryptographic coprocessor is zeroized and initialized during the next CPC activation, **Auto-initialize** is automatically selected again by default.

   4) Select the **Save** push button to save the settings and close the window.

d. **Additional instruction** for loading no configuration data during activation if configuration data is currently set to be loaded:

   Select the **Reset** push button to reset the **Next Configuration** field for loading no configuration data during activation. This also saves the setting and closes the window.

Configuring and initializing cryptographic coprocessors prepares the Cryptographic Coprocessor feature for performing cryptographic functions. Using the functions requires preparing either the central processor complex (CPC) or one or more of its logical partitions for running software products that work with the Cryptographic Coprocessor feature.

Preparing the CPC for using cryptographic functions

To prepare the central processor complex (CPC) for running software products that work with the Cryptographic Coprocessor feature, load it with an operating system, such as OS/390 or MVS/ESA, that supports using cryptographic functions.

The activation profile you use to activate the CPC can load the operating system. For more information, see “Tips for loading operating systems” on page 6-37.

Preparing logical partitions for using cryptographic functions

To prepare one or more logical partitions for running software products that work with the Cryptographic Coprocessor feature, activate the central processor complex (CPC) in logically partitioned (LPAR) mode, and activate each logical partition as follows:

- Assign it at least one cryptographic coprocessor.
- Set whether it can use the public key algorithm (PKA).
- Select the cryptographic domain index (CDX) numbers of its control domains and usage domains.
- Set whether and how it can use cryptographic functions.
- Load it with an operating system, such as OS/390 or MVS/ESA, that supports using cryptographic functions.

The activation profile you use to activate the CPC can activate it in LPAR mode. For more information, see “Supporting LPAR mode operation” on page 6-8. The activation profiles you use to activate logical partitions can establish their support for using cryptographic functions. For more information, see “Using the Cryptographic Coprocessor feature” on page 6-28.

Note: After activating one or more logical partitions to establish their initial support for using cryptographic functions, you can change some settings for using cryptographic functions *without* activating the logical partitions again. For more information, see “Changing logical partition cryptographic controls” on page 9-5.

Using cryptographic functions of the Cryptographic Coprocessor feature

The Cryptographic Coprocessor feature works with the IBM Resource Access Control Facility (RACF) and Integrated Cryptographic Service Facility (ICSF), or equivalent software products, in an MVS/ESA or OS/390 environment. For information about using the cryptographic functions of the Cryptographic Coprocessor feature, refer to the documentation provided with the operating system and software products you are using.

Monitoring and managing the Cryptographic Coprocessor feature

Upon completing the configuration and initialization of the Cryptographic Coprocessor feature, you can monitor and manage it by:

- Checking the status of the cryptographic coprocessors.
- Testing the pseudo-random number (PRN) generators of the cryptographic coprocessors.

- Authorizing software applications to perform public key secure cable (PKSC) initialization.
- Zeroizing the cryptographic coprocessors.

Checking cryptographic coprocessor status

You can use the support element workplace to monitor the Cryptographic Coprocessor feature by checking the status of the cryptographic coprocessors.

To check the status of the cryptographic coprocessors:

1. Start the task for working with cryptographic coprocessors. For instructions, see “Working with the cryptographic coprocessors” on page 10-13.

   The Cryptographic Coprocessor Configuration window lists the cryptographic coprocessors installed in the CPC, and provides push buttons for working with them.
2. The status of each cryptographic coprocessor is displayed in the **Status** list column.
3. Select from the list the cryptographic coprocessor for which you want more information, then select the **View status** push button.

Testing the PRN generator

Each cryptographic coprocessor includes a pseudo-random number (PRN) generator that provides or supports some of its cryptographic functions.

Testing a PRN generator verifies whether the numbers it generates are sufficiently random.

Ordinarily, a PRN generator is tested automatically when it is initialized. But you can use the support element workplace at any time to manually test a PRN generator.

Before testing a cryptographic coprocessor's PRN generator:

1. A power-on reset of the CPC must be complete.
2. The CP to which the cryptographic coprocessor is attached cannot be checkstopped.
3. The initialization of the PRN generator must be complete.
4. You must be logged on the support element in the system programmer or service representative user mode.

To test a cryptographic coprocessor's PRN generator:

1. Start the task for working with cryptographic coprocessors. For instructions, see “Working with the cryptographic coprocessors” on page 10-13.

   The Cryptographic Coprocessor Configuration window lists the cryptographic coprocessors installed in the CPC, and provides push buttons for working with them.
2. Select from the list the cryptographic coprocessor you want to test, then select the **Test PRN** push button to test it.

   A message is displayed to indicate the results of the test.

Authorizing applications to perform PKSC initialization

You can use the support element workplace to enable or disable the setting that controls whether software applications can issue public key secure cable (PKSC) initialization commands to cryptographic coprocessors.

To enable or disable the PKSC initialization setting:

1. You must be logged on the support element in the system programmer or service representative user mode and the Cryptographic Coprocessor feature must be installed.
2. Start the task for working with cryptographic coprocessors. For instructions, see “Working with the cryptographic coprocessors” on page 10-13.

   The Cryptographic Coprocessor Configuration window lists the cryptographic coprocessors installed in the CPC, and provides push buttons for working with them.
3. Select the **PKSC initialization** push button.
4. Review the current settings for PKSC initialization.
   - The **PKSC initialization** check box displays a check mark while PKSC initialization is enabled.
   - Otherwise, the check box is empty while PKSC initialization is disabled.
5. Click once on the check box to change its setting. That is, click once on an empty check box to mark it, or click once on a marked check box to unmark it.
6. Select the **Save** push button to save the setting and close the window.

Zeroizing cryptographic coprocessors manually

Zeroizing a cryptographic coprocessor erases its configuration data and clears all cryptographic keys by resetting them to binary zeroes.

You can use the support element workplace to zeroize cryptographic coprocessors either automatically during an activation of the central processor complex (CPC) or manually at any time. This topic describes using the support element workplace to manually zeroize cryptographic coprocessors. For more information about zeroizing cryptographic coprocessors during CPC activation, see “Loading cryptographic coprocessor configuration data” on page 10-15.

Warning: Zeroizing a cryptographic coprocessor erases its configuration data and clears all cryptographic keys. Cryptographic coprocessors should be zeroized manually only when absolutely necessary, typically when cryptographic coprocessor configuration data must be erased immediately.

For example:

- You must zeroize cryptographic coprocessors prior to selling or transferring ownership of the CPC.
- A service representative may zeroize cryptographic coprocessors prior to upgrading the CPC, if required.
- You may want to zeroize cryptographic coprocessors if, in an emergency, it is the only way to maintain the security of encrypted data.

Before manually zeroizing cryptographic coprocessors:

1. You must have configured and enabled the cryptographic coprocessors. That is, you must have imported each cryptographic coprocessor's configuration data.
2. A power-on reset of the CPC must be complete.
3. The CP to which the cryptographic coprocessor is attached cannot be checkstopped.
4. You must be logged on the support element in the system programmer or service representative user mode.

To manually zeroize cryptographic coprocessors:

1. Start the task for working with cryptographic coprocessors. For instructions, see “Working with the cryptographic coprocessors” on page 10-13.

   This displays the Cryptographic Coprocessor Configuration window. The window lists the cryptographic coprocessors installed in the CPC, and provides push buttons for working with them.
2. Select the **Zeroize** push button to zeroize the cryptographic coprocessors.
3. A message is displayed to notify you of the consequences of zeroizing the cryptographic coprocessors. Select the **Zeroize** push button to confirm your request to zeroize them.

   A message is displayed to indicate the results of the function.

Chapter 11. Internal code change management

This section describes tasks from the **Change Management** task list that you can use to manage internal code changes provided by IBM for changing the licensed internal code of the central processor complex (CPC) and its support element. After describing licensed internal code and internal code changes in more detail, this section provides instructions for starting the tasks.

Licensed internal code

Licensed internal code, referred to also as *internal code*, controls many of the operations of the hardware with which it is provided. For example, internal code is provided with the central processor complex (CPC) and support element of each system, and is often provided with other system components such as channels and optional features.

Activating internal code makes it operational. If you have experience using other systems, you may have performed an *initial microcode load (IML)* to make a system's internal code operational. Though their names are different, the principle and purpose of the processes are the same: to load internal code so the system can use it.

Internal code is stored on system hardware by IBM during manufacturing. After IBM delivers and installs your system, it may be necessary to change its internal code to add new functions, improve existing functions, or correct problems. For those purposes, IBM provides internal code changes.

Internal code changes

IBM provides *internal code changes* to change the internal code provided with system hardware. Changing the internal code may be necessary to add new functions, improve existing functions, or correct problems.

One unit of internal code is called an *engineering change (EC)*. An *internal code change level*, referred to also as a *change level*, is a group of internal code changes provided to change all or part of the internal code in an EC. The internal code changes in a change level may replace one or more single bytes of internal code in an EC, or may entirely replace one or more modules of internal code.

Clearly, changing internal code directly affects the internal code already stored on system hardware, which is the internal code that the system uses when the hardware is made operational. So following an orderly process in a timely manner is essential for managing internal code changes correctly.

IBM recommends following the internal code change process described in the next topic.

Internal code change process

This is a summary of the process you should follow to correctly manage the internal code changes for a system. Ordinarily, an IBM service representative will provide new internal code changes and manage their initial use. For internal code changes already stored on the support element, IBM recommends that you manage these changes only under the supervision of an IBM service representative or with the assistance of the IBM Support Center.

Note to service representatives: Use the system's service guide to follow service procedures for changing internal code.

The internal code change process is a sequence of tasks you perform upon receiving internal code changes from IBM. Changing the internal code may be necessary to add new functions, improve existing functions, or correct problems.

The goal of the internal code change process is to make the system operate with the most current internal code available.

If you have multiple systems, IBM recommends you complete the process to your satisfaction on one system before distributing the changes to the other systems.

The process begins when IBM either delivers new internal code changes to you on an optical cartridge or diskette, or makes changes available on the IBM Service Support System. Then you should:

1. Backup critical data of the system's support element.
2. Accept *previous* internal code changes, if any, that you retrieved, installed, and activated the last time you used this process.
3. Retrieve *all* new internal code changes from their source to the support element.
4. Install and activate *all* new internal code changes to make them operational.
5. Operate the system to determine whether it is operating correctly and satisfactorily with the new internal code changes.
6. **If you have multiple systems**: When you are satisfied with the operation of the new internal code changes on one system, distribute the changes to other systems and repeat the internal code change process.

You should use a Hardware Management Console, if available, to follow the recommended internal code change process for changing a system's internal code and distributing its internal code changes to other systems. Otherwise, if a Hardware Management Console is not available, you can use each system's support element console to change its internal code.

Changing internal code

If the system's central processor complex (CPC) is connected to and managed by a Hardware Management Console, it is recommended you use the Hardware Management Console, rather than the CPC's support element console, to change the system's internal code. Refer to the documentation provided with the Hardware Management Console for more information and instructions.

Otherwise, if you do not have or do not use a Hardware Management Console to manage the CPC, you can use its support element console to follow the recommended process for changing internal code. You can either:

- Use scheduled operations to automate much of the process.
- Or use change management tasks to manually perform each step in the process.

Automating the process

You can use the support element of a central processor complex (CPC) to automate much of the process IBM recommends following for managing internal code changes.

You can automate the process by:

- Identifying the task, or *operations*, you want performed automatically.
- Scheduling when you want each operation performed.
- Customizing how often you want the schedule of operations repeated.

IBM recommends using regularly scheduled operations for managing internal code changes. The advantages include:

- Installing and activating changes promptly, which may correct internal code errors before they occur or cause problems on your system.
- Accepting changes regularly, which makes installing and activating subsequent changes possible.
- Performing a potentially disruptive operation, like activating the CPC, when its interruption of system availability has the least impact.

Scheduled operations

Use the support element to customize scheduled operations for automatically performing the following operations in the recommended process for managing internal code changes.

- Backup critical data of the support element.
- Accept *previous* internal code changes, if any, that were retrieved, installed, and activated.
- Retrieve the new internal code changes from the IBM Service Support System to the support element.
- Install and activate concurrent internal code changes to make them operational.

To schedule operations for managing internal code changes:

1. You must be logged on the support element in the system programmer or service representative user mode.
2. Open the **Task List** from **Views** area.
3. Open **CPC Operational Customization** from the **Task List Work Area**.

The CPC Operational Customization task list contains the **Scheduled Operations** task that you will start.

4. Open **Groups** from the **Views** area.
5. Open the **CPC** group from the **Groups Work Area**.
6. Drag and drop the CPC on the **Scheduled Operations** task to start it.

   This opens the Scheduled Operations window. It provides controls for scheduling operations.
7. After you start the task, use the online **Help** for information on using a control to start a task for changing internal code. Press **F2** to request help for the window.

Making changes manually

You can use the support element of a central processor complex (CPC) to manually change the internal code of the system.

Use the support element to start the following tasks for changing internal code:

- Accept internal code changes to make them permanent internal code.
- Retrieve internal code changes from a source to the support element.
- Check whether internal code changes meet all the dependencies that must be met to use them with operations that change internal code.
- Install and activate internal code changes to make them operational.
- Remove and activate internal code changes to resolve problems.
- Delete internal code changes to attempt error recovery.
- Distribute internal code changes to other systems.

Starting a task for changing internal code

Note: If the system's central processor complex (CPC) is connected to and managed by a Hardware Management Console, it is recommended you use the Hardware Management Console, rather than the CPC's support element console, to change the system's internal code.

If a Hardware Management Console is available, you can still use the CPC's support element console to change the system's internal code, but it is recommended that you log on the support element directly, rather than connecting to it from a Hardware Management Console. The following tasks cannot be performed when connected to the CPC's support element console from a Hardware Management Console:

- Installing and activating internal code changes
- Removing and activating internal code changes

To start a task for changing internal code:

1. You must be logged on the support element in the system programmer or service representative user mode.

2. Open the **Task List** from the **Views** area.
3. Open **Change Management** from the **Task List Work Area**.

   The Change Management task list contains the **Change Internal Code** that task you will start.
4. Open **Groups** from the **Views** area.
5. Open the **CPC** group from the **Groups Work Area**.

   Note: Changing internal code on a CPC can be considered disruptive. If the CPC is locked, unlock it. See "Setting lockout for disruptive tasks on an object" on page 2-15.
6. Drag and drop the CPC on the **Change Internal Code** task to start it.

   This opens the Change Internal Code window. It provides controls for changing internal code.

   Use the online **Help** for information on using a control to start a task for changing internal code. Press **F2** to request help for the window.
7. Locate the Change internal code options list.

   It lists a radio button for each task available for working with internal code changes.
8. Select the radio button that describes the task you want to start, then select the **OK** push button to start the task.
9. Follow the instructions on the subsequent windows to complete the task.

   Use the online **Help** for any window for information on using a control to perform a task. Press **F2** to request help for the window.

Accepting internal code changes

Internal code changes that are currently installed and activated are eligible for being accepted. Accepting the internal code changes makes them permanent; that is, accepting the internal code changes makes them internal code.

To accept internal code changes:

1. You must be logged on the support element in the system programmer or service representative user mode, and one or more internal code changes must currently be installed and activated.
2. Start the task for working with internal code changes. For instructions, see "Starting a task for changing internal code" on page 11-4.

   This opens the Change Internal Code window. It lists a radio button for each task available for working with internal code changes.

   Use the online **Help** for more information for a radio button, or for any control on any subsequent window. Press **F2** to request help for the window.
3. Select **Accept installed changes that were activated** from the list, then select the **OK** push button.

   This opens the Select Internal Code Changes window. It lists options for deleting either all or specific installed changes that were activated.
4. Accepting *all* installed changes that were activated is recommended. Select **All internal code changes**, then select **OK**.

This displays a confirmation window.

Note: If you want to accept specific internal code changes instead, contact your IBM service representative or your IBM Support Center to determine the engineering change (EC) numbers and change levels of the internal code changes you want to accept, and to get instructions and assistance for completing the task.

5. Review the information on the confirmation window, then select **Accept** to begin the process of accepting all installed changes that were activated.
6. Wait until a message indicates the process is complete.

   Select **OK** to close the message when the process is completed successfully. Otherwise, if the process is not completed successfully, follow the instructions in the message to determine how to proceed.

Retrieving internal code changes

Retrieving internal code changes copies them from their source to the support element.

You must have a source from which to retrieve internal code changes. The source may be either:

- A diskette.
- An optical cartridge.
- The IBM Service Support System, if the support element is configured and enabled for communicating with it.

To retrieve internal code changes:

1. You must be logged on the support element in the system programmer or service representative user mode.
2. Start the task for working with internal code changes. For instructions, see “Starting a task for changing internal code” on page 11-4.

   This opens the Change Internal Code window. It lists a radio button for each task available for working with internal code changes.

   Use the online **Help** for information for a radio button, or for any control on any subsequent window. Press **F2** to request help for the window.
3. Select **Retrieve internal code changes** from the list, then select the **OK** push button.

   This opens the Retrieve Internal Code Changes window. It lists the sources by which IBM provides internal code changes.
4. Select the source of the internal code changes you want to retrieve, then select **OK**.

   Additional windows are displayed upon selecting some sources. Follow the instructions on subsequent windows, if any, to make the selected source available to the support element.

When the support element is ready to retrieve changes from the selected source, the Select Internal Code Changes window is displayed. It lists options for retrieving either all or specific changes from the selected source.

5. Retrieving *all* changes is recommended. Select **All internal code changes**, then select **OK**.

   This displays a confirmation window.

   Note: If you want to retrieve specific internal code changes instead, contact your IBM service representative or your IBM Support Center to determine the engineering change (EC) numbers and change levels of the internal code changes you want to retrieve, and to get instructions and assistance for completing the task.

6. Review the information on the confirmation window, then select **Retrieve** to begin the process of retrieving all internal code changes available from the selected source.

7. Wait until a message indicates the process is complete.

   Select **OK** to close the message when the process is completed successfully. Otherwise, if the process is not completed successfully, follow the instructions in the message to determine how to proceed.

Checking dependencies

Internal code is organized into units called *engineering changes (ECs)*, which are referred to also as *streams*.

Internal code changes may provide new internal code, or correct or improve existing internal code, for particular streams. If internal code changes for multiple streams are needed, together, to complete an addition, correction, or improvement of the internal code, then the internal code changes have *dependencies*. For example, if engineering change (EC) E12345, change level 001, must be installed and activated before EC E54321 level 005 can be installed and activated, then EC E54321 level 005 has a dependency on EC E12345 level 001.

The dependencies of internal code changes are designated by IBM when the changes are created. After internal code changes are retrieved to the support element of the central processor complex (CPC), their dependencies, if any, are checked automatically whenever you start an operation that will change the system's internal code. Such an operation will be attempted only if all dependencies of the internal code changes are met.

But you can use the support element to also *manually* check the dependencies of internal code changes. Manually checking dependencies is useful:

- Before you perform an operation for changing the system's internal code.

  By manually checking the dependencies of internal code changes you intend to select while performing the operation, you may get a detailed list of the dependencies that would not be met, but which you must meet before or while actually attempting the operation.

  Note: This is especially important if you intend to use specific internal code changes, rather than all changes, while performing the operation. Using specific changes increases the possibility of *not* specifying one or more dependencies of the specific changes.

- After automatic dependency checking notifies you, upon attempting an operation, that one or more dependencies are not met.

  By manually checking the dependencies of internal code changes you selected while attempting the operation, you get a detailed list of the dependencies that were not met, but which you must meet before or while attempting the operation again.

But ordinarily, only an IBM service representative checks the dependencies of internal code changes, typically while following a service procedure for changing the system's internal code. If you are not following a service procedure, IBM recommends that you check dependencies only with assistance from IBM Product Engineering, provided through your IBM service representative or IBM Support Center.

To manually check dependencies:

1. You must be logged on the support element in the system programmer or service representative user mode.
2. One or more internal code changes must be eligible for being either accepted, installed, or removed.
3. Start the task for working with internal code changes. For instructions, see “Starting a task for changing internal code” on page 11-4.

   This opens the Change Internal Code window. It lists a radio button for each task available for working with internal code changes.
4. Select **Check dependencies** from the list, then select the **OK** push button.

   Use the online **Help** for more information for any radio button and the operation it describes and the dependency checking it performs. Press **F2** to request help for the window.
5. Select the radio button that describes the operation and internal code changes for which you want dependencies checked, then select **OK** to begin the dependency checking.
6. Wait until a window indicates the dependency checking is complete. The window also indicates whether all dependencies were met for performing the selected operation:

   - If all dependencies were met, you can return to the service procedure you are following and proceed with its instructions for actually performing the operation.
   - If one or more dependencies were not met, the window lists messages that describe each dependency that was not met, identify the operations you must perform to meet the dependencies, and identify the EC number and change level of each internal code change you can or must use with the operations to meet the dependencies. Upon returning to the service procedure you are following, you can proceed with its instructions and refer to its recovery actions for meeting failed dependencies described by the messages.

   In either case, select the **OK** push button to close the window.

Installing and activating internal code changes

Internal code changes that are currently retrieved but not already installed are eligible for being installed and activated. Installing and activating the internal code changes makes them operational.

To install and activate internal code changes:

1. You must be logged on the support element in the system programmer or service representative user mode, and one or more internal code changes must currently be retrieved but not already installed.
2. Start the task for working with internal code changes. For instructions, see "Starting a task for changing internal code" on page 11-4.

   This opens the Change Internal Code window. It lists a radio button for each task available for working with internal code changes.

   Use the online **Help** for information on using a radio button, or for any control on any subsequent window. Press **F2** to request help for the window.
3. Select **Install and activate changes that were retrieved** from the list, then select the **OK** push button.

   This opens the Select Internal Code Changes window. It lists options for installing and activating either all or specific changes that were retrieved.
4. Installing and activating *all* changes that were retrieved is recommended. Select **All internal code changes**, then select **OK**.

   This displays the Request Selection window.

   Note: If you want to install and activate specific internal code changes instead, contact your IBM service representative or your IBM Support Center to determine the engineering change (EC) numbers and change levels of the internal code changes you want to install and activate, and to get instructions and assistance for completing the task.
5. The Request Selection window indicates whether the internal code changes retrieved for the central processor complex (CPC) include concurrent or disruptive changes. The type of changes determine whether installing and activating all changes will disrupt operating system activity on the CPC.

   Use the online **Help** for more information about concurrent and disruptive internal code changes and considerations for activating them. Use the window to select the type of changes you want to install and activate, then select the **Install and activate** push button to continue.
6. Review the information on the confirmation window. The leftmost push button indicates whether installing and activating the retrieved changes will be performed concurrently or disruptively. Select the push button to begin the process.
7. Wait until a message indicates the process is complete.

   Select **OK** to close the message when the process is completed successfully. Otherwise, if the process is not completed successfully, follow the instructions in the message to determine how to proceed.

Removing and activating internal code changes

Removing and activating internal code changes removes the change levels currently installed and activates the previous change levels, which makes the previous change levels operational. But internal code changes should be removed only if it is necessary to resolve a problem that occurred after installing and activating the changes.

Note: IBM recommends that you remove internal code changes only under the direction of IBM Product Engineering.

To remove and activate internal code changes:

1. You must be logged on the support element in the system programmer or service representative user mode, and one or more internal code changes must currently be installed.
2. Start the task for working with internal code changes. For instructions, see “Starting a task for changing internal code” on page 11-4.

   This opens the Change Internal Code window. It lists a radio button for each task available for working with internal code changes.

   Use the online **Help** for more information on a radio button or any control on any subsequent window. Press **F2** to request help for the window.
3. Select **Remove and activate changes** from the list, then select the **OK** push button.

   This opens the Select Internal Code Changes window. It lists options for removing and activating either all or specific changes that are installed.
4. To remove and activate *all* changes that are installed, select **All internal code changes**, then select **OK**.

   This displays the Request Selection window.

   Note: If you want to remove and activate specific internal code changes instead, contact your IBM service representative or your IBM Support Center to determine the engineering change (EC) numbers and change levels of the internal code changes you want to remove and activate, and to get instructions and assistance for completing the task.
5. The Request Selection window indicates whether the internal code changes installed for the central processor complex (CPC) include concurrent or disruptive changes. The type of changes determine whether removing and activating all changes will disrupt operating system activity on the CPC.

   Use the online **Help** for the window for mode information on concurrent and disruptive internal code changes and considerations for activating them. Use the window to select the type of changes you want to remove and activate, then select the **Remove and activate** push button to continue.
6. Review the information on the confirmation window. The leftmost push button indicates whether removing and activating the installed changes will be performed concurrently or disruptively. Select the push button to begin the process.
7. Wait until a message indicates the process is complete.

Select **OK** to close the message when the process is completed successfully. Otherwise, if the process is not completed successfully, follow the instructions in the message to determine how to proceed.

Deleting internal code changes

Deleting internal code changes erases them from the support element. Internal code changes that are currently not installed are eligible for being deleted. This includes changes that were retrieved but never installed, and changes that were installed but have since been removed.

Internal code changes should be deleted only if errors occurred during previous attempts to retrieve, install, or activate them. Deleting the changes allows retrieving them again. Retrieving the changes again may correct the problem that caused the errors.

To delete internal code changes:

1. You must be logged on the support element in the system programmer or service representative user mode, and one or more internal code changes must currently be available but not installed.
2. Start the task for working with internal code changes. For instructions, see “Starting a task for changing internal code” on page 11-4.

   This opens the Change Internal Code window. It lists a radio button for each task available for working with internal code changes.

   Use the online **Help** for a radio button, or for information on using any control on any subsequent window. Press **F2** to request help for the window.
3. Select **Delete retrieved changes that were not installed** from the list, then select the **OK** push button.

   This opens the Select Internal Code Changes window. It lists options for accepting either all or specific installed changes that were activated.
4. To delete *all* changes that are currently available but not installed, select **All internal code changes**, then select **OK**.

   This displays the Request Selection window.

   Note: If you want to delete specific internal code changes instead, contact your IBM service representative or your IBM Support Center to determine the engineering change (EC) numbers and change levels of the internal code changes you want to delete, and to get instructions and assistance for completing the task.
5. Review the information on the confirmation window, then select **Delete** to begin the process of deleting all changes that are available but not installed.
6. Wait until a message indicates the process is complete.

   Select **OK** to close the message when the process is completed successfully. Otherwise, if the process is not completed successfully, follow the instructions in the message to determine how to proceed.

Distributing changes to other systems

If you have multiple CPCs connected to and managed by one or more Hardware Management Consoles, it is recommended you use a Hardware Management Console to distribute internal code changes to the systems.

If you have multiple systems but do not use a Hardware Management Console to manage them, you can still distribute internal code changes to the systems, but by somewhat more manual processes:

- If you receive internal code changes on an optical cartridge or diskette delivered by IBM, you can distribute the same changes among multiple systems simply by using the support element of each system's CPC to retrieve the changes from the cartridge or diskette.
- If you receive internal code changes from the IBM Service Support System, you can use one support element to retrieve the changes from the IBM Service Support System to an optical cartridge or diskette. Then use the support element of each system's CPC to retrieve the changes from the cartridge or diskette.

The support element must be configured and enabled for connecting to the IBM Service Support System.

To retrieve internal code changes for distribution:

1. You must be logged on the support element in the system programmer or service representative user mode.
2. Open the **Task List** from the **Views** area.
3. Open **Change Management** from the **Task List Work Area**.

   The Change Management task list contains the **Change Internal Code** task that you will start.
4. Open **Groups** from the **Views** area.
5. Open the **CPC** group from the **Groups Work Area**.

   Note: Changing internal code on a CPC can be considered disruptive. If the CPC is locked, unlock it. See “Setting lockout for disruptive tasks on an object” on page 2-15.
6. Drag and drop the CPC on the **Change Internal Code** task to start it.

   The Change Internal Code window lists a radio button for each task available for working with internal code changes.
7. Select **Retrieve internal code changes** from the list, then select the **OK** push button.

   The Retrieve Internal Code Changes window lists a radio button for each option available for retrieving internal code changes.
8. Select **Retrieve changes to removable media** from the list, then select **OK**.

   The Retrieve Changes to Media window provides controls for choosing whether you want to retrieve the changes to an optical cartridge or diskette.

9. Follow the instructions on the Retrieve Changes to Media window and subsequent windows to complete the task.

   Use the online **Help** for more information on any window control to use it while performing the task. Press **F2** to request help for the window.

Considerations when activating internal code changes

Internal code changes for a system may include changes for the central processor complex (CPC), its support element, and other system components such as channels and optional features.

Activating internal code makes it operational after it is changed. The topics in this section describe how activating internal code affects the system component for which internal code was changed.

Activating changes for the CPC

Activating internal code for the central processor complex (CPC) after installing or removing internal code changes may require activating the CPC.

The types of internal code changes you installed or removed determine whether activating the CPC is necessary to activate its internal code afterwards. There are two types of internal code changes:

- *Concurrent* changes

  You do not need to activate the CPC to activate internal code that is changed by installing or removing concurrent changes.

- *Disruptive* changes

  You must activate the CPC to activate internal code that is changed by installing or removing disruptive changes.

Since activating a CPC ends its operating system activity, you may want to consider that consequence when you choose and use workplace tasks to install or remove changes and activate the internal code:

- Schedule an operation to automatically change and activate concurrent internal code changes.

  Note: Installing or removing disruptive changes must be done from the Change Internal Code window.

- Or manually change and activate internal code to control whether the CPC is activated by choosing the type of changes to make.

  Note: The task you use to manually change internal code will indicate whether internal code changes include concurrent or disruptive changes. You can choose the type of changes you want installed or removed based on whether it is OK to activate the CPC to activate the changes:

  – If it is OK to activate the CPC, you can install or remove both concurrent and disruptive internal code changes.

  – Otherwise, if it is not OK to activate the CPC, you can either install concurrent changes up to the first disruptive change, or remove concurrent changes down to the first disruptive change.

  The online **Help** for the task's windows provides information and instructions for choosing the type of changes you can install or remove.

Activating changes for the support element

Activating internal code for the support element after installing or removing internal code changes may require reinitializing the support element.

Since you do not need to activate the central processor complex (CPC) to activate support element internal code that was changed, support element internal code changes are considered *concurrent* changes. The CPC and its operating systems continue to operate while the support element internal code is activated.

However, support element operations are interrupted and its applications are ended when its internal code is activated. You may want to consider those consequences when you choose and use workplace tasks to install or remove changes and activate the internal code:

- Schedule an operation to automatically change and activate internal code for a day and time when the support element is not in use.
- Or manually change and activate internal code when the support element can be reinitialized without interrupting other operations or ending other applications.

Remote connections to the support element from another console are disrupted when the support element's internal code is activated.

Activating changes for channels

Activating internal code for channels after installing or removing internal code changes will require reinitializing the channels.

In most cases, channel internal code can be activated concurrently. That is, the central processor complex (CPC) can continue operating while channel internal code is activated.

Channel internal code cannot be activated concurrently for channels that are in continuous use. Channels in continuous use are referred to here as *continuous usage channels*.

Activating the channel internal code is held pending for continuous usage channels, rather than interrupting and ending their activity, until either:

- Channel activity stops.
- A power-on reset of the CPC is performed.

Stopping channel activity: The internal code for continuous usage channels will be activated when the channels are no longer in use. To stop channel activity, you can either:

- Use an operating system facility to end channel activity.
- Use tasks from the CHPID Operations task list of the support element workplace to end channel activity.

  Note: The operating system may not be notified when channel activity ends. For this reason, it is recommended you use an operating system facility rather than the workplace to end channel activity.
- Wait for channel activity to end.

Note: This action may be impractical. Typically, channels with activation of internal code pending are always in use.

Performing a power-on reset: The internal code for continuous usage channels will be activated when a power-on reset of the CPC is performed. To perform a power-on reset, you can either:

- Use the **Activate** task from the Daily task list to activate the CPC.
- Use the **Power-on reset** task from the CPC Recovery task list to perform a power-on reset of the CPC.

Keeping records of internal code changes

The support element automatically keeps records of information about the internal code changes stored on it. The record-keeping begins when changes are retrieved from their source to the support element.

For each internal code change, the information identifies:

- Its engineering change (EC) number.
- The change level most recently retrieved.
- The highest retrieved internal code change level that can be installed and activated concurrently.
- The change level most recently installed.
- The change level most recently activated.
- The change level most recently accepted.
- The lowest installed change level that can be removed and activated concurrently.
- The lowest change level that can be activated after removing installed change levels.
- Additional details include the most recent date and time each task was performed.

The information may assist you with planning and managing internal code changes. For example, review the information to either:

- Determine whether the central processor complex (CPC) is operating with your latest available levels of internal code changes.
- Determine which tasks you must perform next to make the CPC operate with your latest available levels of internal code changes.

Use the support element to view the internal code change information for the CPC.

Viewing internal code change information

You can use the support element of a central processor complex (CPC) to display information about the internal code changes stored on it.

To view internal code change information:

1. You must be logged on the support element in the advanced operator, system programmer, or service representative user mode.
2. Open the **Task List** from the **Views** area.
3. Open **Change Management** from the **Task List Work Area**.

   The Change Management task list contains the **System Information** task you will start.
4. Open **Groups** from the **Views** area.
5. Open the **CPC** group from the **Groups Work Area**.
6. Drag and drop the CPC on the **System Information** task to start it.

   This opens the System Information window. It displays internal code change information.

   Use the online **Help** for more information on the internal code change information.

Settings for internal code change management

Both the remote service settings and change management settings of a central processor complex (CPC) affect how you can use its support element for internal code change management:

- The CPC's *remote service settings* control whether you can use the IBM Service Support System as a source for retrieving internal code changes to the support element.
- The CPC's *change management settings* control whether and how you can use retrieved internal code changes to change the internal code of the CPC and its support element.

Settings for retrieving internal code changes from the IBM Service Support System

IBM provides internal code changes by delivering them on an optical cartridge or diskette, and by making them available on the IBM Service Support System. Although the same internal code changes are available from each source, the most direct source is the IBM Service Support System. But you can use the IBM Service Support System as a source only by customizing, in advance, the remote service settings of a central processor complex (CPC) to *enable* remote service.

While remote service is enabled, the IBM Service Support System is *another* source for manually retrieving internal code changes; that is, optical cartridges and diskettes remain eligible sources. But if you intend to *schedule an operation* for retrieving internal code changes regularly and automatically, the IBM Service Support System is the only eligible source. So you must enable remote service before scheduling an operation for retrieving internal code changes.

To use the IBM Service Support System as a source for retrieving internal code changes, either manually or during a scheduled operation, see “Customizing remote service settings” on page 7-4 for instructions for enabling remote service.

Settings for changing internal code

The *change management settings* of a central processor complex (CPC) include:

Internal code change authorization
Controls whether you can use retrieved internal code changes to change the internal code of the CPC and its support element.

This setting is referred to also as the *change management services* setting.

Concurrent internal code change authorization
Controls whether you can activate concurrent internal code changes concurrently.

Both change management settings are *enabled* by default. That is, the settings allow both:

- Using retrieved internal code changes to change the internal code of the CPC and its support element.
- And activating concurrent internal code changes concurrently.

Normally, the default change management settings should remain enabled. But the support element's change management tasks include tasks for changing the settings if necessary.

Authorizing internal code changes

When the internal code change authorization setting is enabled, you can use the support element console to install and activate internal code changes and to perform subsequent change management operations:

- Accept internal code changes to make them permanent internal code.
- Remove internal code changes to resolve problems.
- Delete internal code changes to attempt error recovery.

Normally, the setting is enabled, which allows changing the internal code of the CPC and its support element. But you can manually disable the setting if there is any reason you do not want internal code to be changed.

The support element console also disables the setting automatically if it detects errors after activating new internal code changes, to prevent accepting the erroneous internal code changes. If this happens, you can manually enable the setting again when you want to install and activate new internal code changes that correct the previously detected error.

To change the setting for internal code change authorization:

1. You must be logged on the support element in the system programmer or service representative user mode.

2. Open the **Task List** from the **Views** area.
3. Open **Change Management** from the **Task List Work Area**.

   The CPC Operational Customization task list contains the **Authorize Internal Code Changes** task that you will start.
4. Open **Groups** from the **Views** area.
5. Open the **CPC** group from the **Groups Work Area**.
6. Drag and drop the CPC on the **Authorize Internal Code Changes** task to start it.
7. Use the Authorize Internal Code Changes window controls to enable or disable the setting for internal code change authorization:

   a. While the setting is enabled, the **Do not allow installation and activation of internal code changes** check box is empty.

      To disable the setting, click once on the check box to mark it.

   b. While the setting is disabled, the **Do not allow installation and activation of internal code changes** check box displays a check mark.

      To enable the setting, click once on the check box to unmark it.

   c. Select **Save** to save the setting and close the window.

   Use the online **Help** for more information to enable or disable the setting for internal code change authorization.

Authorizing concurrent internal code changes

When the concurrent internal code change authorization setting is enabled, you can use the support element console to activate concurrent internal code changes concurrently.

Activating internal code changes *concurrently* activates the changes without disrupting operating system activity on the central processor complex (CPC). In contrast, activating internal code changes *disruptively* will disrupt operating system activity on the CPC.

Activating internal code changes concurrently requires the support of both the CPC and the internal code changes:

- The internal code changes must be *concurrent*. That is, they must be eligible for being activated concurrently.

  This support is designated by IBM when the internal code changes are created.
- The CPC must be *enabled* for activating internal code changes concurrently. That is, its concurrent internal code change authorization setting must be enabled.

  Normally, the setting is enabled, which allows activating concurrent internal code changes concurrently. But you can manually disable the setting if there is any reason you do not want concurrent internal code changes to be activated concurrently.

To change the setting for concurrent internal code change authorization:

1. You must be logged on the support element in the system programmer or service representative user mode.
2. Open the **Task List** from the **Views** area.
3. Open **Change Management** from the **Task List Work Area**.

   The Change Management task list contains the **Authorize Concurrent Internal Code Change** task that you will start.
4. Open **Groups** from the **Views** area.
5. Open the **CPC** group from the **Groups Work Area**.
6. Drag and drop the CPC on the **Authorize Concurrent Internal Code Change** task to start it.

   This opens the Authorize Concurrent Internal Code Change window.
7. Use the Authorize Concurrent Internal Code Change window controls to enable or disable the setting for concurrent internal code change authorization:
   a. While the current authorization setting is enabled, select **Disable** from the **Authorization status for next activation** list to disable the setting upon the next activation of the CPC.
   b. While the current authorization setting is disabled, select **Enable** from the **Authorization status for next activation** list to enable the setting upon the next activation of the CPC.
   c. Select **OK** to save the setting then select **Cancel** to close the window.

   Use the online **Help** for more information to enable or disable the setting for internal code change authorization.

   Note: The new setting is saved, but it will not become the current setting until the next activation of the CPC.

Chapter 12. Processor and storage operations

This section describes tasks you can use to monitor and control the operation and storage of specific central processors (CPs) in the central processor complex (CPC).

The **CP Toolbox** task list contains the tasks, referred to here as *CP tools*. This section provides instructions for starting the tasks.

Processor operations: start and stop

Start and *stop* are processor operations you can use, together, to control whether a processor can process instructions. If you have experience using other systems, you may have used START and STOP commands or Start and Stop keys to start and stop a processor.

You can use the support element workplace to start and stop any eligible processor. Eligible processors include:

- Physical processors that support the image of a central processor complex (CPC) activated in basic mode.
- Logical processors that support logical partitions activated in operating modes other than coupling facility mode.

Stopping processors

Follow your local procedures for determining when to stop processors. But generally, stopping processors for an image is effective only when the image and processors are operating.

To stop processors for an image:

1. You must be logged on the support element in the advanced operator, system programmer, or service representative user mode.
2. Open the **Task List** from the **Views** area.
3. Open **CP Toolbox** from the **Task List Work Area**.

   The CP Toolbox task list contains the **Stop** task that you will perform.
4. Open **Groups** from the **Views** area.
5. Open the **Images** group, or any group that contains the image.
6. Right click on the image supported by the processors you want to stop.
7. Select the **CPs** menu choice from the pop-up menu.
8. Drag and drop a processor that is operating on the **Stop** task to stop it.

   This immediately performs the operation; the processor is stopped.

Starting processors

Follow your local procedures for determining when to start processors. But generally, starting processors for an image is most effective after you've used the **Stop** task to stop processors for the image.

To start processors for an image:

1. You must be logged on the support element in the advanced operator, system programmer, or service representative user mode.
2. Open the **Task List** from the **Views** area.
3. Open **CP Toolbox** from the **Task List Work Area**.

   The CP Toolbox task list contains the **Start** task that you will perform.
4. Open **Groups** from the **Views** area.

   This opens the Groups Work Area.
5. Open the **Images** group, or any group that contains the image.
6. Right click on the image supported by the processors you want to stop.
7. Select the **CPs** menu choice from the pop-up menu.
8. Drag and drop a processor that is stopped on the **Start** task to start it.

   This immediately performs the operation; the processor is started and resumes operating

Setting the operation rate of a processor

The *operation rate* of a central processor (CP) controls how it processes instructions:

- At the *processing rate*, a CP processes instructions indefinitely.
- At the *instruction stepping rate*, a CP processes one instruction or one unit of instructions, and is then stopped.

The processing rate is the CP's operation rate for normal use, while the instruction stepping rate typically is used for testing the CP. Follow your local procedures for determining when to set the operation rate to the instruction stepping rate. You can use the support element workplace to set the operation rate of CPs.

To set the operation rate of CPs:

1. You must be logged on the support element in the system programmer or service representative user mode, and the CPC must be activated in basic mode.
2. Open the **Task List** from the **Views** area.
3. Open **CP Toolbox** from the **Task List Work Area**.

The CP Toolbox task list contains the **Change Operation Rate** task that you will start.

4. Open **Groups** from the **Views** area.
5. Open the **Images** group, or any group that contains the image.
6. Right click on the CPC's image.
7. Select the **CPs** menu choice from the pop-up menu.
8. Drag and drop a CP on the **Change Operation Rate** task to start it.

   Use the online **Help** for the window for more information about how its controls indicate the CP's current operation rate.
9. Use the Operation Rate window controls to change the CP's operation rate, and if necessary, to stop and start the CP.

   Use the online **Help** for the window for more information about using its controls to change the CP's operation rate.

Displaying or altering data in processor storage

A processor stores data in the following storage locations:

- Registers, which are special-purpose storage locations:
  - Program status word (PSW)
  - General purpose registers
  - Control registers
  - Floating point registers
  - Access registers
  - Prefix register
- Main storage locations:
  - Real storage
  - Real storage key
  - Primary virtual storage
  - Secondary virtual storage
  - Absolute storage
  - Home virtual storage
  - Virtual storage identified using access registers

Displaying or altering data in processor storage locations typically is done only by system programmers with experience in interpreting and altering the data. Follow your local procedures for determining when to display or alter data. You can use the support element workplace to display or alter the data in storage locations used by any eligible processor. Eligible processors include:

- Physical processors that support the image of a central processor complex (CPC) activated in basic mode.
- Logical processors that support the images of logical partitions activated in operating modes other than coupling facility mode.

To display or alter data in processor storage:

1. You must be logged on the support element in the system programmer or service representative user mode.
2. Open the **Task List** from the **Views** area.
3. Open **CP Toolbox** from the **Task List Work Area**.

   The CP Toolbox task list contains the **Display or Alter** task that you will start:
4. Locate the image supported by the processors you want to work with:
5. Open **Groups** from the **Views** area.
6. Open the **Images** group, or any group that contains the image.

   This opens the group's work area. The area contains the target image.
7. Right click on the image supported by the processors you want to work with.
8. Select the **CPs** menu choice from the pop-up menu.

   This displays the image's processors in the work area. The area contains the target processors.
9. Drag and drop a processor on the **Display or Alter** task to start it.

   This displays the Display or Alter window.
10. Use the window's controls to display or alter the data in the processor's storage locations.

    Use the online **Help** for the window for more information about using its controls to display or alter the data.

Restarting a processor

A *restart* or *PSW restart* is a processor operation you can use to restart a processor. If you have experience using other systems, you may have used a RESTART command or Restart key to restart a processor.

Restarting a processor typically is done during a software error recovery procedure. But follow your local procedures for determining when to restart a processor. You can use the support element workplace to restart any eligible processor. Eligible processors include:

- Physical processors that support the image of a central processor complex (CPC) activated in basic mode.
- Logical processors that support the images of logical partitions activated in operating modes other than coupling facility mode.

To restart a processor:

1. You must be logged on the support element in the advanced operator, system programmer, or service representative user mode.

2. Open the **Task List** from the **Views** area.
3. Open **CP Toolbox** from the **Task List Work Area**.

   The CP Toolbox task list contains the **PSW Restart** task that you will start.
4. Open **Groups** from the **Views** area.
5. Open the **Images** group, or any group that contains the image.

   Note: restarting a processor on an image can be considered disruptive. If the CPC image is locked, unlock it. See "Setting lockout for disruptive tasks on an object" on page 2-15.
6. Right click on the image supported by the processors you want to work with.
7. Select the **CPs** menu choice from the pop-up menu.
8. Drag and drop a processor on the **PSW Restart** task to start it.
9. Select reason for restarting the processor, then select the **OK** push button to continue.
10. Review the information on the PSW Restart Confirmation window to verify the processor that you will restart is the one you want.
11. If the information is correct, select the **OK** push button to perform the restart.

    A message displays when it is completed.
12. Select **OK** to close the message when the restart completes successfully.

    Otherwise, if the restart does not complete successfully, follow the directions in the message to determine the problem and how to correct it.

Interrupting a processor

An *interrupt* is a processor operation you can use to present an external interruption to a processor. If you have experience using other systems, you may have used an IRPT command or an Irpt key to interrupt a processor.

Follow your local procedures for determining when to interrupt a processor. You can use the support element workplace to interrupt any eligible processor. Eligible processors include:

- Physical processors that support the image of a central processor complex (CPC) activated in basic mode.
- Logical processors that support the images of logical partitions activated in operating modes other than coupling facility mode.

To interrupt a processor:

1. You must be logged on the support element in the advanced operator, system programmer, or service representative user mode.
2. Open the **Task List** from the **Views** area.
3. Open **CP Toolbox** from the **Task List Work Area**.

The CP Toolbox task list contains the **Interrupt** task that you will perform.

4. Open **Groups** from the **Views** area.
5. Open the **Images** group, or any group that contains the image.

   This opens the group's work area. The area contains the target image.
6. Right click on the image supported by the processors you want to work with.
7. Select the **CPs** menu choice from the pop-up menu.

   This displays the image's processors in the work area. The area contains the target processors.
8. Drag and drop a processor on the **Interrupt** task to interrupt it.

   An interrupt request is generated for the processor.

Stopping CPs on address matches or events

The processing and input/output (I/O) activity of central processors (CPs) is reflected in how the activity affects the contents of main storage, the status of I/O devices, and the contents of program status word (PSW). That is, CP activity is indicated by the conditions of main storage, I/O devices, and the PSW.

Monitoring these conditions provides another means for monitoring and controlling CP activity. By setting an *address match* or *event* that identifies the specific condition you want to watch for, all CPs are automatically stopped when the actual condition of main storage, I/O devices, or the PSW matches the condition you set. You can set the following conditions for stopping CPs:

CP address match
: Set for monitoring main storage and stopping all CPs when a CP accesses a specific main storage location while processing non-I/O operations.

I/O address match
: Set for monitoring main storage and stopping all CPs when a CP accesses a specific main storage location while processing I/O operations.

I/O event
: Set for monitoring I/O devices for specific condition codes or status and stopping all CPs when they occur.

PSW event
: Set for monitoring the PSW and stopping all CPs when specific information or codes are stored in PSW fields.

Follow your local procedures for determining when to set conditions for stopping CPs. You can use the support element workplace to set conditions for stopping CPs.

To set conditions for stopping CPs:

1. You must be logged on the support element in the system programmer or service representative user mode.

2. Open the **Task List** from **Views** area.
3. Open **CP Toolbox** from the **Task List Work Area**.

   The CP Toolbox task list contains the following tasks that you can start:

   - **Stop on CP Address Match**
   - **Stop on I/O Address Match**
   - **Stop on I/O Event**
   - **Stop on PSW Event**
4. Open **Groups** from the **Views** area.
5. Open the **CPC** group, or any group that contains the CPC.
6. Right click on the CPC.
7. Select the **CPs** menu choice from the pop-up menu.

   This displays the CPC's CPs in the work area. The area contains the target CPs.
8. Drag and drop a CP on a task to start it.

   The Control's window displays controls for setting the conditions that you want to stop the CP.

   Use the online **Help** for the window for information about using its controls to set conditions for stopping the CP.

Tracing CP operations

Trace is a central processor (CP) function you can use to monitor CP operations by collecting data during:

- Operations that change the program status word (PSW).
- Input/output (I/O) operations.
- Coupling facility operations.

Follow your local procedures for determining when to trace CP operations. You can use the support element workplace to trace CP operations.

To trace CP operations:

1. You must be logged on the support element in the system programmer or service representative user mode, the CPC must be activated in basic mode.
2. Open the **Task List** from the **Views** area.
3. Open **CP Toolbox** from the **Task List Work Area**.

   The CP Toolbox task list contains the **Trace** task that you will start.
4. Open **Groups** from the **Views** area.
5. Open the **CPC** group, or any group that contains the CPC.

6. Right click on the CPC.
7. Select the **CPs** menu choice from the pop-up menu.
8. Drag and drop a CP on the **Trace** task to start it.

   The PSW & I/O Trace Controls window displays controls for setting up traces and managing trace data.

   Use the online **Help** for the window for more information about using its controls to set up traces and manage trace data.

Performing store status

Store status is a processor operation you can use to store the contents of a processor's registers, excluding the time-of-day (TOD) clock, in assigned storage locations. The contents of the following registers are stored by the store status operation:

- CPU timer
- Clock comparator
- Current program status word (PSW)
- Prefix
- Access registers 0-15
- Floating point registers 0-6
- General registers 0-15
- Control registers 0-15

If you have experience using other systems, you may have used a store-status key to initiate the store status operation for a processor.

Follow your local procedures for determining when to perform the store status operation. You can use the support element workplace to perform the store status operation for any eligible processor. Eligible processors include:

- Physical processors that support the image of a central processor complex (CPC) activated in basic mode.
- Logical processors that support the images of logical partitions activated in operating modes other than coupling facility mode.

To perform the store status operation:

1. You must be logged on the support element in the advanced operator, system programmer, or service representative user mode.
2. Open the **Task List** from the **Views** area.
3. Open **CP Toolbox** from the **Task List Work Area**.

   The CP Toolbox task list contains the **Store Status** task that you will start.
4. Open **Groups** from the **Views** area.
5. Open the **Images** group, or any group that contains the image.
6. Right click on the image supported by the processors you want to work with.

7. Select the **CPs** menu choice from the pop-up menu.
8. Drag and drop a processor on the **Store Status** task to start it.

   A message displays when it is completed.
9. Select **OK** to close the message when the operation completes successfully.

   If the operation does not complete successfully, follow the directions in the message to determine the problem and how to correct it.

Chapter 13. Channel path operations

This section describes tasks you can use to monitor and control the operation of specific channel paths with channel path identifiers (CHPIDs) defined in the input/output (I/O) configuration of the central processor complex (CPC).

The **CHPID Operations** task list contains the tasks, referred to here as *CHPID operations*. This section provides instructions for starting the tasks.

Configuring channel paths on or off

Configure on and *configure off* are channel path operations you can use to control whether channel paths are online or on standby in the active input/output (I/O) configuration:

- A channel path is *online* while configured on. It is in the active I/O configuration and it can be used.
- A channel path is on *standby* while configured off. It is in the active I/O configuration but it cannot be used until it is configured on.

If you have experience using other systems, you may have used a CHPID command with ON and OFF parameters to configure channel paths on and off.

You can use the support element workplace to configure channel paths on and off. However, operating systems will not be notified when you use the workplace to configure channel paths on or off. For example, if you configure off a channel path, the operating system running in any image that owns or shares the channel path is not notified, and the next operation from the operating system to the channel path will cause an error. So it is recommended you use operating system facilities rather than the support element workplace, whenever possible, to configure channel paths on and off.

To use the workplace to configure channel paths on or off:

1. You must be logged on the support element in the advanced operator, system programmer, or service representative user mode, and the CPC must be power-on reset.
2. Open the **Task List** from the **Views** area.
3. Open **CHPID Operations** from the **Task List Work Area**.

   The CHPID Operations task list contains the **Configure On/Off** task that you will start.
4. Locate the object, either the CPC or one of its images, that you want to configure channel paths on or off. One or more images is created and the active I/O configuration is established during a power-on reset of the CPC:
   - When the power-on reset puts the CPC in logically partitioned (LPAR) mode, each logical partition is an image. Locate the CPC if you want to

work with *all* channel paths in the active I/O configuration. Locate an image if you want to work only with channel paths defined for a specific logical partition.

- Otherwise, when a power-on reset puts the CPC in a basic mode, the CPC has a single image. You can locate either the CPC or its image to work with all channel paths in the active I/O configuration.

5. Open **Groups** from the **Views** area.
6. Open the **CPC** group, or any group that contains the CPC.
7. Open **Groups** from the **Views** area.
8. Open the **Images** group, or any group that contains the image.
9. Right click on the target object, either the CPC or an image, to which the target channel paths are defined.
10. Select the **CHPIDs** menu choice from the pop-up menu.

    This displays the object's channel paths in the work area. The area contains the target channel paths.
11. Select the channel paths you want to configure on or off.
12. Drag and drop the selected channel paths on the **Configure On/Off** task to start it.

    This displays the Configure On/Off window. The window lists the CHPID, current state, target state, and messages for each channel path you selected.
13. Initially, each channel path's current state and target state are the same. Use the window's controls to change the target states of the channel paths you want to configure on or off:

    - If the current state of a channel path is **Online**, toggle its target state to **Standby** if you want to configure off the channel path.
    - If the current state of a channel path is **Standby**, toggle its target state to **Online** if you want to configure on the channel path.

    Note: If you attempt to change the target state of a channel path that cannot be configured on or off, a message is displayed in the **Messages** list column to indicate changing the channel path's state is not allowed. Double-click on the message for more information about why the channel path state cannot be changed.
14. When you finish changing the target states of the channel paths you want to configure on or off, select the **Apply** push button to make each CHPID's new target state its current state.

Configuring reconfigurable channel paths in LPAR mode

When the central processor complex (CPC) is power-on reset in logically partitioned (LPAR) mode, the active input/output configuration data set (IOCDS) determines which logical partition each channel path is assigned to and whether any of the channel paths are reconfigurable. Ordinarily, channel paths assigned to a single logical partition are available only to that logical partition. That is, the channel paths cannot be configured on to other logical partitions, even after they are configured off from their assigned logical partition. But channel paths assigned to a single logical partition and defined as reconfigurable can be reassigned to other logical

partitions. That is, reconfigurable channel paths can be configured off from their assigned logical partitions and configured on to other logical partitions.

The logical partition to which a reconfigurable channel path is currently assigned is referred to here as the *owning logical partition*. The logical partition to which you want to reassign the channel path is referred to here as the *target logical partition*. Reassigning the channel path requires:

1. Configuring off the channel path from the owning logical partition, if the channel path is currently configured on.
2. Releasing the channel path from the owning logical partition, if the channel path is currently isolated.
3. Configuring on the channel path to the target logical partition.

IBM recommends you use operating system facilities rather than the support element workplace, whenever possible, to perform the steps necessary to reassign reconfigurable channel paths. However, if you must use the workplace, you can either:

- Perform each step for multiple channel paths:
  1. Use the **Configure On/Off** task to configure off the channel paths that are online. For instructions, see “Configuring channel paths on or off” on page 13-1.
  2. Use the **Release** task to release the channel paths that are isolated. For instructions, see “Releasing reconfigurable channel paths.”
  3. Use operating system facilities to configure on the channel paths to other logical partitions.
- Or perform all steps at once for a single channel path by using the **Reassign Channel Path** task. For instructions, see “Reassigning reconfigurable channel paths” on page 13-4.

Releasing reconfigurable channel paths

Release is a channel operation you can use to free reconfigurable channel paths from their assignment to isolated logical partitions.

The active input/output configuration data set (IOCDS) determines whether channel paths are reconfigurable, and which logical partition each channel path is assigned to. Each logical partition's security settings determine whether it is isolated. A logical partition's initial security settings are set by the activation profile used to activate it. Afterwards, the **Change LPAR Security** task can be used to change the settings. For more information, see “Logical partition security” on page 9-1.

Reconfigurable channel paths assigned to an isolated logical partition do not become available to other logical partitions when they are configured off. But releasing such channel paths will make them available to other logical partitions.

Channel paths that are both reconfigurable and isolated are eligible for being released. You can use the CHPIDs Work Area to locate reconfigurable channel paths assigned to isolated logical partitions. The icon label for any reconfigurable channel path displays **Reconfigurable** and either **Isolated** or **Not isolated** to indicate whether it is assigned to an isolated logical partition.

To release channel paths:

1. You must be logged on the support element in the advanced operator, system programmer, or service representative user mode.
2. The central processor complex (CPC) must be power-on reset in logically partitioned (LPAR) mode.
3. The channel paths must be defined as reconfigurable in the active input/output (I/O) configuration.
4. The channel paths must be assigned to isolated logical partitions.
5. The channel paths must be configured off.
6. Open the **Task List** from the **Views** area.
7. Open **CHPID Operations** from the **Task List Work Area**.

   The CHPID Operations task list contains the **Release** task that you will start.
8. Open **Groups** from the **Views** area.
9. Open the **CPC** group, or any group that contains the CPC.
10. Right click on the CPC to open its pop-up menu.
11. Select the **CHPIDs** menu choice.

    This displays the CPC's channel paths in the work area. The area contains the target channel paths.
12. Select the reconfigurable channel paths you want to release.
13. Drag and drop the selected channel paths on the **Release** task.
14. Select **Release** from the confirmation window to confirm your request to release the selected channel paths.

    This releases the channel paths.

Note: Upon configuring off and releasing reconfigurable channel paths from isolated logical partitions, you must use operating system facilities to configure them on to other logical partitions.

Reassigning reconfigurable channel paths

Reassign is a channel operation you can use to perform at once all the steps necessary to reassign a reconfigurable channel path from its owning logical partition to another logical partition:

1. Configuring off the channel path from its owning logical partition, if necessary.
2. Releasing the channel path, if necessary.
3. Configuring on the channel path to the other logical partition.

Any channel path that is reconfigurable is eligible for being reassigned. You can use the CHPIDs Work Area to locate reconfigurable channel paths. The icon label for a reconfigurable channel path displays **Reconfigurable**.

To reassign a channel path:

1. You must be logged on the support element in the advanced operator, system programmer, or service representative user mode.
2. The central processor complex (CPC) must be power-on reset in logically partitioned (LPAR) mode.
3. The channel paths must be defined as reconfigurable in the active input/output (I/O) configuration.
4. Open the **Task List** from the **Views** area.
5. Open **CHPID Operations** from the **Task List Work Area**.

   The CHPID Operations task list contains the **Reassign Channel Path** task that you will start.
6. Open **Groups** from the **Views** area.
7. Open the **CPC** group, or any group that contains the CPC.
8. Select the **CHPIDs** menu choice from the pop-up menu.
9. Select *one* reconfigurable channel path you want to reassign.
10. Drag and drop the selected channel path on the **Reassign Channel Path** task.

    The Reassign Channel Path window identifies the logical partition that the selected channel path is currently assigned, and lists the logical partitions to which it can be reassigned.

    Use the online **Help** for more information about using the window to reassign the channel path.
11. Select from the list the logical partition that you want to reassign the channel path, the select the **Reassign** push button.
12. Select **Reassign** from the confirmation window to confirm your request to reassign the selected channel path to the target logical partition.

    This reassigns the channel path to the logical partition.

    Note: If the target logical partition is not activated, the channel path is still configured on, but its status does not immediately become **Online**. The status remains **Standby** instead, and becomes **Online** only when the target logical partition is activated.

Setting channel path service on or off

Service on and *Service off* are channel path operations you can use to control whether channel paths are on standby in, or reserved from, the active input/output (I/O) configuration:

- A channel path is on *standby* while service is set off. It is in the active I/O configuration but it cannot be used until it is configured on. It will remain in the active I/O configuration until service is set on.

- A channel path is *reserved* while service is on. It is not in the active I/O configuration and cannot be used. It will remain out of the active I/O configuration until service is set off.

Setting service on for a channel path, which removes it from the active I/O configuration, allows running diagnostic tests on the channel path without disturbing other channel paths being used by the system. Setting service on for a channel path can be used also to remove failing channel paths from the I/O configuration so subsequent power-on resets will not attempt to initialize the failing channel paths.

If you have experience using other systems, setting service on or off for channel paths may have been referred to as taking channel paths in and out of single channel service (SCS), for which you may have used an SCS command with IN and OUT parameters.

You can use the support element workplace to set channel path service on and off.

To set channel path service on and off:

1. You must be logged on the support element in the advanced operator, system programmer, or service representative user mode, and the CPC must be power-on reset.
2. Open the **Task List** from the **Views** area.
3. Open **CHPID Operations** from the **Task List Work Area**.

   The CHPID Operations task list contains the **Service On/Off** task that you will start.
4. Open **Groups** from the **Views** area.
5. Open the **CPC** group, or any group that contains the CPC.
6. Locate the target channel paths:
7. Right click on the CPC to open its pop-up menu.
8. Select the **CHPIDs** menu choice.
9. Select the CPC's channel paths that you want to set service on or off.
10. Drag and drop the selected channel paths on the **Service On/Off** task to start it.
11. Initially, each channel path's current state and target state are the same. Use the Service On/Off window controls to change the target states of the channel paths that you want to set the service state on or off:

    - If the current state of a channel path is **Reserved**, toggle its target state to **Standby** if you want to set service off for the channel path.
    - If the current state of a channel path is **Standby**, toggle its target state to **Reserved** if you want to set service on for the channel path.

    If you attempt to change the target state of a channel path that cannot have service set on or off, a message is displayed in the **Messages** list column to indicate changing the channel path's state is not allowed. Double-click on the

message for more information about why the channel path state cannot be changed.

12. When you finish changing the target states of the channel paths that you want to set service on or off, select the **Apply** push button to make each CHPID's new target state its current state.

Resetting the I/O interface

In a multiple system environment, systems may share the control units in their input/output (I/O) configurations. A shared control unit may hold reserves on a device for one system, which provides the system with exclusive use of the device. If shared control units are holding reserves on devices for a system that becomes check stopped, the system cannot use the reserved devices, yet they remain unavailable to other systems. The unavailability of a reserved device may disturb the operation of the other systems.

Resetting the input/output (I/O) interface of channel paths that attach shared control units cause the control units to release any outstanding reserves they hold on devices. Although resetting the I/O interface will not recover the system that is check stopped, releasing the reserves on devices held for it makes the devices available to other systems.

Attention: Do not reset the I/O interface to reset channel paths that are check stopped or not operating. The reset will temporarily stop all processor clocks in the system. This will stop its processors and interrupt I/O operations on all channel paths in its I/O configuration.

Instead, to reset channel paths that are check stopped or not operating, configure them off and then configure them on.

To reset the I/O interface of a channel path:

1. You must be logged on the support element in the advanced operator, system programmer, or service representative user mode, and the CPC must be power-on reset.
2. Open the **Task List** from the **Views** area.
3. Open **CHPID Operations** from the **Task List Work Area**.

   The CHPID Operations task list contains the **Reset I/O Interface** task that you will start.
4. Open **Groups** from the **Views** area.
5. Open the **CPC** group, or any group that contains the CPC.
6. Right click on the CPC to open its pop-up menu.
7. Select the **CHPIDs** menu choice.
8. Select the CPC's channel paths for which you want to reset the I/O interfaces.
9. Drag and drop the selected channel paths on the **Reset I/O Interface** task to start it.

10. Initially, each channel path's current state and target state are the same. Use the Reset I/O Interface window's controls to change the target states of the channel paths for which you want to set the service state on or off:
    - If the current state of a channel path is **Reserved**, toggle its target state to **Standby** if you want to set service off for the channel path.
    - If the current state of a channel path is **Standby**, toggle its target state to **Reserved** if you want to set service on for the channel path.

    Note: If you attempt to change the target state of a channel path that cannot have service set on or off, a message is displayed in the **Messages** list column to indicate changing the channel path's state is not allowed. Double-click on the message for more information about why the channel path state cannot be changed.
11. When you finish changing the target states of the channel paths for which you want to set service on or off, select the **Apply** push button to make each CHPID's new target state its current state.

Performing channel problem determination

You can use the CHPIDs Work Area to determine the state and status of specific channel paths in the input/output (I/O) configuration of the central processor complex (CPC). The label for each channel path's icon includes its CHPID, state, and status. When you need more detailed information, you can use the support element workplace to perform channel problem determination. Perform channel problem determination to get the following types of information, referred to here as *problem determination information*, for a channel path:

- Channel information
- Subchannel data
- Control unit header
- Paths to a device
- Device status
- Serial link status

If you have experience using other systems, you may have performed *input/output (I/O) problem determination* to get similar information for a channel path.

To perform channel problem determination:

1. You must be logged on the support element in the advanced operator, system programmer, or service representative user mode, and the CPC must be power-on reset.
2. Open the **Task List** from the **Views** area.
3. Open **CHPID Operations** from the **Task List Work Area**.

   The CHPID Operations task list contains the **Channel Problem Determination** task that you will start.

4. Locate the image that owns or shares the channel paths that you want to perform channel problem determination. One or more images is created and the active I/O configuration is established during a power-on reset of the CPC:
   - When the power-on reset puts the CPC in logically partitioned (LPAR) mode, each logical partition is an image.
   - Otherwise, when a power-on reset puts the CPC in a basic mode, the CPC has a single image.
5. Open **Groups** from the **Views** area.
6. Open the **Images** group, or any group that contains the image.
7. Right click on the image to which the target channel paths are defined to open its pop-up menu.
8. Select the **CHPIDs** menu choice from the pop-up menu.
9. Select *one* target channel path that you want to perform channel problem determination.
10. Drag and drop the selected channel path on the **Channel Problem Determination** task to start it.

    The Channel Problem Determination window lists the types of problem determination information you can get for the selected channel path.

    Note: The CHPID of the channel path you selected to start the task is the task's initial input. One or more windows are displayed if additional input is needed to display the type of information you want.
11. Select the radio button beside the type of problem determination information you want, then select **OK**.

    Follow the instructions on each subsequent window, if any, to provide the additional input needed to display the type of information you selected.

    Upon providing the additional input, if any, the channel path's problem determination information is displayed.

Identifying channel definition errors

Performing a power-on reset of the central processor complex (CPC) includes defining its input/output (I/O) configuration and allocating its storage. A *channel definition error* occurs when either:

- The definition of a channel defined in the I/O configuration does not match the characteristics of the channel hardware installed in the CPC.
- The channel type of a channel defined in the I/O configuration is incompatible with the CPC's storage allocation.

You can use the CHPIDs Work Area to locate channel paths that have definition errors. The icon label for any channel path that has a definition error displays **Definition error** for its status. After locating channel path that has a definition error, perform channel problem determination to determine the channel path's exact definition error.

To determine a channel path's exact definition error:

1. You must be logged on the support element in the advanced operator, system programmer, or service representative user mode.

2. The CPC must be power-on reset, and the status displayed for the channel path must be **Definition error**.
3. Start the **Channel Problem Determination** task for *one* channel path that has a definition error. See “Performing channel problem determination” on page 13-8 for instructions for starting the task.

   This displays the Channel Problem Determination window. The window lists the types of problem determination information you can get for the selected channel path.
4. Select the **Analyze Channel Information** radio button, then select **OK**.

   This displays the Analyze Channel Information window. The window displays channel information for the selected channel path.
5. Select the **Error details** push button.

   This displays a message that describes the selected channel path's exact definition error.

   Note: The **Error details** push button is *not* available if the status displayed for the selected channel path is *not* **Definition error**.

Chapter 14. Maintaining Security

The security of information assets is controlled by user identification with passwords. Access to security functions or sensitive data is restricted by user modes. The access administrator user mode is used to set up user identifications and passwords, and allow access to a particular user mode of operation. This user mode also controls authorization for Operations Management requests. The system programmer user mode can access sensitive data and control remote access.

Each user is given access to the system through a user identification and password. This password should be kept confidential and changed if necessary to maintain security. Both the user identification and password must have a minimum of four characters with a maximum of eight characters.

Enabling the application programming interface

You can allow other system management applications to use the Management Application Programming Interfaces (APIs) to the Support Element Console Application. Management APIs allow applications to exchange information about objects and send commands to an object managed by the Support Element Console Application.

To change your Application Programming Interface:

1. Open the **Console Actions** from the Views area.
2. Open **Support Element Settings** from the Console Actions Work Area.

   Attention: This task requires a system reboot. Rebooting ends hardware and software activity. The system with be put into a non-operating state. It is recommended to deactivate the CPC prior to rebooting the system to avoid possible data loss.
3. Select the API page.

Use the online **Help** for more information on completing this task.

Customizing your automatic logon

You can customize your automatic logon feature for the support element console by enabling or disabling it.

When enabled, the automatic logon feature will log on the support element console automatically using the userid you specify whenever the support element console is powered-on.

To change your automatic logon:

1. Open the **Console Actions** from the Views area.
2. Open **Customize Automatic Logon** from the Console Actions Work Area.

The Customize Automatic Logon window is displayed to allow you to select the userid that you want the support element console to use when it is powered on. Online help is available to guide you through completion of the task.

Assigning domain security to your support element console

If you want to customize domain security, use this task to establish and maintain different domains for multiple Hardware Management Consoles and support element consoles attached to the same local area network (LAN). Ordinarily, to add or move a CPC from a domain is done from the Hardware Management Console, but this can be accomplished from the support element console.

To define the domain security:

1. Open the **Console Actions** from the Views area.
2. Open **Domain Security**.

   Attention: This task automatically reboots the system. Rebooting ends hardware and software activity. The system with be put into a non-operating state. It is recommended to deactivate the CPC prior to rebooting the system to avoid possible data loss.

Use the online **Help** for more information on completing this task.

Customizing your user profiles for access

Note: This task is available only in *Access Administrator* mode.

Enables you to create, modify, or delete user profiles for the user modes on the Support Element Console or for service mode on the support element. A user profile consists of a user identification, password, and user mode. The user identification and password are used to verify a user's authorization to log on the Support Element Console. The user mode determines the user's level of access to Support Element Console tasks and operations.

To customize a user profile:

1. Open **Console Actions** from the **Views** area.
2. Open **User Profiles** from the **Console Action Work Area**. The **User Profiles** notebook window is displayed.

Use the online Help to get additional information for working with a user profile.

The Support Element Console has a secured Desktop. You can select whether or not the Desktop on the support element is displayed to all users or to only selected users. By checking the **Enable secure desktop** box on the **Options** page of the User Profiles notebook window, no user modes will have access to the Desktop. If

Enable secure desktop is not checked, all user modes will have access to the desktop. If you want certain user modes or particular userids to have access to the Desktop, do the following:

1. Open **Console Actions** from the **Views** area.
2. Open **User Profiles** from the **Console Action Work Area**. The **User Profiles** notebook window is displayed.
3. Select the notebook tab of the user mode you want.
4. If the *userid* you want to give access to already exists in the window list, select the *userid* from the list, and then select the **Open** push button. The **Open a User Profile** window is displayed.

   or

   If you are creating a new *userid,* select the **Create** push button. The **New User Profile** window is displayed.
5. Check the **Allow access to desktop** box and then select the **OK** push button. This userid now has access to the Desktop.

   Note: Repeat **steps 3** through **5** for each additional userid you want to give access to the Desktop.
6. Close the **User Profiles** notebook window.

If you select Secure Desktop for all or any user modes, you must not select the Warp Center option that shows the Warp Center only when the mouse pointer is over the Warp Center area.

Note: If a person, who has access to the Desktop, is logged on and has opened up one or more application windows (such as, OS/2 Window, TCP/IP Configuration), they must close those applications before logging off the Support Element Console; otherwise, those applications will be available to anyone logging on to the Support Element Console even if their userid does not have access to the Desktop. If any applications are left open, they will be left open for any other userid until the Support Element Console is rebooted.

Attention: When using the OS/2 desktop Lock-out feature, pressing the Ctl-Alt-Del keys, if they are disabled, will cause the system to perform a system reboot.

This task also lets you give access to particular userids for the Support Element Console Web Server. The Web Server is a remote capability that allows an operator to monitor and/or control defined CPCs, CPC images, or groups from a remote site to a local Support Element Console through a Web browser. For more information on the Web Server and how to use it, see “Remote Control Using the Web Server” on page A-2.

Note: The Web Server is available in *Operator, Advanced Operator,* and *System Programmer* modes.

To give access to the Web Server:

1. Open **Console Actions** from the **Views** area.
2. Open **User Profiles** from the **Console Action Work Area**. The **User Profiles** notebook window is displayed.
3. Select the notebook tab of the user mode (Operator, Advanced Operator, or System Programmer) you want.

4. If the *userid* you want to give access to already exists in the window list, select the *userid* from the list, and then select the **Open** push button. The **Open a User Profile** window is displayed.

   or

   If you are creating a new *userid,* select the **Create** push button. The **New User Profile** window is displayed.

5. Check the **Allow access through Web Server** box and then select the **OK** push button. This userid now has access to the Web Server.

   Note: Repeat **steps 3** through **5** for each additional userid you want to give access to the Web Server.

6. Close the **User Profiles** notebook window.

Customizing product engineering access

You can verify or change the authorization of IBM Product Engineering access to the support element console.

With access authority, IBM Product Engineering can log on the support element console in an exclusive user mode that provides tasks and operations for problem determination.

Product Engineering access is provided by a reserved password and permanent user identification. You cannot view, discard, or change the password and user identification, but you can control their use for accessing the support element.

Use this task to control whether the support element console accepts the PE user identification and password for logging on. This task is only available to users with access administration authorization.

To customize your product engineering access:

1. Open the **Console Actions** from the Views area.
2. Open **Customize Product Engineering**.

The Customize Product Engineering Access window is displayed to allow you to authorize or to not authorize Product Engineering access to your support element console.

Use the online **Help** for more information on completing this task.

Customizing User Tasks

You can customize the task bars and/or tasks that are available to a user after logging on the support element console

This task is only available to a user with access administration authorization.

The tasks and task bars can be customized in the following ways:

- New task bars added
- New tasks added to a task bar
- Existing task bars removed
- Existing tasks removed from a task bar

To use **Customize User Tasks**:

1. Open the **Console Actions** from the Views area.
2. Open **Customize User Tasks**.

The Customize User Tasks window is displayed. Select the userid and use the lists provided to tailor the tasks that you want for each user.

Use the online **Help** for more information on completing this task.

Chapter 15. Operation of the console

This section describes the tasks from the **Console Actions** task list you can use to monitor and operate the support element console.

Keeping records of console operations and activities

The support element console automatically keeps records of significant operations and activities, referred to as *console events*, performed either:

- Manually by a console operator.
- Through Management-type Application Programming Interfaces (APIs) to the Support Element Console Application.
- Automatically by the Support Element Console Application.
- Through an Operations Management focal point.

Some console events simply indicate an operation or activity occurred. For example, a console event is logged when a console operator logs on the console.

Other console events are logged in pairs, to indicate when an operation or activity began and when it ended. For example, a console event is logged when a power-on reset is started, and another console event is logged when the power-on reset ends. Console events logged when an operation or activity ends typically also indicate whether the operation or activity succeeded or failed.

Viewing console events

You can use the support element workplace to start the console action for viewing console events.

To view console events:

1. Open the **Console Actions** from the **Views** area.
2. Double-click on the **View Console Events** to display the Views Console Events window.

   Use the online **Help** for more information about using the window to review the console events.

Monitoring and managing outgoing modem transmissions

When performing a support element task or operation requires transmitting data to a remote system, a request to transmit the data is sent to the phone server for the

support element. The support element's *phone server* is the console that provides modem and telecommunications services to it.

Enabling the phone server service of a support element makes it its own phone server. The support element will use its own modem, as needed, for transmitting data to remote systems.

The support element can process only one request to transmit data at a time. Requests to transmit data are put on the support element's *remote support telephone queue* until they can be processed. The support element manages its remote support telephone queue automatically. It puts requests on the queue and processes them in the order in which they are received. But you can manage the queue manually, if necessary, to stop transmissions, move priority requests ahead of others, or delete requests.

You can use the support element workplace to start a console action for manually managing on the support element's remote support telephone queue.

To manually manage the support element's remote support telephone queue:

1. The support element's phone server service must be enabled. (the support element must be its own phone server)
2. Open the **Console Actions** view on the support element workplace.

   This opens the Console Actions Work Area. The work area contains the console action you will start: **Remote Support Telephone Queue**.
3. Double-click on the **Remote Support Telephone Queue** console action to start it.

   This displays the Remote Support Telephone Queue window. The window lists the requests to transmit data, if any, currently on the support element's remote support telephone queue. The window's **Options** menu provides menu choices for managing both the entire queue and the individual requests to transmit data.

   Move the cursor to any menu choice in the **Options** menu and request help for more information about using the choice to manage the queue or individual transmission requests. Press **F2** to request help for the window.

Viewing Network Diagnostic Information

You can use the support element workplace to start the task to view network diagnostic information on your support element console for your LAN, TCP/IP and SNA connection.

The LAN notebook page displays the contents of the LANTRAN.LOG file. The TCP/IP initial notebook page can be used to send an echo request (ping) to a remote host to see if the host is accessible. Other tabs on the TCP/IP notebook page include: Interfaces, Addresses, Routes, ARP, Sockets, TCP, UDP, IP, ICMP, and Memory Buffers. The SNA notebook page displays information about the active configuration. Other tabs on the notebook page include: Link Definitions, Active Links, and Sessions.

To view your LAN, TCP/IP, or SNA information:

1. Open the **Console Actions** from the **Views** area.
2. Double-click on the **Network Diagnostic Information** to display the window.
3. Select the notebook tab for LAN, TCP/IP, or SNA to view the network diagnostic information.

   Use the online **Help** for more information about using the window to view the network diagnostic information.

Pinging the TCP/IP Address

To ping a TCP/IP address:

1. Open the **Network Diagnostic Information** notebook.
2. Select the TCP/IP page and type the TCP/IP address you want to ping.
3. Select the **ping** push button.

Viewing security logs

You can use the support element workplace to start the console action for viewing security logs for the CPC.

To view security logs:

1. Open the **Console Actions** from the **Views** area.
2. Open **View Security Logs** from the **Console Actions Work Area**. The View Security Logs window is displayed.
3. The window displays the **Security Event** and the **Date** and **Time** the security log is created.
4. If you need to view a security event log that is not displayed. Select the **Show Earlier Events** or **Show Later Events** push button.

Use the online **Help** for more information about using the window to review the console events.

Chapter 16. Settings for console operations

This section describes tasks from the **Console Actions** task list you can use to customize settings that control how the support element console operates.

Setting colors of unacceptable status

You can check the colors set for indicating an object's unacceptable status by double-clicking on an object to open its *details window*. This window includes detailed information about the object, including a list of its unacceptable statuses and the colors used to indicate them. You can use an object's details window to change its settings that determine whether a status is acceptable and unacceptable. But to change the colors set for indicating unacceptable statuses, you must change the support element console's settings.

To set the console's colors of unacceptable status:

1. Open the **Console Actions** from the **Views** area.

   The work area contains the **Support Element Settings** action that you will start.

2. Double-click on the **Support Element Settings** console action to start it.

   Attention: This tasks requires a system reboot. Rebooting ends hardware and software activity. The system will be put into a non-operating state. It is recommended to deactivate the CPC prior to rebooting the system to avoid possible data loss.

   Use the online **Help** for more information about using the window to change the console's settings.

3. Click on the **Colors** page tab.

   The first page of the console's color settings is labelled: Page 1 of 3.

   Use the online **Help** for more information on using the window to change the console's colors set for indicating unacceptable statuses.

4. To check the color currently set for a status, select the status term from the list labelled **Status values**.

   This highlights the color, in the **Exception Color** group box, currently set for the status.

   Notes:

   a. Use the group box's horizontal scroll bar, if necessary, to scroll the list to the highlighted color.

   b. To use black and white patterns instead of colors for indicating unacceptable statuses, mark the **Use patterns instead of colors** check box. The check box displays a check mark when you mark it.

5. To change the color set for a status:

   a. Select the status term from the **Status values** list.

b. Select the color from the **Exception Color** group box.

c. Select the **Apply** push button.

6. When you finish changing the colors set for indicating unacceptable statuses, close the notebook by double-clicking on its system menu icon, located in the upper left corner of the notebook.

Setting colors of summarized system status

You can change the support element console's settings to change the colors set for indicating the summarized status of the system.

To set the console's colors of summarized system status:

1. Open the **Console Actions** from the **Views** area.

   The work area contains the **Support Element Settings** action that your will start.

2. Open the **Support Element Settings** in the Console Actions Work Area.

   Attention: This tasks requires a system reboot. Rebooting ends hardware and software activity. The system will be put into a non-operating state. It is recommended to deactivate the CPC prior to rebooting the system to avoid possible data loss.

   The pages display the support element console's current settings.

   Use the online **Help** for more information on using the window to change the console's settings.

3. Select on the **Colors** page tab.

   This displays the first page of the console's color settings. The page is labelled: Page 1 of 2.

4. Locate the paging buttons in the lower right corner of the page, and click on the right-pointing button.

   This displays the second page of the console's color settings. The page is labelled: Page 2 of 2.

   Use the online **Help** for more information on using the window to change the console's colors set for summarized system status.

5. To check the color currently set for a summarized system status, select either **Views area background no exceptions** or **Views area background exceptions** from the list labelled **Items**.

   This highlights the color, in the **Item Color** group box, currently set for the summarized system status.

Notes:

a. Use the group box's horizontal scroll bar, if necessary, to scroll the list to the highlighted color.

b. To use black and white patterns instead of colors for summarized system statuses, mark the **Use patterns instead of colors** check box. The check box displays a check mark when you mark it.

6. To change the color set for a summarized system status:

   a. Select either **Views area background no exceptions** or **Views area background exceptions** from the **Items** list.

   b. Select the color from the **Item Color** group box.

   c. Select the **Apply** push button.

7. When you finish changing the colors set for summarized system statuses, close the notebook by double-clicking on its system menu icon, located in the upper left corner of the notebook.

Setting colors of message indicators

You can change the support element console's settings to change the colors set for indicating messages were received.

To set the console's colors of message indicators:

1. Open the **Console Actions** from the **Views** area.

   The work area contains the **Support Element Settings** action that you will start.

2. Open the **Support Element Settings** in the Console Actions Work Area to start it.

   Attention: This tasks requires a system reboot. Rebooting ends hardware and software activity. The system will be put into a non-operating state. It is recommended to deactivate the CPC prior to rebooting the system to avoid possible data loss.

   The pages display the support element console's current settings.

   Use the online **Help** for more information on using the window to change the console's settings.

3. Select on the **Colors** page tab.

   The first page of the console's color settings is labelled: Page 1 of 2.

4. Locate the paging buttons in the lower right corner of the page, and click on the right-pointing button.

   The second page of the console's color settings is labelled: Page 2 of 2.

   Use the online **Help** for more information on using the window to change the console's colors set for message indicators.

5. To check the color currently set for a message indicator, select either **Hardware Messages Pending** or **Operating System Messages Pending** from the list labelled **Items**.

   This highlights the color, in the **Item Color** group box, currently set for the message indicator.

   Notes:

   a. Use the group box's horizontal scroll bar, if necessary, to scroll the list to the highlighted color.

   b. To use black and white patterns instead of colors for message indicators, mark the **Use patterns instead of colors** check box. The check box displays a check mark when you mark it.

6. To change the color set for a message indicator:

   a. Select either **Hardware Messages Pending** or **Operating System Messages Pending** from the **Items** list.

   b. Select the color from the **Item Color** group box.

   c. Select the **Apply** push button.

7. When you finish changing the colors set for message indicators, close the notebook by double-clicking on its system menu icon, located in the upper left corner of the notebook.

Synchronizing the support element TOD clock and the CPC TOD clock

Both the central processor complex (CPC) and its support element have time-of-day (TOD) clocks. The time and date of both TOD clocks should be the same or very nearly the same. For this reason, the TOD clocks are automatically synchronized with each other as follows:

- If the CPC does not or cannot use a System Complex (Sysplex) Timer as a time source, the CPC TOD clock is synchronized with the support element TOD clock whenever a power-on reset of the CPC is performed.
- The support element TOD clock is synchronized to the CPC TOD clock whenever the CPC TOD clock is changed either manually or automatically:
  - You can use SET CLOCK or a similar operating system command to manually set the CPC TOD clock.
  - If the CPC uses a Sysplex Timer® as a time source, changing the time, date, or time-zone offset of the Sysplex Timer automatically synchronizes the CPC TOD clock to the Sysplex Timer.
- At 11:00PM on the support element TOD clock, it is synchronized with the CPC TOD clock if:
  - The CPC is operating.
  - And the support element TOD clock was *not* set manually since the TOD clocks were last synchronized.

  Otherwise:
  - If the CPC is not operating, the support element TOD clock remains unchanged.

– Or if the CPC is operating, but the support element TOD clock was set manually since the TOD clocks were last synchronized, then both TOD clocks remain unchanged and are not synchronized.

Using a Sysplex Timer as a time source for the CPC is intended to make manually setting the CPC TOD clock unnecessary. It prevents manually setting the support element TOD clock.

But if the CPC does not or cannot use a Sysplex Timer as a time source, you can manually set either TOD clock. Instructions for setting the support element TOD clock are provided in the next topic. For instructions for setting the CPC TOD clock, see “Setting the CPC TOD clock manually” on page 6-55.

Setting the support element time-of-day clock manually

You can use the support element workplace to start the console action for manually setting the support element time-of-day (TOD) clock.

To set the support element TOD clock:

1. Open the **Console Actions** from the **Views** area.
2. Open the **Customize Date/Time** task in the Console Actions Work Area to start it.

   The Customize Support Element Date and Time window displays the current date, time, and time-zone offset set for the support element TOD clock, and provides controls for changing the settings.

   Use the online **Help** for more information on using the window to set the support element TOD clock.

Authorizing system operation by remote consoles

The support element used for monitoring and operating S/390 Multiprise 3000 Enterprise Server systems provide a *remote operation service* that supports using a remote console for monitoring and operating the system also. A *remote console* is a workstation installed at a remote location, connected to the support element, and customized for operating the support element and its central processor complex (CPC).

The setting of the remote operation service determines whether remote consoles can be used to operate the support element and CPC:

- Disable the service to prevent using remote consoles to operate the support element and CPC. This is the default setting. The support element will not allow remote consoles to establish the communications link necessary to conduct remote operations while the service is disabled.
- Enable the service to authorize using remote consoles to operate the support element and CPC.

  Note: Enabling the support element's remote operation service is one part of the procedures you should follow for getting ready to use remote

consoles for remote operation of the support element and CPC. See Appendix A, “Remote Operations” on page A-1 for more information about remote operations and for instructions for installing and customizing remote consoles.

To enable or disable the support element's remote operation service:

1. You must be logged on the support element in the system programmer or service representative user mode.
2. Open the **Console Actions** from the **Views** area.
3. Open the **Enable Console Services** task in the Console Actions Work Area to start it.

   This displays the Enable Support Element Console Services window.
4. Locate the Remote Operation group box on the Enable Support Element Console Serviced window. It lists choices for enabling or disabling the remote operation service. The selected choice indicates the current setting of the service.

   Move the cursor to any choice in the group box and use the Online **Help** for more information about the choices. Press **F2** for help on the window.
5. Select a different choice to change the setting, then select **OK** to save the setting and close the window.

   The new setting takes effect immediately.

Controlling the system exclusively from the support element console

The system's support element serves both as a console for controlling the system and as an interface that other supported consoles and applications can use for controlling the system. For example:

- Properly customized Hardware Management Consoles with network connections to the support element can be used to monitor and operate the system.
- System control or automation applications, such as System Automation for OS/390 Processor Operations Component (SA OS/390 Procops) and Automated Operations Control (AOC), running on systems with network connections the support element can be used to send it commands for controlling the system.

The support element console does not have *exclusive control* of the system. That is, the system can be controlled from the support element console and from any other supported consoles and applications using the support element as a system interface, all at the same time.

You can temporarily give the support element console exclusive control of the system, if necessary, to prevent other consoles and applications from controlling it. For example, you may want to give the support element console exclusive control to prevent other consoles and applications from starting disruptive operations, such

as a system activation or power-on reset, while you are using the support element console to perform system operations.

The setting of the *exclusive control service* of a support element determines whether it has exclusive control of the system:

- The setting is disabled by default. The system can be controlled from the support element console and from any other supported consoles and applications using the support element as a system interface.
- Enable the setting to temporarily allow using only the support element console to control the system.
- Disable the setting again to resume controlling the system from the support element console and from any other supported consoles and applications using the support element as a system interface.

To enable or disabling the support element's exclusive control service:

1. You must be logged on the support element in the system programmer or service representative user mode.
2. Open the **Console Actions** from the **Views** area.

   The work area contains the **Enable Console Services** action that you will start.

   Attention: This tasks requires a system reboot. Rebooting ends hardware and software activity. The system will be put into a non-operating state. It is recommended to deactivate the CPC prior to rebooting the system to avoid possible data loss.
3. Double-click on the **Enable Console Services** console action to start it.

   This displays the Enable Support Element Console Services window.
4. Locate the Exclusive Control group box from the Enable Support Element Console Services window. It lists choices for enabling or disabling the exclusive control service. The selected choice indicates the current setting of the service.

   Move the cursor to any choice in the group box and use the Online **Help** for more information about the choices. Press **F2** for help on the window.
5. Select a different choice to change the setting, then select **OK** to save the setting and close the window.

Enabling Netfinity Services

You can use the support element workplace to control whether the support element is to be managed by Netfinity®. Refer to the Netfinity documentation for additional information.

To enable or disable netfinity:

1. You must be logged on the support element in the system programmer user mode.

2. Open the **Console Actions** from the **Views** area.
3. Open the **Enable Console Services** task in the Console Actions Work Area to start it.

   Attention: This tasks requires a system reboot. Rebooting ends hardware and software activity. The system will be put into a non-operating state. It is recommended to deactivate the CPC prior to rebooting the system to avoid possible data loss.

   This displays the Enable Support Element Console Services window.
4. Locate the Netfinity group box from the Enable Support Element Console Services window. It lists choices for enabling or disabling Netfinity. The selected choice indicates the current setting of the service.

   Move the cursor to any choice in the group box and use the Online **Help** for more information about the choices.
5. Select the **Enabled** or **Disabled** radio button, then select **OK** to save the setting.

   If you selected **Enabled**, the Network Driver Configuration window displays that allows you to configure Netfinity.

Use the online **Help** for more information on using the network driver configuration window.

Providing modem services to the support element

When performing a support element task or operation requires establishing a communication link to a remote system, a request to establish the link is sent to the phone server for the support element. The support element's *phone server* is the console that provides modem and telecommunications services to it.

Only a Hardware Management Console can be a phone server for *integrated* support elements, since such support elements are not equipped with a modem. A Hardware Management Console serves as the support element's phone server if:

- The support element's central processor complex (CPC) is defined to the Hardware Management Console and, in the CPC's definition, the Hardware Management Console is set to act as the CPC's phone server.
- And the Hardware Management Console's *phone server service* is enabled.

See *Hardware Management Console Operations Guide* for instructions for defining CPCs and for enabling or disabling a Hardware Management Console's phone server service.

A Hardware Management Console can be a phone server for the support elements. The support element is equipped with an external modem and telecommunications software. The support element can be a phone server for itself if a Hardware Management Console is not available or is not used as its phone server. The setting of the *phone server service* of a support element determines whether it is its own phone server:

- The setting is enabled by default, which makes a support element its own phone server. The support element will use its own modem, as needed, for telecommunications with remote systems.

- Disable the service only if the CPC becomes part of a Parallel System Complex (Parallel Sysplex), in which a Hardware Management Console will serve as the phone server for the CPC's support element.

To enable or disable the support element's phone server service:

1. you must be logged on the support element in the system programmer or service representative user mode.
2. Open the **Console Actions** from the **Views** area.
3. Open the **Enable Console Services** task in the Console Actions Work Area to start it.

   Attention: This tasks requires a system reboot. Rebooting ends hardware and software activity. The system will be put into a non-operating state. It is recommended to deactivate the CPC prior to rebooting the system to avoid possible data loss.

   This displays the Enable Support Element Console Services window.
4. Locate the Phone Server group box. It lists choices for enabling or disabling the phone server service. The selected choice indicates the current setting of the service.

   Move the cursor to any choice in the group box and use the Online **Help** for more information about the choices. Press **F2** for help on the window.
5. Select a different choice to change the setting, then select **OK** to save the setting and close the window.

Performing Problem Analysis of optical errors

The support element automatically and continuously monitors itself and the central processor complex (CPC) for problems. If the support element detects a problem, it uses a knowledge-based expert system called *Problem Analysis* to automatically:

- Analyze the problem, attempt to determine its cause, and determine whether service is required to correct the problem.
- Issue a hardware message to notify you of the problem. Information provided with the message includes a detailed description of the problem and instructions for correcting it or calling for service.
- Send problem information for optical errors to a designated console, if available, for additional analysis.

Optical errors are problems that may affect more than one CPC in a Parallel System Complex (Parallel Sysplex). Currently, optical errors for which additional analysis is available include:

- ESCON® channel problems
- Coupling facility channel problems

A Hardware Management Console can analyze optical errors for the support elements if Hardware Management Console is not available or is not used to analyze optical errors.

See *Hardware Management Console Operations Guide* for instructions for enabling or disabling a Hardware Management Console's optical error analysis setting.

The *optical error analysis setting* of a support element determines whether it analyzes its own optical errors:

- The setting is disabled by default. The support element will perform Problem Analysis, but will not perform additional analysis of optical errors.
- Enable the setting to allow the support element to perform its own optical error analysis if:
  - The CPC uses ESCON channels or coupling facility channels.
  - *And* a Hardware Management Console does *not* perform optical error analysis for the support element.
- Disable the setting again only if the CPC becomes part of a Parallel Sysplex, in which a Hardware Management Console will perform optical error analysis for the CPC's support element.

To enable or disable the support element's optical error analysis setting:

1. You must be logged on the support element in the system programmer or service representative user mode.
2. Open the **Console Actions** from the **Views** area.
3. Open the **Enable Console Services** task in the Console Actions Work Area to start it.

   Attention: This tasks requires a system reboot. Rebooting ends hardware and software activity. The system will be put into a non-operating state. It is recommended to deactivate the CPC prior to rebooting the system to avoid possible data loss.

   This displays the Enable Support Element Console Services window.
4. Locate the Optical Error Analysis group box. It lists choices for enabling or disabling the optical error analysis setting. The selected choice indicates the current setting.

   Move the cursor to any choice in the group box and use the Online **Help** for more information about the choices. Press **F2** for help on the window.
5. Select a different choice to change the setting, then select **OK** to save the setting and close the window.

Authorizing the support element to answer calls automatically

When the *remote operation service* of a support element is enabled, operators at remote sites can operate the support element and central processor complex (CPC) by establishing a communications link between a remote console and the support element. Similarly, when IBM is your service provider for the CPC, service representatives at IBM can perform problem determination and other service procedures by establishing a communications link between the IBM Service Support System and the support element.

In either case, remote consoles or remote systems can attempt to establish a communications link with a support element by dialing the support element's modem. But the link will be established only if the support element answers the incoming call. The setting of the *automatic call answering service* of a support element determines whether it answers incoming calls automatically:

- Enable the service to authorize the support element to answer incoming calls automatically, thereby authorizing remote consoles and remote systems to establish communications links to the support element.
- Disable the service to prevent the support element from answering incoming calls, thereby preventing remote consoles and remote systems from establishing communications links to the support element.

  Note: Disabling the automatic call answering service does *not* prevent:

  – The support element from making outgoing calls when performing a support element task or operation requires establishing a communication link to a remote system.

  – Access to the support element through a local area network (LAN) connection.

To enable or disable the support element's automatic call answering service:

1. You must be logged on the support element in the advanced operator, system programmer, or service representative user mode.
2. Open the **Console Actions** from the **Views** area.
3. Open the **Enable Console Services** task in the Console Actions Work Area to start it.

   Attention: This tasks requires a system reboot. Rebooting ends hardware and software activity. The system will be put into a non-operating state. It is recommended to deactivate the CPC prior to rebooting the system to avoid possible data loss.

   This displays the Enable Support Element Console Services window.
4. Locate the Automatic Call Answering group box. It lists choices for enabling or disabling the automatic call answering service. The selected choice indicates the current setting of the service.

   Move the cursor to any choice in the group box and use the Online **Help** more information about the choices. Press **F2** for help on the window.

5. Select a different choice to change the setting, then select **OK** to save the setting and close the window.

Setting up the support element as an S/390 application enabling technology control center

The OS/390 Application Enabling Technology system uses the services of S/390 hardware and software to provide an application platform for users. The OS/390 Control Center is an OS/2 application that runs on the support element connected to an EZ Application Enabling system. It provides a graphical user interface application developers and system administrators can use to start the EZ Application Enabling system, apply service, and perform other tasks.

Note: For information and instructions for setting up an EZ Application Enabling system, see *OS/390 EZ Application Enabling Customization Guide*, GC28-1994.

To enable or disable the OS/390 Application Enabling Technology system:

1. You must be logged on the support element in the access administrator or system programmer user mode.
2. Open the **Console Actions** from the **Views** area.
3. Open the **Enable Console Services** task in the Console Actions Work Area to start it.

   This displays the Enable Support Element Console Services window.
4. Locate the OS/390 Application Enabling Technology box and select the **Enabled** radio button.
5. Select **OK** to save the setting.
6. Customize the API page of the support element's settings notebook to enable APIs for the support element. (see “Enabling the application programming interface” on page 14-1)

   After you enable the service, you must shut down and reboot the console to display the **OS/390 EZ Control Center** icon on the console's desktop. Then, to use the EZ Control Center see *OS/390 Application Enabling Technology: System's Administrator's Guide*, GC28-1993

Use the online **Help** for more information on using the window to complete this task.

Enabling the Availability and Operations Manager (AO Manager) Bridge

The Availability and Operations Manager (AO Manager) Bridge software allows the support element to communicate with an IBM AO Manager system. The AO Manager is a service offering you can purchase to control and automate the operation of a systems center. You can set up a support element to run its AO Manager Bridge software if:

- An AO Manager system is installed for controlling the systems center that includes the support element's CPC.
- The CPC's support element is physically connected to the AO Manager System.
- You want the AO Manager to monitor and control the CPC.

To set up a support element to communicate with the AO Manager system:

1. You must be using a support element, and you must be logged on the support element in the Access Administrator or System Programmer user mode.
2. Open the **Console Actions** from the **Views** area.
3. Open the **Enable Console Services** task in the Console Actions Work Area to start it.

   Attention: This tasks requires a system reboot. Rebooting ends hardware and software activity. The system will be put into a non-operating state. It is recommended to deactivate the CPC prior to rebooting the system to avoid possible data loss.

   This displays the Enable Support Element Console Services window.
4. Locate the AO Manager box and select the **Enabled** radio button.
5. Select **OK** to save the setting.

   After you enable the service, you must shut down and reboot the console.

   Note: There is additional configuration needed to enable the AO Manager system to communicate with the Support Element. See the documentation provided with the AO Manager system.

Use the online **Help** for more information on using the window to complete this task.

Enabling or Disabling Ctl-Alt-Del

You can use the support element workplace to disable the Ctl-Alt-Del keys. When disabled, pressing the Ctl-Alt-Del keys prevents OS/2 from performing a system reboot.

Attention: When using the OS/2 desktop Lock-out feature, pressing the Ctl-Alt-Del keys, if they are disabled, will cause the system to perform a system reboot.

To disable or enable Ctl-Alt-Del:

1. You must be logged on the support element in the Access Administrator or System Programmer user mode.
2. Open the **Console Actions** from the **Views** area.

3. Open the **Enable Console Services** task in the Console Actions Work Area to start it.

   This displays the Enable Support Element Console Services window.

4. Locate the Clt-Alt-Del group box from the Enable Support Element Console Services window.

5. Select the **Disable** or **Enable** radio button.

6. Select **OK** to save the setting.

Use the online **Help** for more information on using the window to complete this task.

Configuring 3270 Emulators

You can use this task to configure the support element console's 3270 emulator. The 3270 emulator is an OS/2 application that allows 3270 terminal emulation at the console to an S/390 host. Configure the emulator to set up whether and how you want 3270 emulator sessions started whenever the Support Element Application is started.

The connection adapter installed in the support element console determines your options for configuring its 3270 emulator. Your support element console can have either a Distributed Function Terminal (DFT) card or token-ring or ethernet adapter.

Note: If both a Distributed Functions Terminal (DFT) card and a Token-Ring or Ethernet adapter are installed, then your options for configuring the emulator are determined by the DFT card.

You can start 1 or 2 emulator sessions if the console has a DFT card or TCP/IP connection to the host. You can start one emulator session if the console has a SNA connection to the host.

To configure your console for a 3270 emulator session:

1. You must be logged on the Support Element in the Access Administrator or System Programmer user mode.
2. Open **Console Actions** in the **Views** area.
3. Open **Configure 3270 Emulators** in the Console Actions Work Area to start it.

   This displays the Configure 3270 Emulators notebook window. After you configure your console, you must shut down and reboot the console.

   Use the online **Help** for more information on using the window to configure the console's 3270 emulator.

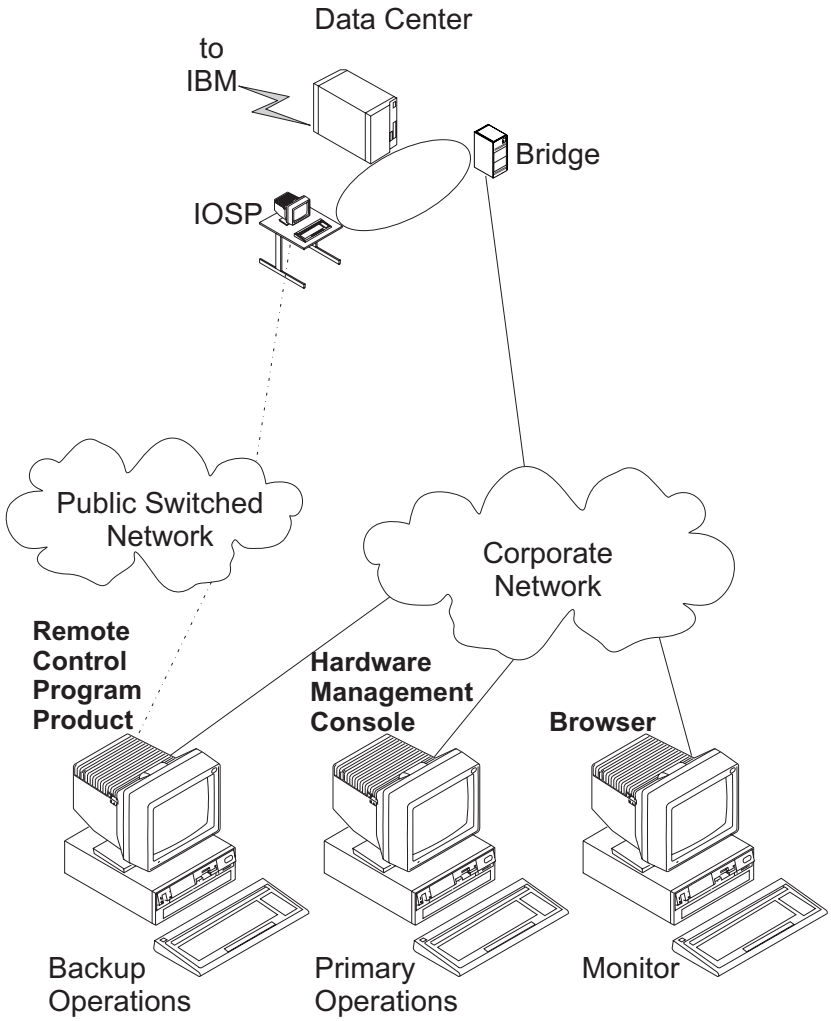
Appendix A. Remote Operations

The ability to monitor or control a system from a central or remote location creates a powerful tool for problem determination and diagnosis and operations assistance. This remote capability can save time and money and increase the productivity of support staff. Technical expertise can be centralized, reducing the need for highly skilled personnel at remote locations.

There are several options available for controlling systems from a remote location:

- Support Element Console
- Web browser
- Remote control program management product

Choosing the best option involves understanding your remote control needs and use patterns. The figure below shows an example configuration for each option.



IBM uses remote control program product facilities to assist in problem determination, and to provide operational assistance as required. IBM also uses the SDLC or TCP/IP asynchronous connection facilities to transmit service data to

and from the IBM service support system, to gather error data, and to receive emergency fixes.

Remote Control Using a Support Element Console

If you need continuous monitoring of the remote system and you have LAN connectivity between the sites, the best choice for remote control is the use of a *remote Support Element Console*. Remote versus local operation of a system is a function of the communication path and supported protocols, ***not*** the physical distance between the system and its controlling Support Element Console.

A remote Support Element Console gives the most complete set of functions because it is a complete Support Element Console; only the connection configuration is different from a local Support Element Console. It also provides the same interface as is used locally so no additional operator training is required.

Security for a remote Support Element Console is provided by the Support Element Console user logon procedures, the secure transmissions between the Support Element Console and support elements, and domain security controls.

Remote Control Using the Web Server

If you need occasional monitoring and control of support elements connected to a S/390 Multiprise 3000 Enterprise Server, then the *Web browser* is a good choice.

Using a Web browser allows a system programmer or operator to monitor and/or control defined CPCs, CPC images, or groups from a remote site with a subset of task lists and tasks that are available on the Support Element Console. An example of use of the Web browser might be an off-hours monitor from home by an operator or system programmer.

Each current Support Element Console has a *Web Server* built in. The Web Server is a service of the Support Element Console Application that provides World Wide Web pages for use in performing Support Element Console tasks from a Web browser. Once the Web Server is enabled, multiple browsers can access the Support Element Console at one time.

The following tasks are available when logged on to the Web Server:

- **Daily**
  - Viewing Hardware Messages
  - Viewing Operating System Messages and entering Operating System commands
  - Activate
  - Reset Normal
  - Deactivate
  - Activity
- **CPC Recovery**
  - Viewing Hardware Messages
  - Viewing Operating System Messages and entering Operating System commands
  - Reset Normal

  - PSW Restart
  - Reset Clear
  - Load

- **CPC Operational Customization**
  - Viewing Hardware Messages
  - Viewing Operating System Messages and entering Operating System commands
  - Customize/Delete Activation Profiles
  - Customize Support Element Date/Time
  - Change LPAR Controls
  - Configure Channel Path On/Off
  - Open Systems Adapter 2 (OSA-2) Advanced Facilities
  - Reassign Channel Path

For information on performing these tasks, see the  **View the Support Element Console Overview** from the Web Server home page.

Performance associated with browser traffic is normally very good due to the relatively short and infrequent messages. Although status and messages are not immediately available at the browser, the browser automatically refreshes its view on a relatively frequent basis.

Reliability of the status information and the availability of the control functions are dependent on the reliability, availability, and throughput of the interconnecting network.

Web Server Requirements

Because any connection to a Support Element Console from the Web browser can potentially affect the operation and/or availability of the Support Element Console and the CPCs that it controls, it is important that security be given adequate consideration. It is recommended that your Support Element Console be installed only on your enterprise-controlled Intranet because the Web Server does not use an encrypted session.

The Support Element Console must be connected through a Token-Ring LAN or an Ethernet LAN and must be connected to the enterprise Intranet via the appropriate router or bridge.

Web Server support requires HTML 2.0, JavaScript 1.0, and Cookies. The following combinations have been tested:

- OS/2 Warp and Netscape Navigator Version 2.02-980101
- Windows 95 and Netscape Navigator Version 3.01
- Windows 95 and Netscape Communicator Version 4.05
- Windows 95 and Microsoft Internet Explorer Version 4.0
- Windows 98 and Netscape Navigator Version 3.01
- Windows 98 and Netscape Communicator Version 4.05
- Windows 98 and Microsoft Internet Explorer Version 4.0
- Windows NT and Netscape Navigator Version 3.01
- Windows NT and Netscape Communicator Version 4.05
- Windows NT and Microsoft Internet Explorer Version 4.0

Getting Ready to Use the Web Server

Before you can use the Web Server, you must:

- Enable the Support Element Console to allow for a Web browser connection
- Know the TCP/IP address of the Support Element Console you want to connect to
- Have a valid userid and password assigned by your Access Administrator for the Support Element Console web access. (For a procedure on how to authorize a userid to the Web Server, see page 14-2.)

Configuring for the Web Server on the Support Element Console

1. Log on to the local Support Element Console in *Access Administrator* mode.
2. Open **Console Actions**.
3. Open **Enable Console Services**.

   This displays the Enable Support Element Console Services window.
4. Select the **Enabled** radio button in the Web Server box.
5. Select the **OK** push button.
6. Log off the Support Element Console.

Note: To put this change into effect, shut down and then reboot the Support Element Console.

Logging On to the Web Server from a Web Browser

From your Web browser:

1. Enter the URL (TCP/IP address) of the Support Element Console you want to connect to.

   When the Support Element Console home page displays, two selections are available:

   Perform Support Element Console Application tasks

   This selection lets you log on to the Support Element Console Web Server for monitoring CPCs and CPC images.

   View the Support Element Console Overview

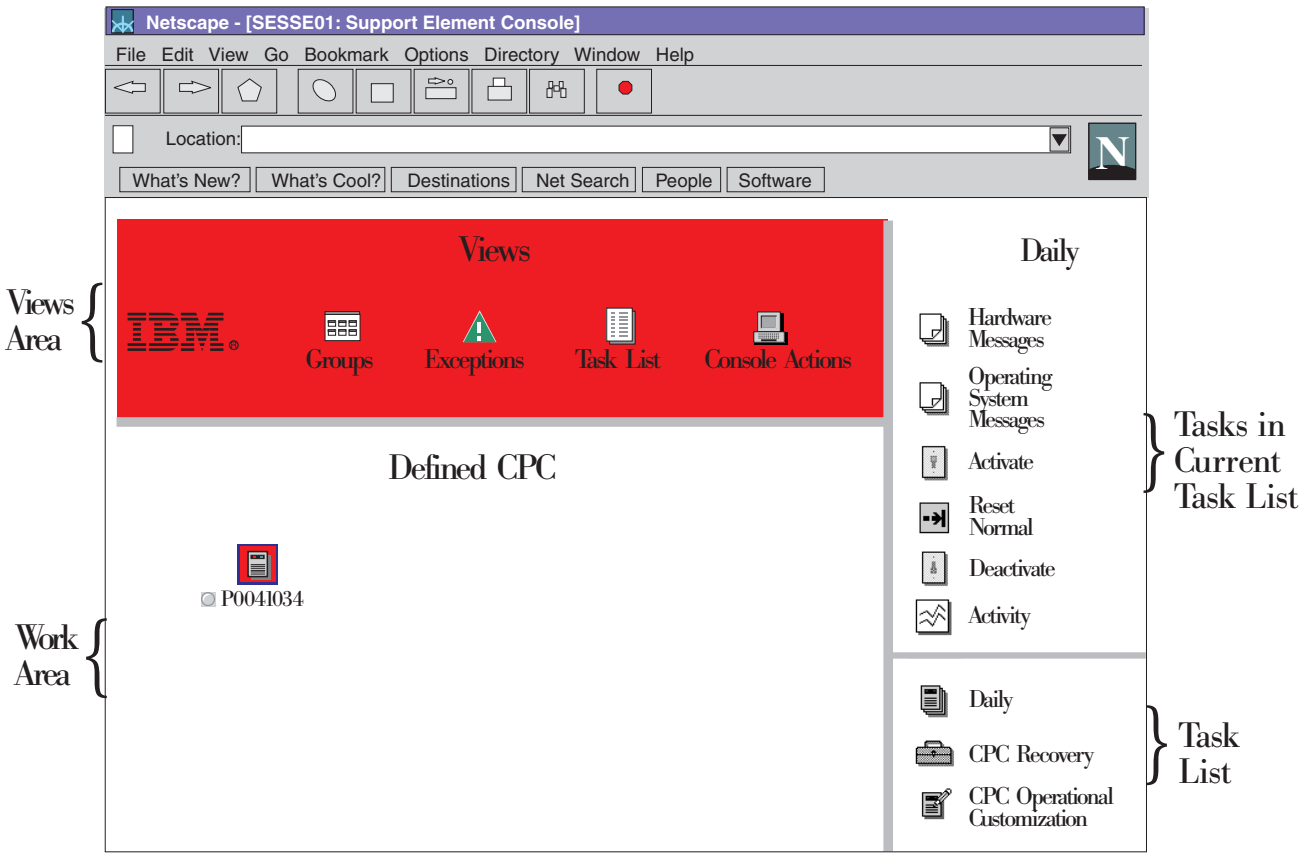
   This selection provides information on how to use the Web Server while working from your Web browser.

2. Select  **Perform Support Element Console Application tasks**.
3. When prompted, enter your *user name* or *userid* (for example, SYSPROG) and the valid *password* assigned by your Access Administrator. (For a procedure on how to authorize a userid to the Web Server, see page 14-2.)

   Note: You can only log on in operator, advanced operator, or system programmer mode.
4. Select the **OK** push button. You should now see the **Groups** view of the Support Element Console workplace.

The Support Element Console Web Pages

The layout of the Support Element Console Web pages, as shown through a Web browser in the example below, is similar to the Support Element Console workplace.



- The *Views Area* displays the views you can select.
- The *Work Area* displays the objects in the current view or group.
- The *Task Area* displays the tasks in the current task list and the task list icons (Daily, CPC Recovery, and CPC Operational Customization) that are available.

The views, objects, and tasks are your means of personalizing your Web Server session, locating objects, monitoring status, and performing tasks.

Object status may change at any refresh. Status indicators are updated automatically whenever the Support Element Console Web pages are reloaded. These pages are reloaded at the refresh rate set for your Web Server session through the **Personalize** Console Action or you may select the **Reload** button of your browser at any time. (The default refresh rate is 2 minutes.) To locate **Personalize**, click on **Console Actions** in the *Views* area.

Unlike the Support Element Console workplace, you must only single click Groups, Defined CPCs, or CPC Images to work with them. The *drag and drop* technique is ***not*** available through the Web Server.

To initiate an action on a CPC or CPC image, select the radio button below the CPC or CPC image icon and then click on the task you want to perform. If you just want to open the **Details** page of the CPC or CPC image, click on the icon itself.

Note: You can initiate a task on only one object at a time using the Web browser interface.

The *Views area* can be green (acceptable status) or red (unacceptable status). The background of the CPC can contain no color (acceptable status), red (unacceptable status), blue (hardware messages), or red/blue (unacceptable status and hardware messages). The background of the CPC image can contain no color (acceptable status), red (unacceptable status), cyan (operating system messages), or red/cyan (unacceptable status and operating system messages). To obtain more information about the reason for an unacceptable status, select the object to view the **Details** page.

Ending Your Web Server Session

It is recommended that you end your Web Server session after using it to prevent unauthorized users from accessing Support Element Console functions. You can end your Web Server session by:

- Closing the Web browser

  or

- Logging off the Web Server by clicking on **Console Actions** in the *Views* area and then clicking on  **Logoff**.

  or

- Automatic Logoff

  You can use your browser to open other Web sites after starting a Web Server session, but there is a time limit on how long you will remain logged on the Web Server while you are browsing other sites. You are automatically logged off the Web Server if you do not return to your Web Server session within the time limit. The time limit is the refresh rate set for your Web Server session, plus five minutes.

  You can remain logged on the Web Server indefinitely while you are browsing Support Element Console Web pages (and your network connection to the console remains uninterrupted). Any action that reloads the current page or loads a new page typically resets the time limit (such as, navigating the workplace or starting tasks).

  If you return after being logged off, your browser will display a message to notify you and give you the option of logging on again.

Things to Consider during Your Web Session

Any time you are logged on to the Support Element Console Web Server through a Web browser, the following conditions do exist:

- If an operator is logged on the Support Element Console locally, they will be aware of Web browser initiated activity through object and task busy indicators and pop-up windows.
- Each connection and active session to the Web Server may cause the response time to increase for any requested task.

- When monitoring system activity data using a Web Server session the following applies:
  - The minimum refresh rate for a Web Server session is 60 seconds, which is longer than the 15 second rate at which support elements send system activity data to the Support Element Console. Initially, a CPC's system activity page indicates system activity is not available for the CPC. This is normal. You must wait at least 15 seconds for the CPC's support element to make system activity data available to the Support Element Console, and then either wait for the Web Server session to reload the system activity page or reload it manually.
  - System activity data sent to the console for a CPC is replaced each time the CPC's support element sends new data.
  - A CPC's system activity data is not used if it is replaced by new data before the Web Server session can read it and reload the CPC's system activity page.

  For example, if the refresh rate is 60 seconds for your Web Server session, it will read data from the Support Element Console and reload system activity pages only once for every four times a CPC's support element sends system activity data to the console. As a result, some variations in a CPC's actual system activity may not be displayed on its system activity page.

Remote Control Using a Remote Control Program Product

If you need only occasional or short duration monitoring and control of the remote system, then a *program product* (such as DCAF) that can provide remote control of a local Support Element Console user interface may be an acceptable solution. An example of this use might be an emergency switched connection backup for a remote Support Element Console.

Even through the DCAF product has been withdrawn from marketing by IBM, the Support Element Console will continue to support its use. Each current Support Element Console has the “target” portion of DCAF built in. When enabled and properly configured, a Support Element Console can present the Support Element Console user interface to a DCAF controller connected through customer provided LAN (either Token Ring or Ethernet) using TCP/IP or SNA protocols or a switched connection using TCP/IP protocols. One way to connect using DCAF to a remote Support Element Console is via TCP/IP through a Serial Line Internet Protocol (SLIP). (Refer to the procedures on the following pages for all the necessary steps.)

All local Support Element Console functions are available through this type of interface.

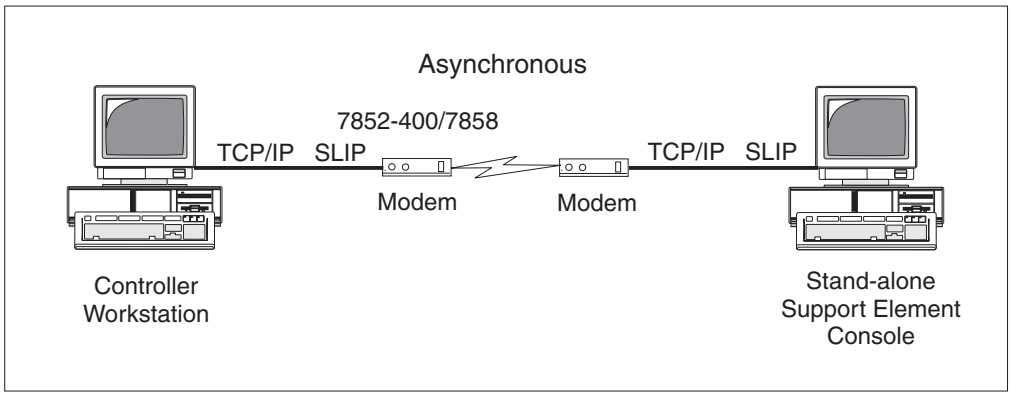
Performance of this class of remote operation is generally slower than other operations and in particular, switched connections should be considered for emergency use only as they are usually very slow.

Availability of the status information and the access to the control functions is dependent on the reliability, availability, and throughput of the interconnecting network.

Security is provided by the Support Element Console enablement functions, Support Element Console user logon controls, and customer network access controls.

Controller to a Support Element Console via Asynchronous TCP/IP through Serial Line Internet Protocol (SLIP)

This scenario describes the use of DCAF to provide a remote console for a Support Element Console using TCP/IP through SLIP.



Note: These procedures assume all the prerequisite software and hardware is installed correctly.

Configuring for a DCAF Connection on the Support Element Console

To use this facility, the Support Element Console must be configured to perform remote support facility functions using the asynchronous, TCP/IP connections.

1. Log on to the Support Element Console in *System Programmer* mode.
2. Open **Console Actions**.
3. Open **Enable Console Services**.

   This displays the Enable Support Element Console Services window.
4. Check **Enabled only if no user is logged on** (recommended setting) or **Enabled even while a user is logged on** in the Remote Operation box.
5. Check the **Enabled** radio button in the Automatic Call Answering box.
6. Select the **OK** push button.
7. Log off the Support Element Console.

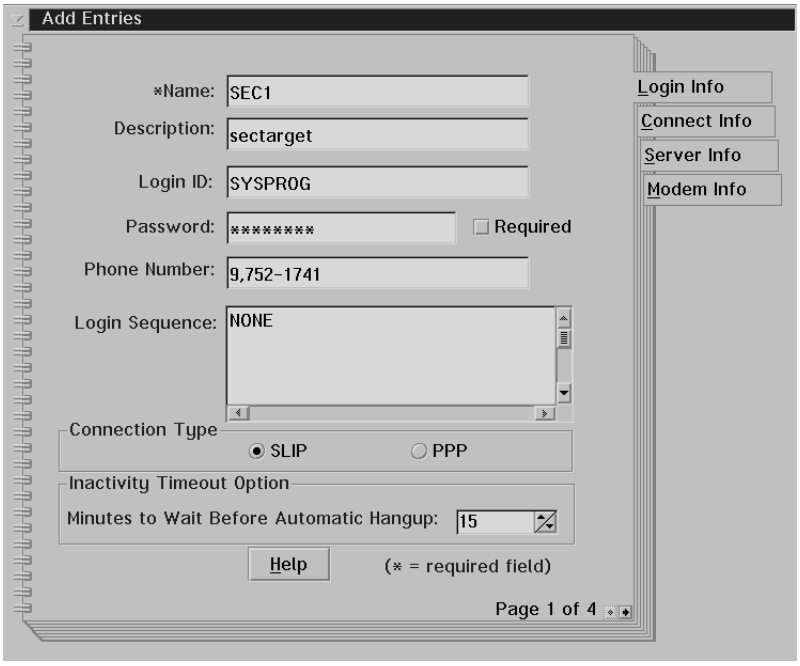
Configuring DCAF on the Controller Workstation

1. On the OS/2 Desktop, locate the **Distributed Console Access Facility** folder and open it. The Distributed Console Access Facility - Icon View is displayed.
2. Open the **DCAF Controller** icon. The Distributed Console Access Facility window is displayed.
3. Select **Session** from the menu bar and then select **Open Workstation directory...** The DCAF - Directory window is displayed.
4. Select **Workstation** from the menu bar and then **Add...**. The Add a Workstation window is displayed.
5. Type the *CP name for the Support Element Console* that will be the target for this connection in the Workstation Name box.

6. Select **TCP/IP** in the Protocol box.
7. Select the **Target** radio button in the Connection box.
8. Select the **Protocol** tab. The Add a Workstation notebook window is displayed.
9. Type **126.1.1.1** in the Remote Host Name box.
10. Make sure **2501** is entered in the Port Number box.
11. Select the **Save** push button. The Distributed Console Access Facility pop-up window is displayed.
12. Select the **OK** push button. The Add a Workstation window is redisplayed.
13. Select the **Cancel** push button. The DCAF - Directory window is displayed.
14. Close the DCAF - Directory window.
15. Close the Distributed Console Access Facility window.
16. Close the Distributed Console Access Facility - Icon View window.

Starting SLIP on the Controller Workstation

1. From an OS/2 window, type **START SLIPPM**. The IBM Dial-Up for TCP/IP window is displayed.
2. Select the **Add Entry** icon. The Add Entries notebook window is displayed.

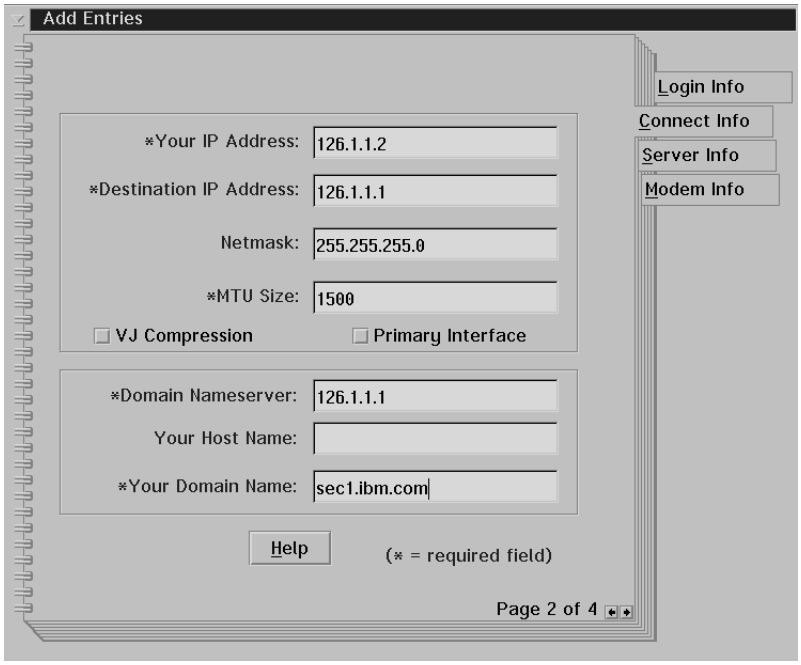


3. Type a *descriptive name* for the Support Element Console that will be the target for this connection in the Name box.
4. Type a *description of the Support Element Console* (up to eleven characters) in the Description box.
5. Type *anything* (for example, SYSPROG) in the Login ID box. (This is not used by the Support Element Console.)

6. Type *anything* in the Password box. (This is not used by the Support Element Console.)

   Note: Make sure the **Required** check box is not checked.

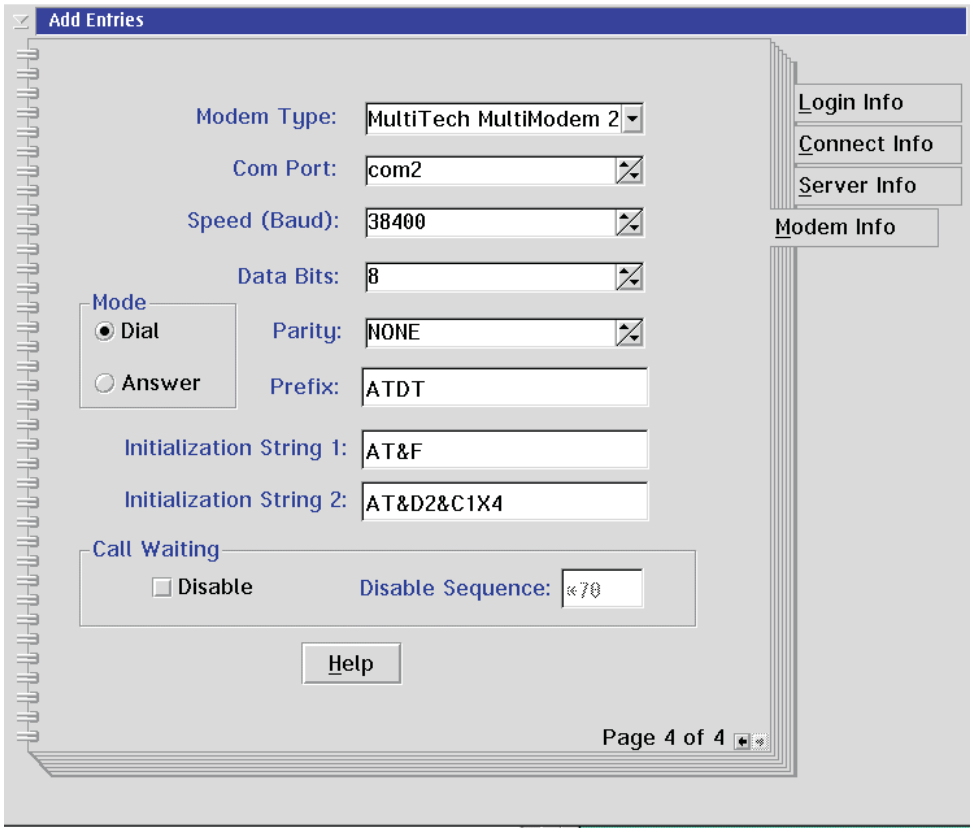
7. Type the *phone number* used to call the Support Element Console in the Phone Number box.
8. Type **NONE** in the Login Sequence box.
9. Select the **SLIP** radio button in the Connection Type box.
10. Select the *appropriate number of minutes* you want to wait before an automatic hang-up in the Inactivity Timeout Option box.
11. Select the **Connect Info** tab.



12. Type **126.1.1.2** in the Your IP Address box. (Use must use 126.1.1.2.)
13. Type **126.1.1.1** in the Destination IP Address box. (Use must use 126.1.1.1.)
14. Type **255.255.255.0** in the Netmask box.
15. Type **1500** in the MTU Size box.

    Note: Make sure the **VJ Compression** and **Primary Interface** check boxes are not checked.

16. Type **126.1.1.1** in the Domain Nameserver box.
17. Type your *Local domain name* (for example hmc.ibm.com) in the Your Domain Name box.
18. Select the **Modem Info** tab.



19. Select the *type of modem* (for example, **Multitech Multimodem 224E7 V.42bis**) you are using from the Modem Type pull-down list. This type of modem is a IBM 7852 Model 400 or 7858 and is shipped with your Support Element Console.
20. Select **com2** from the Com Port spin button list.
21. Select **38400** from the Speed (Baud) spin button list.
22. Select the **Dial** radio button from the Mode box.
23. Select **8** from the Data Bits spin button list.
24. Select **NONE** from the Parity spin button list.
25. Type **ATDT** in the Prefix box.
26. Type **AT&F** in the Initialization String 1 box. (This setting is required when using a 7852 or 7858 modem.)
27. Type **AT&D2&C1X4** in the Initialization String 2 box. (This setting is required when using a 7852 or 7858 modem.)
28. Close the Add Entry notebook window. The Closing Dial Configuration pop-up window is displayed.
29. Select the **Save** push button.
30. The IBM Dial-Up for TCP/IP window redisplays.
31. Select the **Dial** icon. If the IBM Dial-Up for TCP/IP pop-up window is displayed, select the **OK** push button.

32. Various status messages will appear in the Status box. When SLIP is running, the following message is displayed:

    ```
    [MON] SLIP Driver Running. Exit with Ctrl-C or Ctrl-Break
    ```

    You are now ready to start a DCAF session.

Starting DCAF on the Controller Workstation

1. On the OS/2 Desktop, locate the **Distributed Console Access Facility** folder and open it. The Distributed Console Access Facility - Icon View is displayed.
2. Open the **DCAF Controller** icon. The Distributed Console Access Facility window is displayed.
3. Select **Session** from the menu bar and then select **Open Workstation directory...** The DCAF - Directory window is displayed.
4. Locate the target workstation you want to work with and then open it. The DCAF - Target Password window is displayed.
5. Type in the password of the target Support Element Console.

   Note: The Support Element Console is shipped with a default password of **PASSWORD**. For security purposes, you should change the password to something other than **PASSWORD**.
6. Select the **OK** push button.
7. After a short delay, a new window should open containing the information currently displayed on the target Support Element Console. Maximize the window to work with the target Support Element Console.

   Note: How fast information is displayed on your controller workstation from the target Support Element Console depends on your modem speed. To reduce extraneous transmission of information across the phone line, at the OS/2 Desktop WarpCenter of the target Support Element Console, click on the  **System Activity Monitor** until the  **Disk Space Monitor** is displayed. In the left-hand corner, click on the **Time** setting until the **Date** setting is displayed.
8. When your DCAF session is finished, select **Session** from the menu bar and then select **Terminate**. The target Support Element Console is no longer available.
9. Close the Distributed Console Activity Facility window.
10. Close the Distributed Console Access Facility - Icon View window.
11. Select the **Hang-Up** icon on the IBM Dial-Up for TCP/IP window. The IBM Dial-Up for TCP/IP pop-up window is displayed.
12. Select the **OK** push button. The following message is displayed in the Status box:

    ```
    Exiting
    Deleting route Sl0: 126.1.1.2 -> 126.1.1.1
    ```
13. Close the IBM Dial-Up for TCP/IP window. The IBM Dial-Up for TCP/IP pop-up window is displayed.
14. Select the **OK** push button to exit.

Appendix B. Warranties

Statement of Limited Warranty

The warranties provided by IBM in this Statement of Limited Warranty apply only to Machines you originally purchase for your use, and not for resale, from IBM or an IBM authorized reseller. The term "Machine" means an IBM machine, its features, conversions, upgrades, elements, or accessories, or any combination of them. Machines are subject to these terms only if purchased in the United States or Puerto Rico, or Canada, and located in the country of purchase. If you have any questions, contact IBM or your reseller.

Machine: S/390 Multiprise 3000 Enterprise Server

Warranty Period*: One Year

**Elements and accessories are warranted for three months. Contact your place of purchase for warranty service information.*

Production Status

Each Machine is manufactured from new parts, or new and serviceable used parts (which perform like new parts). In some cases, the Machine may not be new and may have been previously installed. Regardless of the Machine's production status, IBM's warranty terms apply.

The IBM Warranty

IBM warrants that each Machine 1) is free from defects in materials and workmanship and 2) conforms to IBM's Official Published Specifications. IBM calculates the expiration of the warranty period from the Machine's Date of Installation. The date on your receipt is the Date of Installation, unless IBM or your reseller informs you otherwise.

During the warranty period, IBM or your reseller will provide warranty service under the type of service designated for the Machine and will manage and install engineering changes that apply to the Machine. IBM or your reseller will specify the type of service.

For a feature, conversion, or upgrade, IBM or your reseller may require that the Machine on which it is installed be 1) the designated, serial-numbered Machine and 2) at an engineering-change level compatible with the feature, conversion, or upgrade. Some of these transactions (called "Net-Priced" transactions) may include additional parts and associated replacement parts that are provided on an exchange basis. All removed parts become the property of IBM and must be returned to IBM.

Replacement parts assume the remaining warranty of the parts they replace.

If a Machine does not function as warranted during the warranty period, IBM or your reseller will repair or replace it (with a Machine that is at least functionally equivalent) without charge. If IBM or your reseller is unable to do so, you may return it to your place of purchase and your money will be refunded.

If you transfer a Machine to another user, warranty service is available to that user for the remainder of the warranty period. You should give your proof of purchase and this Statement to that user.

Warranty Service

To obtain warranty service for the Machine, you should contact your reseller or call IBM. In the United States, call IBM at **1-800-IBM-SERV (426-7378)**. In Canada, call IBM at **1-800-465-6666**. You may be required to present proof of purchase.

Depending on the Machine, the service may be 1) a “Repair” service at your location (called “On-site”) or at one of IBM's or a reseller's service locations (called “Carry-in”) or 2) an “Exchange” service, either On-site or Carry-in.

When a type of service involves the exchange of a Machine or part, the item IBM or your reseller replaces becomes its property and the replacement becomes yours. The replacement may not be new, but will be in good working order and at least functionally equivalent to the item replaced.

It is your responsibility to:

1. obtain authorization from the owner (for example, your lessor) to have IBM or your reseller service a Machine that you do not own;
2. where applicable, before service is provided —
   a. follow the problem determination, problem analysis, and service request procedures that IBM or your reseller provide,
   b. secure all programs, data, and funds contained in a Machine,
   c. inform IBM or your reseller of changes in a Machine's location, and
   d. for a Machine with exchange service, remove all features, parts, options, alterations, and attachments not under warranty service. Also, the Machine must be free of any legal obligations or restrictions that prevent its exchange; and
3. be responsible for loss of, or damage to, a Machine in transit when you are responsible for the transportation charges.

Extent of Warranty

IBM does not warrant uninterrupted or error-free operation of a Machine.

Misuse, accident, modification, unsuitable physical or operating environment, improper maintenance by you, or failure caused by a product for which IBM is not responsible may void the warranties.

THESE WARRANTIES REPLACE ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. HOWEVER, SOME LAWS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES. IF THESE LAWS APPLY, THEN ALL EXPRESS AND IMPLIED WARRANTIES ARE LIMITED IN DURATION TO THE WARRANTY PERIOD. NO WARRANTIES APPLY AFTER THAT PERIOD.

In Canada, warranties include both warranties and conditions.

Some jurisdictions do not allow limitations on how long an implied warranty lasts, so the above limitation may not apply to you.

Limitation of Liability

Circumstances may arise where, because of a default on IBM's part (including fundamental breach) or other liability (including negligence and misrepresentation), you are entitled to recover damages from IBM. In each such instance, regardless of the basis on which you are entitled to claim damages, IBM is liable only for:

1. bodily injury (including death), and damage to real property and tangible personal property; and
2. the amount of any other actual loss or damage, up to the greater of $100,000 or the charge for the Machine that is the subject of the claim.

Under no circumstances is IBM liable for any of the following:

1. third-party claims against you for losses or damages (other than those under the first item listed above);
2. loss of, or damage to, your records or data; or
3. economic consequential damages (including lost profits or savings) or incidental damages, even if IBM is informed of their possibility.

Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

This warranty gives you specific legal rights and you may also have other rights which vary from jurisdiction to jurisdiction.

IBM Agreement for Licensed Internal Code

You accept the terms of this Agreement by your initial use of a machine that contains IBM Licensed Internal Code (called “Code”).

These terms apply to Code used by certain machines IBM or your reseller specifies (called “Specific Machines”). International Business Machines Corporation or one of its subsidiaries (“IBM”) owns copyrights in Code. IBM owns all copies of Code, including all copies made from them.

If you are the rightful possessor of a Specific Machine, IBM grants you a license to use the Code (or any replacement IBM provides) on, or in conjunction with, only the Specific Machine for which the Code is provided. IBM licenses the Code to only one rightful possessor at a time.

Under each license, IBM authorizes you to do only the following:

1. execute the Code to enable the Specific Machine to function according to its Official Published Specifications (called “Specifications”);
2. make a backup or archival copy of the Code (unless IBM makes one available for your use), provided you reproduce the copyright notice and any other legend of ownership on the copy. You may use the copy only to replace the original, when necessary; and
3. execute and display the Code as necessary to maintain the Specific Machine.

You agree to acquire any replacement for, or additional copy of, Code directly from IBM in accordance with IBM's standard policies and practices. You also agree to use that Code under these terms.

You may transfer possession of the Code to another party only with the transfer of the Specific Machine. If you do so, you must 1) destroy all your copies of the Code that were not provided by IBM, 2) either give the other party all your IBM-provided copies of the Code or destroy them, and 3) notify the other party of these terms. IBM licenses the other party when it accepts these terms. These terms apply to all Code you acquire from any source.

Your license terminates when you no longer rightfully possess the Specific Machine.

Actions You May Not Take

You agree to use the Code only as authorized above. You may not do, for example, any of the following:

1. otherwise copy, display, transfer, adapt, modify, or distribute the Code (electronically or otherwise), except as IBM may authorize in the Specific Machine's Specifications or in writing to you;
2. reverse assemble, reverse compile, or otherwise translate the Code unless expressly permitted by applicable law without the possibility of contractual waiver;
3. sublicense or assign the license for the Code; or

Z125-4144-03 11/95

4. lease the Code or any copy of it.

Appendix C. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States or other countries or both:

ESA/390
ESCON
IBM
MVS/ESA
Multiprise
Netfinity
OS/2
OS/390
Parallel Sysplex
Processor Resource/Systems Manager
PR/SM
RACF
RETAIN
Sysplex Timer
System/390
S/370
S/390

Microsoft, Windows, Windows NT, and the windows logo are trademarks of the Microsoft Corporation in the United States, other countries, or both.

Other company, product, and service names, may be trademarks or service marks of others.

Electronic Emission Notices

The following statement applies to this IBM product. The statement for other IBM products intended for use with this product will appear in their accompanying manuals.

Federal Communications Commission (FCC) Statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions contained in the installation manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors, by installation or use of this equipment other than as specified in the installation manual, or by any other unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Canadian Department of Communications Compliance Statement

This equipment does not exceed Class A limits per radio noise emissions for digital apparatus, set out in the Radio Interference Regulation of the Canadian Department of Communications. Operation in a residential area may cause unacceptable interference to radio and TV reception requiring the owner or operator to take whatever steps are necessary to correct the interference.

Avis de conformité aux normes du ministère des Communications du Canada

Cet équipement ne dépasse pas les limites de Classe A d'émission de bruits radioélectriques pour les appareils numériques, telles que prescrites par le Règlement sur le brouillage radioélectriques établi par le ministère des Communications du Canada. L'exploitation faite en millieu résidentiel peut entrainer le brouillage de réceptions radio et télé, ce qui obligerait le propriétaire ou l'opérateur à prendre les dispositions nécessaires pour en éliminer les causes.

Taiwan Class A Compliance Statement

警告使用者:
這是甲類ㄉ 資訊產品，在
居住的環境中使用時，可
能會造成射頻干擾，在這
種情況下，使用者會被要
求採取某些適當的對策。

Index

A

B

C

D

E

G

H

I

L

N

O

P

R

S

T

U

V

W

Readers' Comments — We'd Like to Hear from You

S/390®
Support Element Operations Guide
Version 1.6.1

Publication No. GC38-0607-01

Is there anything you especially like or dislike about this book? Feel free to comment on specific errors or omissions, accuracy, organization, or completeness of this book.

IBM may use or distribute whatever information you supply in any way it believes appropriate without incurring any obligation to you, and all such information will be considered nonconfidential.

No postage stamp necessary if mailed in the U.S.A. (Elsewhere, an IBM office or representative will be happy to forward your comments or you may mail directly to the address in the Edition Notice on the back of the front cover or title page.)

Note

Do not use this form to report system problems or to request copies of publications. Instead, contact your IBM representative or the IBM branch office serving you.

Would you like a reply? ___YES ___ NO

Name

Address

Company or Organization

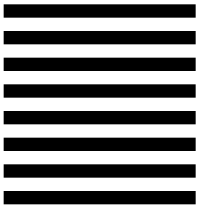
Phone No.

Readers' Comments — We'd Like to Hear from You
GC38-0607-01

Cut or Fold
Along Line

Fold and Tape | **Please do not staple** | Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES



BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

International Business Machines Corporation
Information Development
Department G60
1701 North Street
ENDICOTT NY 13760-5553

Fold and Tape | **Please do not staple** | Fold and Tape

GC38-0607-01

Cut or Fold
Along Line

Level 01a, February 28, 2001

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

GC38-0607-01