System z9

Support Element Operations Guide

Version 2.9.1

SC28-6858-01

System z9

Support Element Operations Guide

Version 2.9.1

SC28-6858-01

Note

Before using this information and the product it supports, be sure to read the information under "Safety notices" on page ix and "Notices" on page B-1.

Second Edition (November 2006)

This edition, SC28-6858-01, applies to the IBM® System z9™ Support Element Console Application, Version 2.9.1.

This edition replaces SC28-6858-00. A technical change to the text or illustration is indicated by a vertical line to the left of the change.

There may be a newer version of this document in **PDF** format available on **Resource Link**™. Go to *http://www.ibm.com/servers/resourcelink* and click on **Library** on the navigation bar. A newer version is indicated by a lower case alphabetic letter following the form number suffix. For example: 00a, 00b, 01a, 01b.

Contents

Safety and Environmental Notices

Safety notices

Safety notices may be printed throughout this guide. **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.

World Trade Safety Information

Several countries require the safety information contained in product publications to be presented in their national languages. If this requirement applies to your country, a safety information booklet is included in the publications package shipped with the product. The booklet contains the safety information in your national language with references to the US English source. Before using a US English publication to install, operate, or service this IBM product, you must first become familiar with the related safety information in the booklet. You should also refer to the booklet any time you do not clearly understand any safety information in the US English publications.

Laser Safety Information

All System z models can use I/O cards such as PCI adapters, ESCON, FICON, Open Systems Adapter (OSA), InterSystem Coupling-3 (ISC-3), or other I/O features which are fiber optic based and utilize lasers or LEDs.

Laser Compliance

All lasers are certified in the U.S. to conform to the requirements of DHHS 21 CFR Subchapter J for class 1 laser products. Outside the U.S., they are certified to be in compliance with IEC 60825 as a class 1 laser product. Consult the label on each part for laser certification numbers and approval information.

CAUTION:
Data processing environments can contain equipment transmitting on system links with laser modules that operate at greater than Class 1 power levels. For this reason, never look into the end of an optical fiber cable or open receptacle. (C027)

CAUTION:
This product contains a Class 1M laser. Do not view directly with optical instruments. (C028)

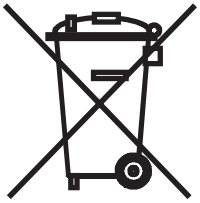
Environmental Notices

Product Recycling and Disposal

This unit must be recycled or discarded according to applicable local and national regulations. IBM encourages owners of information technology (IT) equipment to responsibly recycle their equipment when it is no longer needed. IBM offers a variety of product return programs and services in several countries to assist

equipment owners in recycling their IT products. Information on IBM product recycling offerings can be found on IBM's Internet site at *http://www.ibm.com/ibm/environment/products/prp.shtml*.

Esta unidad debe reciclarse o desecharse de acuerdo con lo establecido en la normativa nacional o local aplicable. IBM a los propietarios de equipos de tecnología de la información (TI) que reciclen responsablemente sus equipos cuando éstrecomiendaos ya no les sean útiles. IBM dispone de una serie de programas y servicios de devolución de productos en varios países, a fin de ayudar a los propietarios de equipos a reciclar sus productos de TI. Se puede encontrar información sobre las ofertas de reciclado de productos de IBM en el sitio web de IBM *http://www.ibm.com/ibm/environment/products/prp.shtml*.



Notice: This mark applies only to countries within the European Union (EU) and Norway.

Appliances are labeled in accordance with European Directive 2002/96/EC concerning waste electrical and electronic equipment (WEEE). The Directive determines the framework for the return and recycling of used appliances as applicable throughout the European Union. This label is applied to various products to indicate that the product is not to be thrown away, but rather reclaimed upon end of life per this Directive.

In accordance with the European WEEE Directive, electrical and electronic equipment (EEE) is to be collected separately and to be reused, recycled, or recovered at end of life. Users of EEE with the WEEE marking per Annex IV of the WEEE Directive, as shown above, must not dispose of end of life EEE as unsorted municipal waste, but use the collection framework available to customers for the return, recycling, and recovery of WEEE. Customer participation is important to minimize any potential effects of EEE on the environment and human health due to the potential presence of hazardous substances in EEE. For proper collection and treatment, contact your local IBM representative.

注意: このマークは EU 諸国およびノルウェーにおいてのみ適用されます。

この機器には、EU 諸国に対する廃電気電子機器指令 2002/96/EC(WEEE) のラベルが貼られています。この指令は、EU 諸国に適用する使用済み機器の回収とリサイクルの骨子を定めています。このラベルは、使用済みになった時に指令に従って適正な処理をする必要があることを知らせるために種々の製品に貼られています。

Remarque : Cette marque s'applique uniquement aux pays de l'Union Européenne et à la Norvège.

L'étiquette du système respecte la Directive européenne 2002/96/EC en matière de Déchets des Equipements Electriques et Electroniques (DEEE), qui détermine les dispositions de retour et de recyclage applicables aux systèmes utilisés à travers l'Union européenne. Conformément à la directive, ladite étiquette précise que le produit sur lequel elle est apposée ne doit pas être jeté mais être récupéré en fin de vie.

Refrigeration

This system contains one or more modular refrigeration units with R-507 refrigerant and a polyol ester oil. This refrigerant must not be released or vented to the atmosphere. Skin contact with refrigerant may cause frostbite. Wear appropriate eye and skin protection. Modular refrigeration units are hermetically sealed and must not be opened or maintained.

This notice is provided in accordance with the European Union (EU) Regulation 842/2006 on fluorinated greenhouse gases. This product contains fluorinated greenhouse gases covered by the Kyoto Protocol. Per Annex I, Part 2, of the EU Regulation 842/2006, the global warming potential of R-507 is calculated to be 3850. Each unit contains 33 ounces of R-507.

Battery Return Program

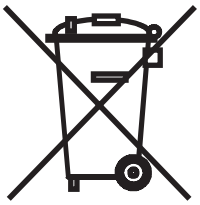
This product may contain sealed lead acid, nickel cadmium, nickel metal hydride, lithium, or lithium ion battery(s). Consult your user manual or service manual for specific battery information. The battery must be recycled or disposed of properly. Recycling facilities may not be available in your area. For information on disposal of batteries outside the United States, go to *http://www.ibm.com/ibm/environment/products/batteryrecycle.shtml* or contact your local waste disposal facility.

In the United States, IBM has established a return process for reuse, recycling, or proper disposal of used IBM sealed lead acid, nickel cadmium, nickel metal hydride, and other battery packs from IBM Equipment. For information on proper disposal of these batteries, contact IBM at 1-800-426-4333. Please have the IBM part number listed on the battery available prior to your call.

In Taiwan, the following applies:

Please recycle batteries 廢電池請回收

For the European Union:



For California:

Perchlorate Material - special handling may apply. See *http://www.dtsc.ca.gov/hazardouswaste/perchlorate*.

The foregoing notice is provided in accordance with California Code of Regulations Title 22, Division 4.5, Chapter 33. Best Management Practices for Perchlorate Materials. This product, part, or both may include a lithium manganese dioxide battery which contains a perchlorate substance.

IBM Cryptographic Coprocessor Card Return Program

The following information applies only for systems originally sold prior to July 1, 2006:

This machine may contain an optional feature, the cryptographic coprocessor card, which includes a polyurethane material that contains mercury. Please follow Local Ordinances or regulations for disposal of this card. IBM has established a return program for certain IBM Cryptographic Coprocessor Cards. More information can be found at *http://www.ibm.com/ibm/environment/products/prp.shtml*.

برنامج ارجاع كرت IBM Cryptographic Coprocessor

هــذه الماكيــنة قد تحتــوي على خاصــية اختيارية، وهى كــارت
Cryptographic Coprocessor
والتي تحتــوي على مـــادة بولــييوريثيـــن التي تحتــوي على الزئبــق
رجـــــاء اتبــاع القوانيــن أو التعليمــات المحــلية للتخــلص من هــذا الكـــارت .
قامــت شركة IBM باعداد برنامج لارجاع بعض كــروت IBM Cryptographic
Coprocessor

لمزيد من المعلومات، رجاء زيارة الموقع
http://www.ibm.com/ibm/environment/products/prp.shtml

Preface

This operations guide is for anyone who is responsible for monitoring and operating the IBM System z9 Enterprise Class (z9 EC) and IBM System z9 Business Class (z9 BC).

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

ACSADMIN	Access Administrator
ADVANCED	Advanced Ooperator
OPERATOR	Operator
SYSPROG	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 be familiar with using:
- Workstations
- Graphical user interfaces
- Printers
- Tapes and tape devices
- Diskettes and diskette devices
- DVD cartridges
- 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 a PDF format on **Resource Link** (http://www.ibm.com/servers/resourcelink). 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. Then double-click on the book icon to open the *Support Element Operations Guide*. After the guide has been opened, bookmarks display on the left side of the view.

The highest level topics are displayed in the order that they appear as chapters in the PDF format. If any of these topics have lower level topics, a "►" displays to the left of the higher level topic. To expand the topic, click once on the "►" and the next level will be displayed.

User Interface

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, controls, 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 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.

What's New in Version 2.9.1

This guide reflects the licensed internal code for Support Element Console Application, Version 2.9.1. 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.

- "Time Synchronization features" on page 9-11and "Synchronizing the CPC TOD clock to a time synchronization source" on page 5-45.

There may be other changes to the system code that are not described in this guide. Please refer to the other documents shipped with your processor for additional information.

How to Send your Comments

Your feedback is important in helping to provide the most accurate and high-quality information. Send your comments by using Resource Link at *http://www.ibm.com/servers/resourcelink*. Select **Feedback** on the Navigation bar on the left. 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).

Chapter 1. Introduction

A *support element* is a dedicated workstation used for monitoring and operating a system. It is attached to the central processor complex (CPC) of a system. If you have experience using other systems, you may have used a processor console, support processor, or a similarly named workstation to monitor and operate them.

The IBM System z9 EC and z9 BC is an *integrated support element*, that is, the support element is located inside the same frame that the central processor complex (CPC) is located. An alternate support element is also provided to give you the option to switch from your primary support element to your alternate support element if hardware problems occur. For more information on the alternate support element, see “Forcing an immediate mirroring of the primary support element to the alternate support element” on page 10-19.

The z9 EC and z9 BC operate only in logically partitioned mode.

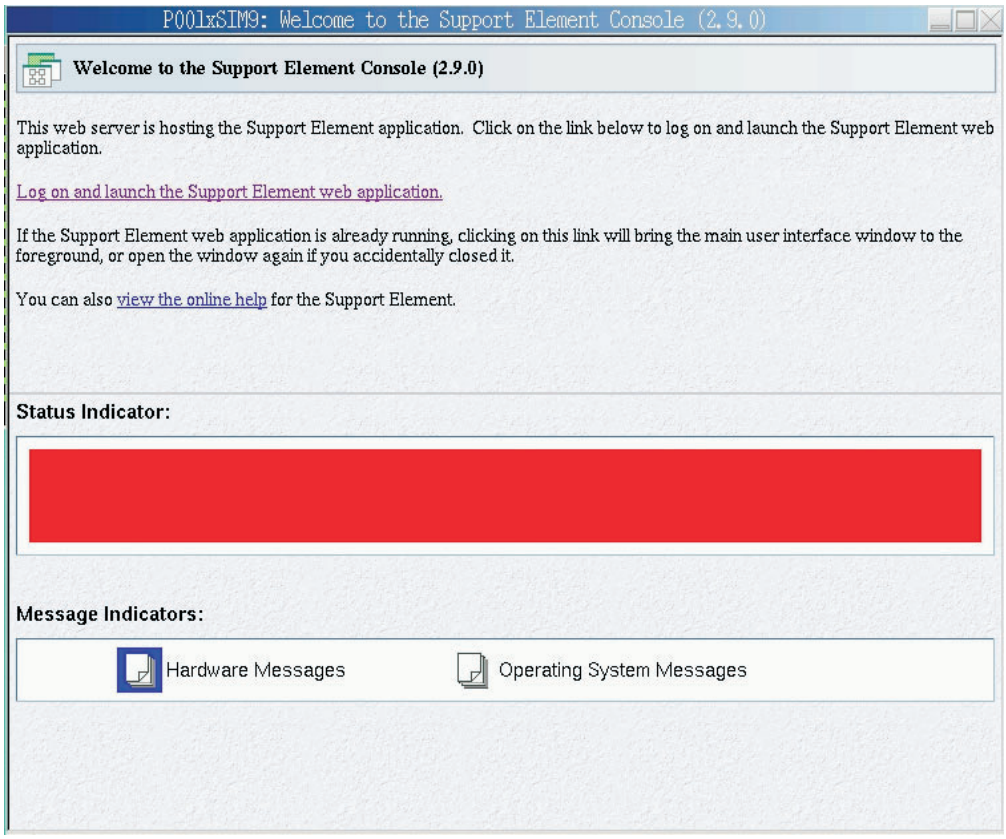
A *Hardware Management Console* is required for monitoring and operating systems with integrated support elements.

The support element console application

The Support Element Console Application version 2.9.1 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 bar of the Support Element Logon window and also the Support Element Workplace window.

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. A window displays the IBM Logo and copyright information. When the process completes, the logon window is displayed.



You are logged on the support element console automatically when you establish a session with the support element from a Hardware Management Console.

Establishing a support element console session from a Hardware Management Console

A Hardware Management Console must be used for monitoring and operating systems with integrated 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. Upon establishing a support element session, you can refer to this manual for information and instructions for using the support element to monitor and operate the system it is attached to.

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 CPC 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 CPC on **Single Object Operations** in the **CPC Recovery** tasks area.

The **Single Object Operations Task Confirmation** window displays. Follow the instructions on the Confirmation window to complete this task.

To log on, enter one of the default user IDs and password combinations, or the user ID and password combination assigned to you by your Access Administrator. Then click **Logon**.

Default user IDs and passwords are established as part of a base Support Element Console. The following default user roles, user IDs, and passwords are:

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

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 System z9.

The workplace is the window from where you start tasks for monitoring and operating the CPC. Your *user role* determines which tasks and controls you can use on the support element workplace. Not all tasks are available for each user role. Refer to the description of the specific task you want to access to see what user role(s) it is available in. To view your login user details and tasks

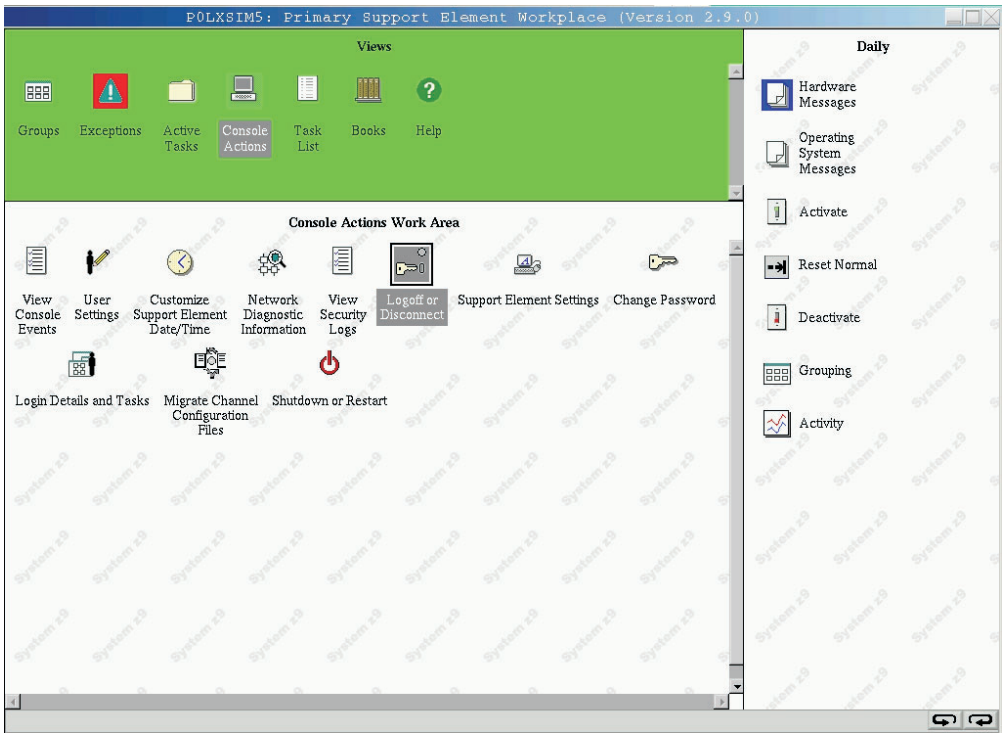
1. Open **Console Actions** from the **Views** area.
2. Open **Login Details and Tasks** in the **Console Actions Work Area**.

   The Login Details and Tasks window displays the current user mode.

Logging off the support element console

Once you have completed your tasks on the support element, log off the console. The **Logoff or Disconnect** task allows you to end the current user session and logs off the support element console or to disconnect while your tasks continue running. If you disconnect, you can reconnect at a later time to continue working. However, a disconnect session is eventually ended (This is because disconnect sessions exist only while the support element console application is running. If the support element console is restarted or the console is shut down or rebooted, all session information is lost).

Select the log off operation when you no longer need access to the support element console. Logging off the console does not affect the status of the CPC or Images. After you log off or disconnect, the **Welcome to the Primary Support Element Console** window is displayed. If you chose to disconnect rather than logoff, when you logon again, the **Choose a Disconnected Session** window is displayed. You can select the disconnected session to continue working or you can begin a new session. (The number of windows displayed depends on the state of the session when it was disconnected. One of the windows is the main user interface; additional windows are for each task that was running when the session was disconnected.)



To log off or disconnect from the Support Element Console:

1. Open **Console Actions** from the **Views** area.
2. Open **Log off or Disconnect** from the **Console Actions Work Area**. The **Choose to Logoff or Disconnect** window displays to let you log off or disconnect.

The support element workplace window closes and the Hardware Management Console workplace window is displayed.

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)
- Physical channels (PCHIDs)
- Central processors
  - This includes : General processors, Internal Coupling Facility (ICF), Integrated Facility for Linux (IFL), Integrated Facility for Applications (IFA), and IBM System z9 Integrated Information Processors (zIIPs).
- Logical channels (CSS.CHPIDs)
- 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. Each logical partition is an image.

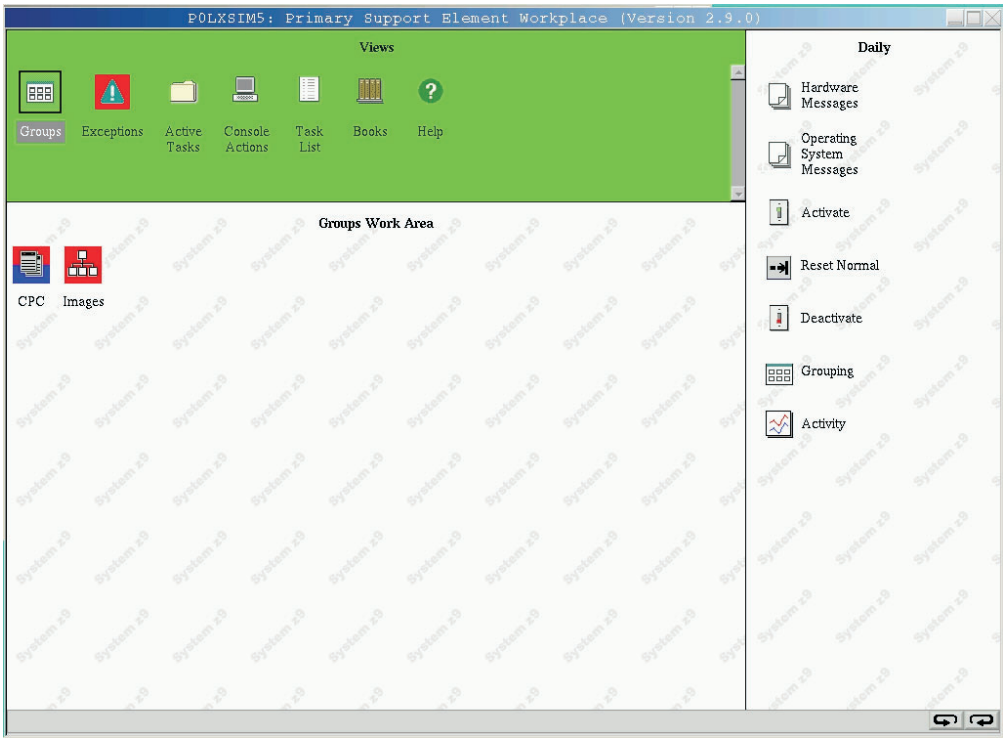
A single icon that represents a set of one or more objects of the same type is referred to as a *group*.

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:

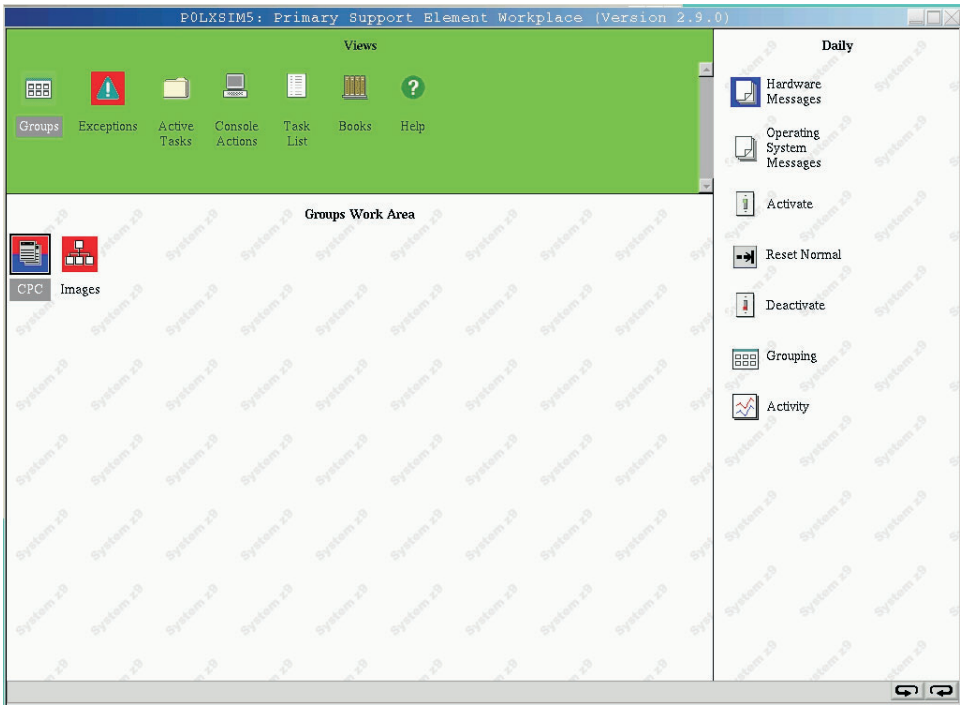
No exceptions
: This is the summarized system status when all objects have acceptable statuses. An *acceptable* status is any object status that is normal, is as expected, or does not require your immediate attention or intervention. That is, an object with an acceptable status is OK as is.

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.

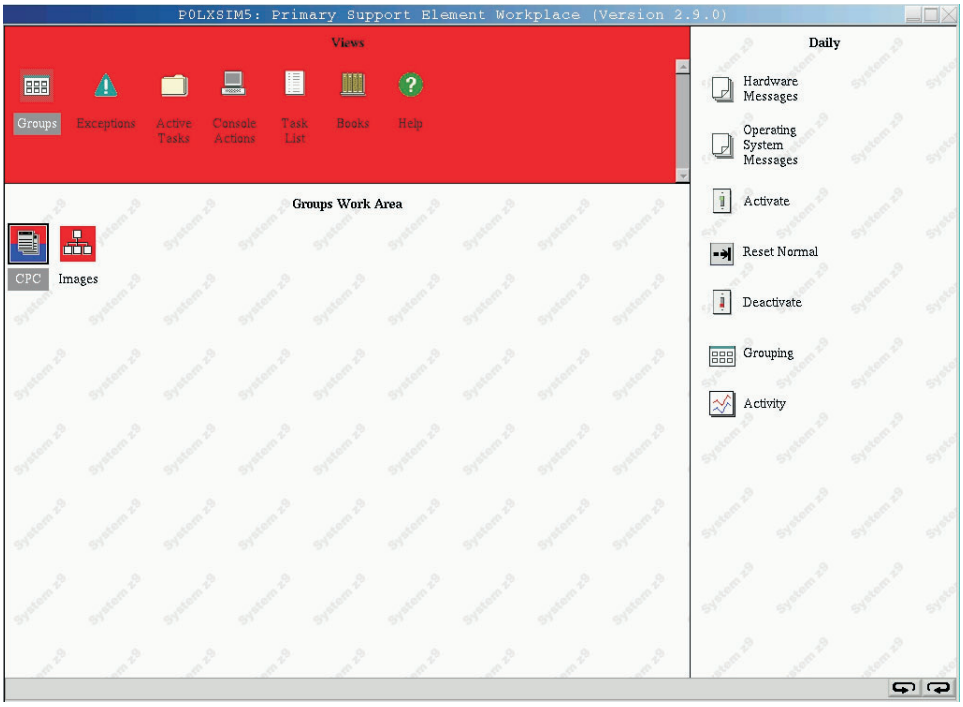
An *exception occurs* when the status of an object becomes unacceptable. The object is referred to as an *exception* while its status remains unacceptable.

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 2-13.

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

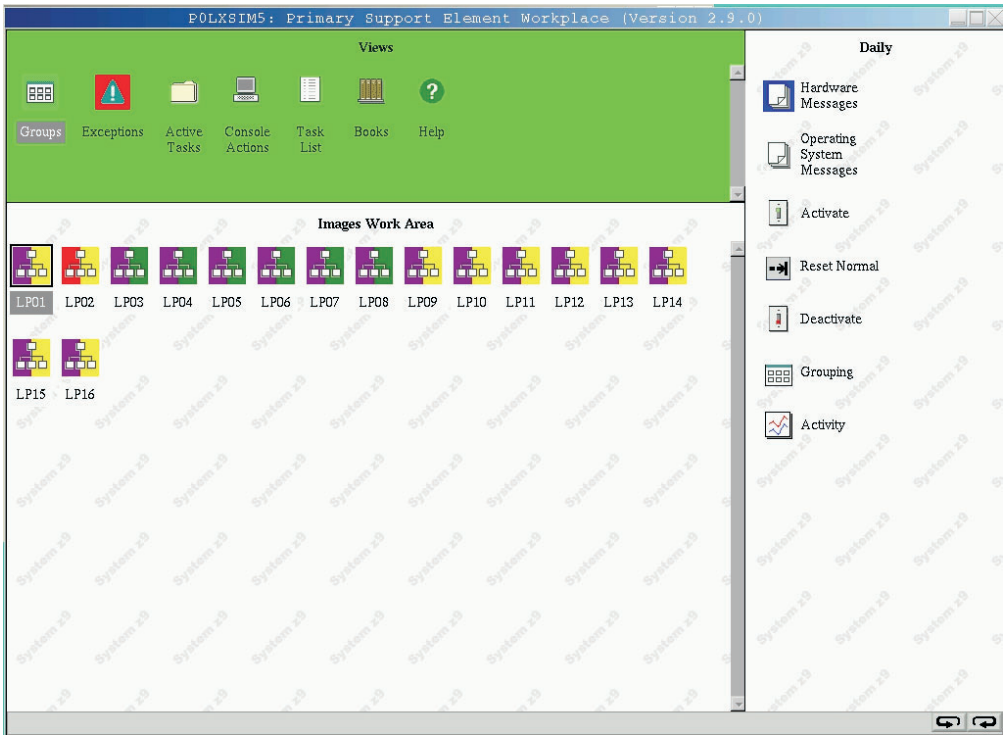
One of console's default groups, the **CPC** group, contains the object that represents the central processor complex (CPC).

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 logical partitions

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



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:

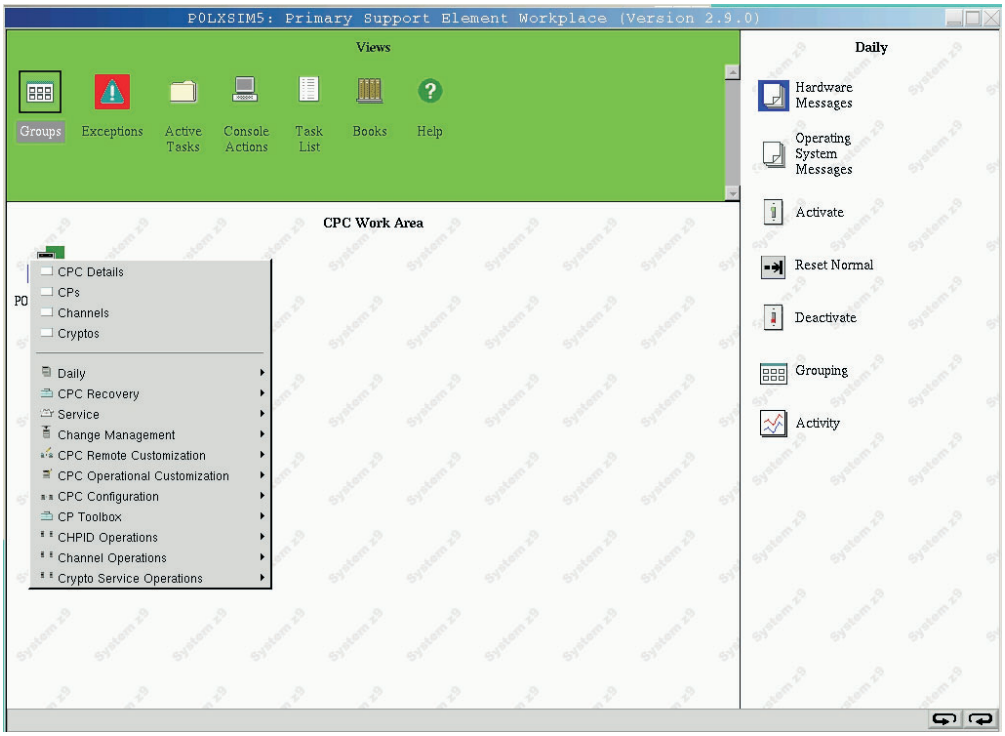
1. Open **Groups** from Views
2. Locate the group labelled **Images** in the Groups Work Area.

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 a logical processor:

- When the CPC is activated, 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 2-6.
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:

1. Open the Images Work Area.

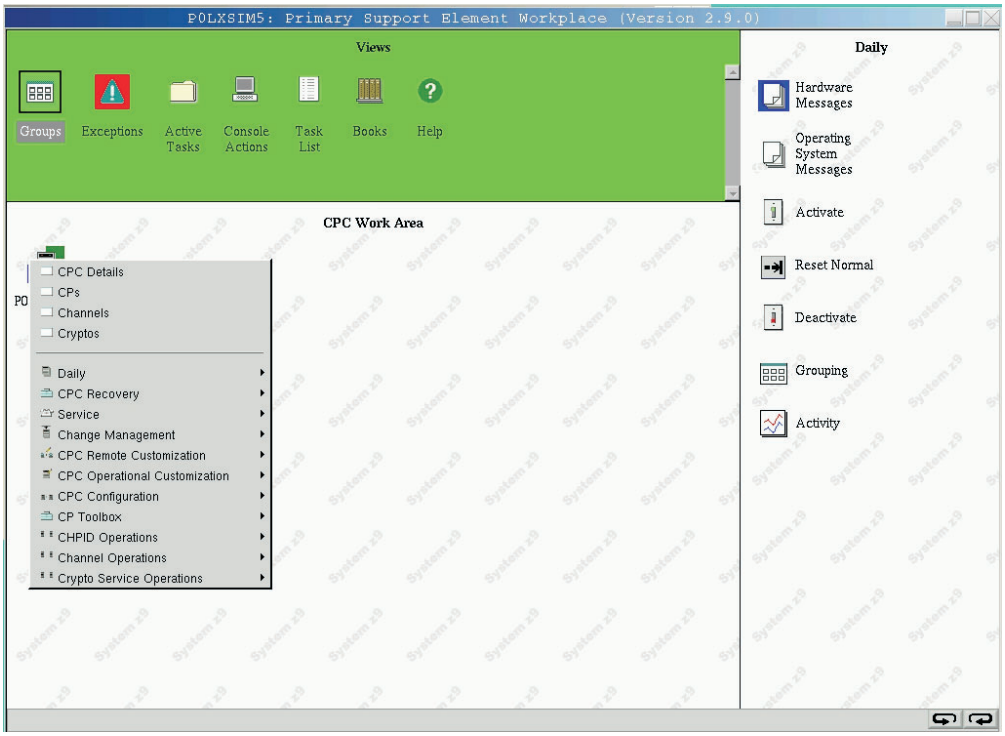
   For instructions, see"Locating logical partitions" on page 2-6.
2. In the Images Work Area, locate the image that represents the logical partition to which the logical processors are assigned.

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 channels

The object that represents the central processor complex (CPC) contains objects that represent all channels configured and not configured in the input/output (I/O) configuration.



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

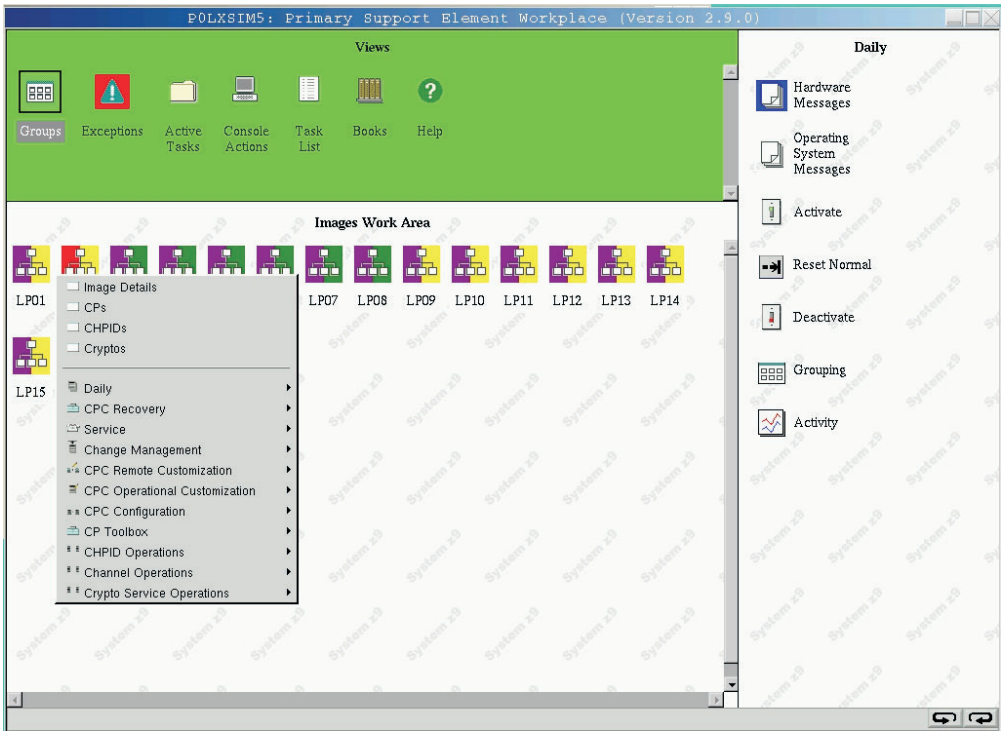
1. Open the CPC Work Area.

   For instructions, see "Locating the CPC" on page 2-6.
2. In the CPC Work Area, locate the CPC.
3. Right click on the CPC to open its pop-up menu.
4. Select the **Channels** menu choice.

   This displays the objects that represent the channels in the work area. Each channel is labelled with its physical channel identifier (PCHID).

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 channel paths assigned to a specific logical partition:

1. Open the Images Work Area.

   For instructions, see “Locating logical partitions” on page 2-6.
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 (CSS.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

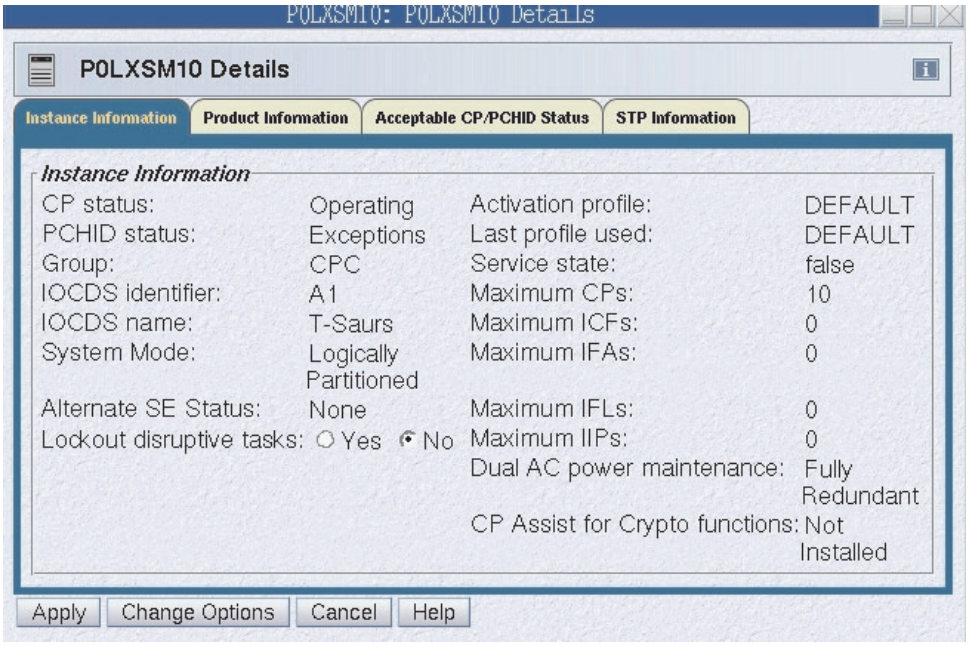
The background color of the icon of a central processor (CP) indicates whether the status of the CP is acceptable or unacceptable. While the status is acceptable, the background of a CP icon has no color. Otherwise, the background color of the CP is the color that indicates its specific unacceptable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

Background color of channel paths

The background color of the icon of a channel path indicates whether the status of 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** tabbed window.



To open an object's **Details** tabbed window:

1. Locate the object.

   For instructions, see the topics that follow "Locating groups and objects" on page 2-6.
2. In the object's work area, double-click on the object.

   This opens the object's **Details** window.

The Details window includes the following tabbed information:

Instance Information
: Includes instance information and task information.

Acceptance Status
: Shows the various states and their associated colors and indicates the current state.

Product Information
: Shows CPC information and machine information.

STP Information
: Shows the current Server Time Protocol (STP) status for the CPC.

Note: This tab is only available when STP is enabled and in the operating state.

Determining conditions causing test status

If the CPC's performance is affected, an object's icon displays **Test**. This indicates a conditions exists, such as PSW even compare or Address compare are enabled. To determined the exact conditions test status:

1. Locate the object.

   For instructions, see the topics that follow "Locating groups and objects" on page 2-6.
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 degraded status, select the *Test Mode* tab on the **Details** window.

   The Test Mode window displays the condition(s) for tests.

Use the online Help for more information on the test indicator.

Determining conditions causing Service Required or Degraded status

There are two types of status messages that cause the CPC to display status that may require attention.

1. **Service Required**

   This status displays in the *Acceptable CP/PCHID Status* tab on the Details window of the CPC. This indicates that the spare hardware shipped with the CPC has been depleted. When a part fails causing the use of the last redundant parts of that type, you now have just the required number of parts to keep the CPC running. This message is a reminder to you and the service representative that repairs should be made at the earliest possible time before addition. Some of the conditions that cause this message to be displayed are:
   - Loss of one bulk power assembly (BPA)
   - Loss of communications to the alternate support element
   - No more spare processing units (PUs)
   - Not enough spare PUs to support either Capacity BackUp or Disaster Recovery Assurance (if either feature is installed)
   - Memory sparing threshold reached
   - An Oscillator/ETR card is defective
   - The alternate support element is fenced
   - A multiple chip module (MCM) is defective.
2. **Degraded**

   This status message displays under the CPC icon in the Groups Work Area. This indicates that, although the CPC is still operating, some hardware is not working.

   Some of the conditions that cause this message to be displayed are:
   - Loss of channels due to CPC hardware failure
   - Loss of memory
   - One or more books are no longer functioning
   - The ring connecting the books is open
   - Capacity Backup resources have expired
   - Processor frequency reduced due to temperature problem
   - CPC was IMLed during temperature problem.

To view what conditions caused the degraded status message to display:

1. Locate the object.

   For instructions, see the topics that follow "Locating groups and objects" on page 2-6.

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 degraded status, select the *Degraded* tab on the **Details** window.

   The **Degraded Details** window displays the current list of reasons why the selected CPC is degraded.

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. 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 2-9. 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:

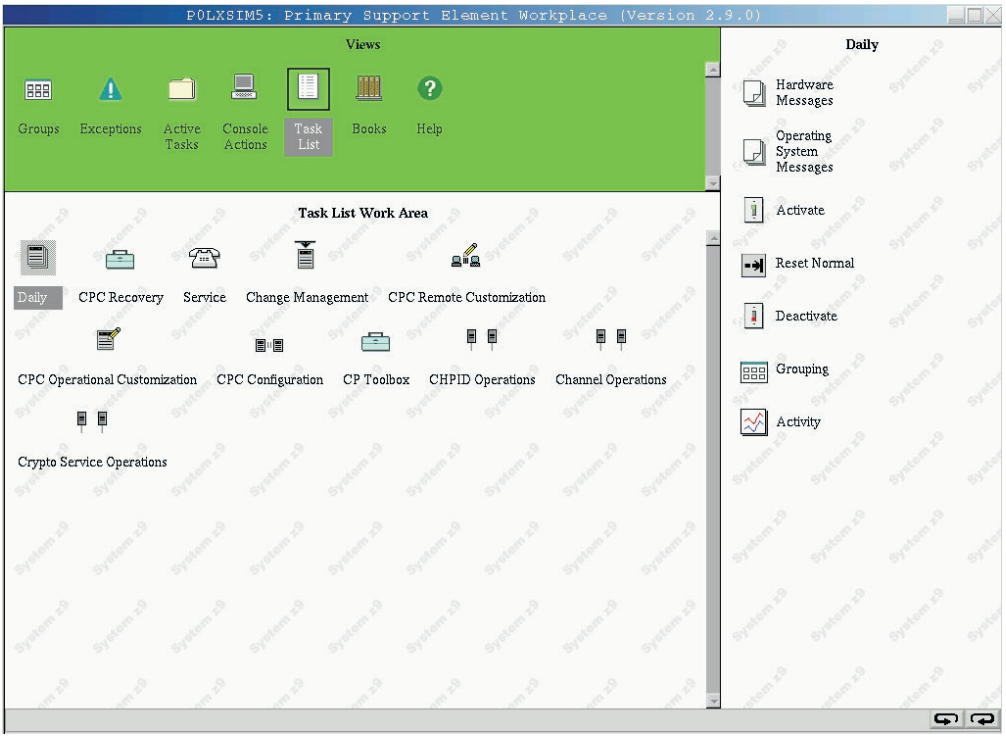
- Assign the exception in the Exceptions Work Area the activation profile you want to use.
- Locate an instance of the same exception, in any group that contains it, that is already assigned the activation profile you want to use.

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 5-41, 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. 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 task list to open it.
4. Locate the task list on the right side of the Support Element Workplace.

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

Note: To view the rings on the support element console, click the maximize icon in the upper right hand corner of the support element workplace.

Until you become familiar with the tasks contained in each task list, use the index of this operations guide to locate instructions for starting the task you want to perform. The instructions will identify the name of the task and the name of the task list that contains it.

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)
- Physical channels (PCHIDs)
- Central processors
- Logical channels (CSS.CHPIDs)
- 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 2-6.

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."

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 2-6.
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.

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 clicking **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 clicking **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 minimize icon of the active task's open window or message.

   Note: The minimize icon is located in the upper right corner of the window or message.

   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.

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. 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. 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.

To restore a minimized open window:

1. Click on the maximize icon located in the upper right corner of the workplace.

   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 object locking 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. 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 object you want to lock in the Work Area.
2. Right-click on the object's icon.
3. Click **CPC Details** from the menu.

   The CPC Details window opens.
4. Set **Lockout disruptive tasks** to **Yes** or **No**.
5. Click **Apply** to lock the object.

If you want to lock all CPCs or CPC images at one time, there is an automatic way to lock all them displayed on the workplace at one time. If using this method, you will cause an object to be relocked automatically if it was unlocked to perform a task on it.

1. Locate the objects you want to lock in the Work Area.
2. Open **Console Actions** from Views.

   This displays the console actions in the Console Actions Work Area.
3. Open the **Support Element Settings** task from the Console Actions Work Area.

   This displays the Support Element Settings Work Area.

4. Open the **Object Locking Settings** task from the Support Element Settings Work Area.
5. Select **Automatically lock all managed objects** or **Relock after a task has been run** or both. All objects currently in the work area are now locked.

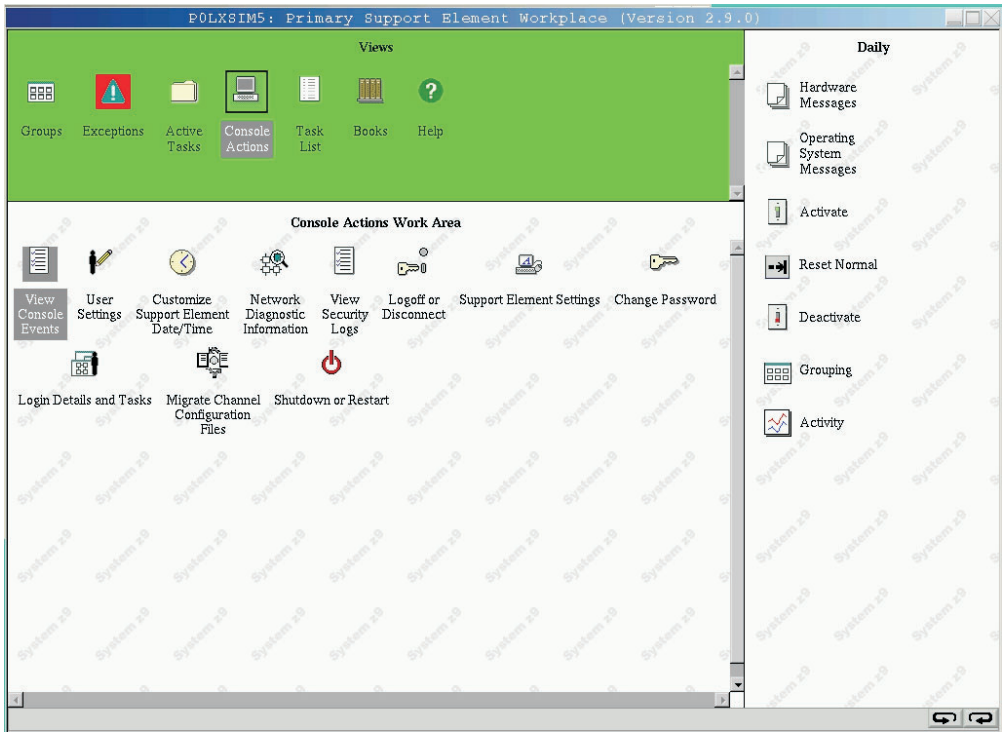
When the object(s) are locked, a small red lock in the upper left hand corner of the icon indicates that the disruptive tasks are locked for that object. If you attempt to perform a disruptive task on a locked object, a window is displayed indicating the object is locked.

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 **Lockout disruptive tasks** to **No**.
4. Click **Save** 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 “Console Actions” on page A-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:

Application Programming Interfaces for Java
: This online book describes the **com.ibm.hwmca.api** package. The purpose of this package is to allow Java™ applications, local or remote, the ability to exchange data related to the objects that the Console application manages.

Support Element Operations Guide
: This online book 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.

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.

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.

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. 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:

- Open **Console Actions** from Views.

  This displays the console actions in the Console Actions Work Area.
- Open the **User Settings** task from the Console Actions Work Area.

  This **User Settings** window is displayed.
- Select the **Controls** tab on the **User Settings** window.
- Select **Show hover help** from the menu choice. This places a check next to it and sets hover help on. If you want to set hover help off, uncheck the choice by selecting it from the menu.
- Click **Apply**, then click **OK** to enable hover help.

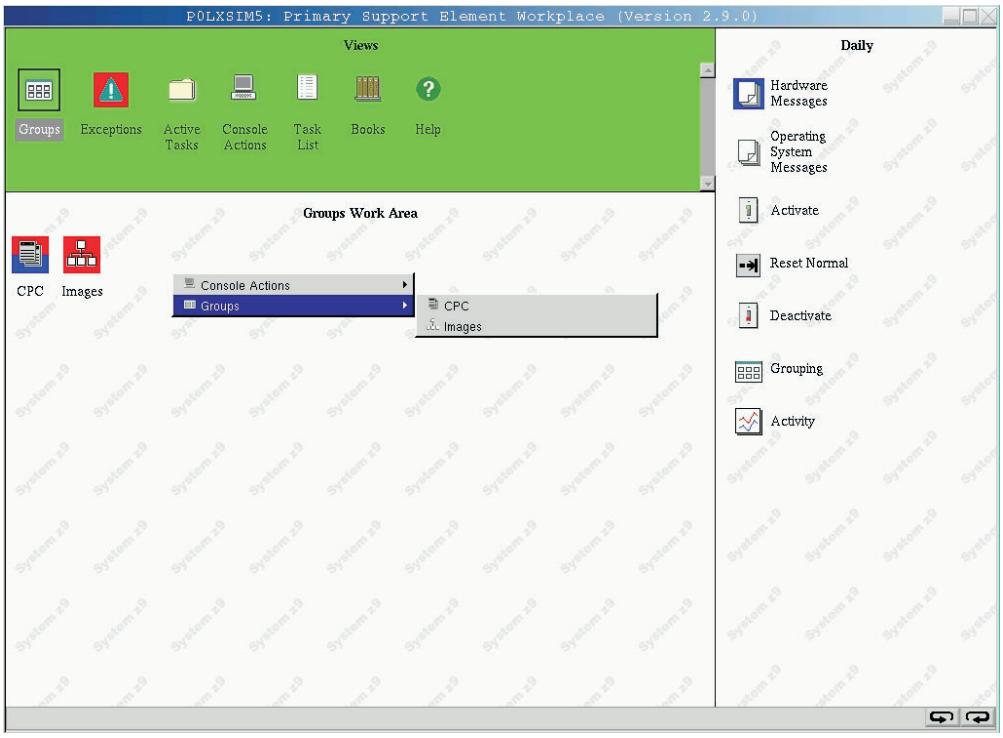
Note: Hover help is not displayed immediately. The cursor must remain placed on a workplace object for several seconds to display the help.

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 "User Interface" on page xiii

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 Console Actions in the Work Area and the Groups in the Work 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
- Starting console actions

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 program load (IPL)* 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:

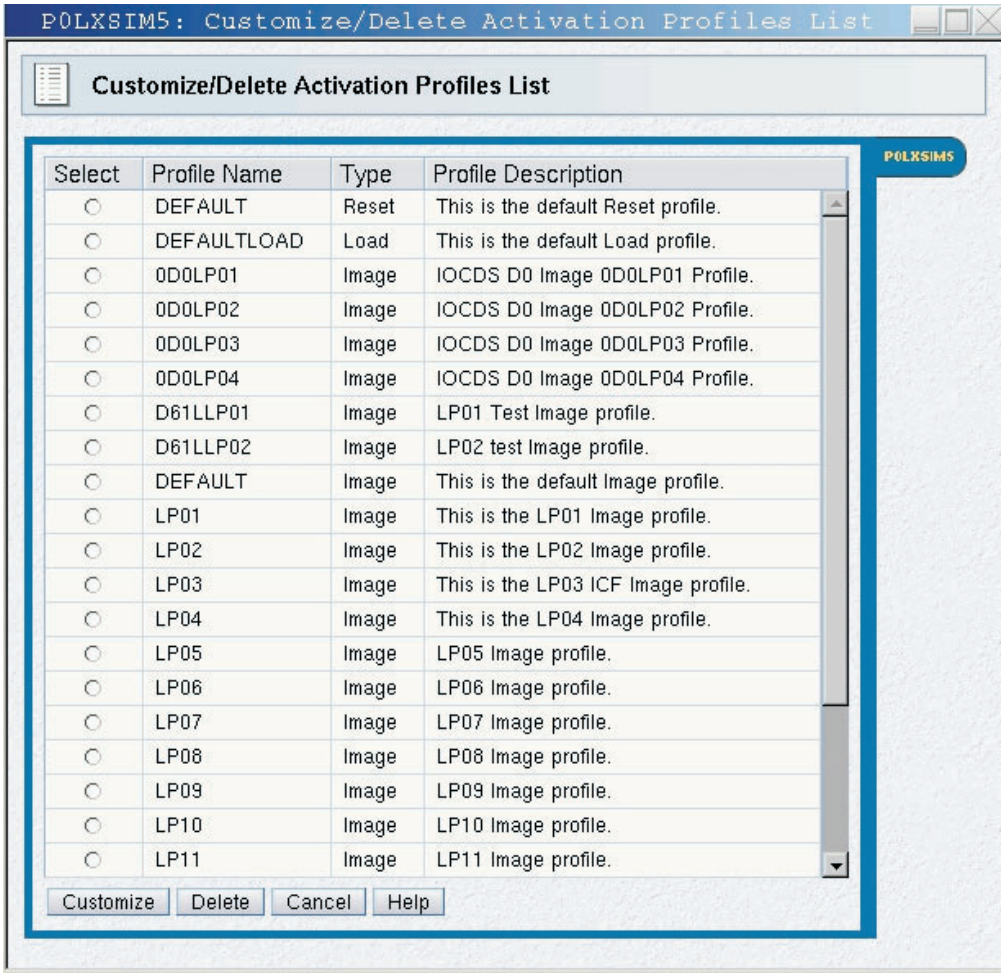
- Activating the CPC does not perform a power-on reset if the CPC has already been power-on reset and the applicable settings in its assigned activation profile, such as the operating mode and active input/output configuration data set (IOCDS), are already in effect.
- Activating the CPC does not perform 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 A-4 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 4, "Error recovery," on page 4-1.

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.
- 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, activate an image with its image profile to activate it individually rather than by activating the CPC.

Getting ready for an activation

To successfully activate a central processor complex (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 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*, SB10-7037.
- 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*, SB10-7040.

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. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, or service representative user mode (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
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 5-1.
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 3-4.
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 object locking for disruptive tasks on an object” on page 2-18.
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, click **Yes** to perform the activation.

    The Activate Progress window indicates the progress of the activation, and the outcome.
11. Click **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. Each logical partition is an image.

To activate an image:

1. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system

programmer, or service representative user mode (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).

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 5-1.
4. The system must have access to the operating system referred to in the activation profile. See “Getting ready for an activation” on page 3-4.
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 object locking for disruptive tasks on an object” on page 2-18.
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, Click **Yes** to perform the activation.

    This displays the Activate Progress window. The window indicates the progress of the activation, and the outcome.
12. Click **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 controls 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 click **Details**.

   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 that a 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 displays operating system messages from all images in the group. Using individual images displays 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 that 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 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 window provides a **Send** command 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 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.

Note: The utilization reported by Activity for most channel types coincides with the utilization reported by Resource Management Facility (RMF™). For Fiber Channels, the **Activity** task considers the channel to be busy any time an operation is pending, even if the channel is waiting for a device to respond. RMF looks at the amount of work done versus the amount of work that could be done by the channel. Therefore, if you have devices that are relatively slow to respond, leaving the channel waiting for a response that would be otherwise idle, Activity shows a utilization that is significantly higher than that reported by RMF

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)
  - General purpose processors
  - Internal Coupling Facility (ICF) processors
  - Integrated Facility for Linux (IFL) processors
  - Integrated Facility for Applications (IFA) processors
  - IBM System z9 Integrated Information Processors (zIIPs)
- System assist processors (SAPs)
- Channels
- Logical partition(s) and logical processor(s)

Note: Central processors (CPs) include the General purpose processors, Internal Coupling Facility (ICF) processors, Integrated facility for Linux (IFL) processors, Integrated facility for applications (IFA) processors, and IBM System z9 Integrated Information Processors (zIIPs).

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. 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.

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.

  Note: Central processors (CPs) include the General purpose processors, Internal Coupling Facility (ICF) processors, Integrated facility for Linux (IFL) processors, Integrated facility for applications (IFA) processors, and IBM System z9 Integrated Information Processors (zIIPs).
- 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. 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 30 logical partitions and some physical processor activity. 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.
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:** You can customize this profile, or a copy of it, to display activity for up to 30 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.
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 3-15.
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 z/VM® and 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 3-15.

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” on page 3-14.

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 includes the channel activity and physical processing activity that has been defined in the system activity profiles that are stored in the selected CPC. For more information about assigning and customizing activity profiles for the CPC, see "Getting ready to monitor the system: customizing system activity profiles" on page 5-51.

Because you are selecting a single object for the task, both a summary window and a details window appear. This details window shows the detailed System Activity Display (SAD) for an object as a rectangular chart.

The Summary window displays the system activity for each object is on a single line. The activity displayed as a blue bar is the average of all reported physical processor processing activity for the CPC. The activity displayed as a green bar is the average of all reported channel activity for the CPC. One or both types of activities can be displayed for the selected objects. A red bar indicates that activity data is not available for the object.

Starting the **Activity** task when another instance of the task is already running does not stop the previous task instance.

Note: The utilization reported by the **Activity** task for most channel types will agree with the utilization reported by Resource Measurement Facility (RMF™). For fiber channels, however, this task considers the channel to be busy any time an operation is pending, even if the channel is waiting for a device to respond. Whereas, RMF looks at the amount of work done versus the amount of work that could be done by the channel. This means that if you have response but otherwise idle, **Activity** will show a utilization that is significantly higher than that reported by RMF.

To start system activity analysis:

1. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, or service representative user mode (see "Establishing a support element console session from a Hardware Management Console" on page 1-2).
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 5-52.
   - 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.
4. 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. To monitor the true processing activity while using an operating system that uses an active wait state, like some versions of z/VM and 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."

   b. 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."

   c. 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 3-16.

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 z/VM and 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 initial logical or reserved processors" on page 5-21.

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 display 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) determines which IOCDS is used to 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 the left mouse button 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. Click **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, images are your targets for resets. An image represents a logical partition, while the CPC is activated.

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

To perform a reset normal:

1. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, or service representative user mode (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
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 object locking for disruptive tasks on an object” on page 2-18
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, Click **Perform reset** to perform the reset normal.
9. Click **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 4, “Error recovery,” on page 4-1.

Shutting down and turning off the system

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

Shutting down and turning off the system, referred to also as *deactivating* the system, includes:

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

Deactivating the CPC

You can use the support element workplace to start the task for deactivating the central processor complex (CPC). The target, or *object*, of a deactivation can be a CPC or an image. For more information about deactivating individual logical partitions, see “Deactivating an image” on page 3-19.

Note: Although you can use the power switch on the CPC itself to turn it off, you should turn off CPC power by deactivating it instead. Unlike using the CPC’s

power switch, deactivating the CPC includes clearing, releasing, and deallocating its hardware resources before turning off its power.

To deactivate the CPC:

1. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, or service representative user mode (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
2. End all operating systems supported by the CPC’s images.

   Important: If you do not end 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 object locking for disruptive tasks on an object” on page 2-18.
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, click **Yes** to perform the deactivation.

   The Deactivate Progress window indicates the progress of the deactivation, and the outcome.
10. Click **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. Each logical partition is an image. You can use one or more images as deactivation targets to deactivate individual logical partitions.

To deactivate an image:

1. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, or service representative user mode (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
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 object locking for disruptive tasks on an object” on page 2-18.
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, click **Yes** to perform the deactivation.

   The Deactivate Progress window indicates the progress of the deactivation, and the outcome.
9. Click **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.

Logging Off the Support Element Console

Log off the support element of each system that is to be powered off:

- Open **Console Actions** from the Views area.
- Select **Shutdown or Restart** from the Console Actions Work Area.

  The Shutdown or Restart window displays.
- Select **Shutdown console** from the Shutdown or Restart window.
- Click **OK**.

After logging off the integrated support element, shutdown the Hardware Management Console, see “Turning Off the Hardware Management Console” in the *Hardware Management Console Operations Guide*.

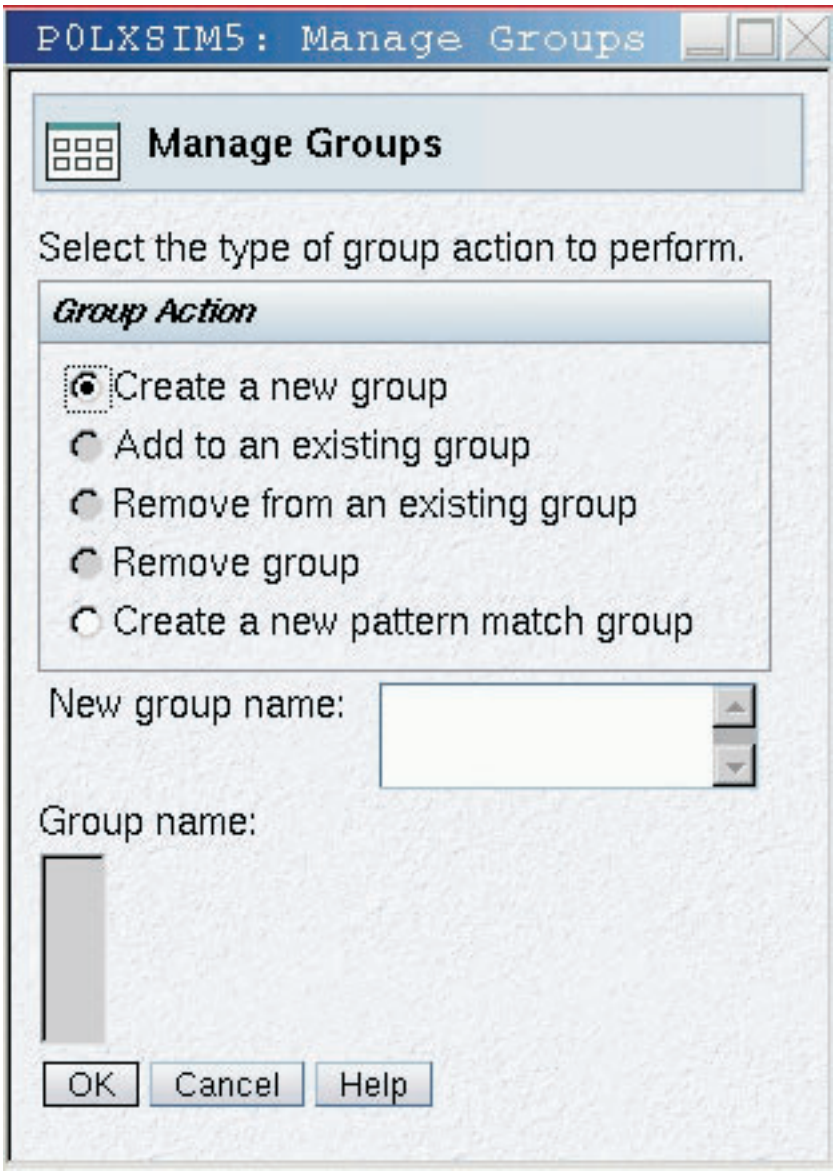
Managing Groups of Objects

Managing groups enables you to create, delete, add to, and delete from user-defined groups of objects. You may want to create a group when you want to perform the same task on several CPC images simultaneously instead of repeating the task on each individual CPC image. This task also allows you to group one or more user-defined groups into other groups.

To group images:

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
2. Open the **Task List** from the **Views** area.
3. Open **Daily** from the **Task List Work Area**.

   The Daily task list contains the **Grouping** task that you will start.
4. Open **Groups** from the **Views** area.
5. Open the group that contains the CPC images that you want to group.
6. Select one or more objects.
7. Drag and drop the selected objects on **Grouping** task in the **Daily** tasks area to start it. The Manage Groups window displays to allow you to add the selected object(s) to an existing group, delete the selected object(s) from a group, create a new group, create a pattern match group, or delete the group.



Use the online Help if you need additional information for working with groups.

You may want to group one or more user-defined groups into other groups if you have many groups in your Groups Work Area and need additional work area space. However, if you group user-defined groups into other groups, you cannot perform any task other than **Grouping** on these groups.

To group groups of user-defined images:

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
2. Open the **Task List** from the **Views** area.
3. Open **Daily** from the **Task List Work Area**.

   The Daily task list contains the **Grouping** task that you will start.
4. Open **Groups** from the **Views** area.
5. Open the group that contains the CPC images that you want to group.

6. Select one or more objects.
7. Drag and drop the selected objects on **Grouping** task in the **Daily** tasks area to start it. The Manage Groups window displays.
8. Click **Create a new group** in the **Group Action** box.
9. Enter a *group name* in the **New group name** box.
10. Click **OK**. A **Create a New Group** pop-up window displays stating you successfully created a new group.
11. Click **OK**. The new group is now displayed in the Group Work Area.
12. Select another group that you want to add to the group you just created above.
13. Drag and drop the selected group on **Grouping** in the **Daily** tasks area. The Grouping window displays.
14. Click **Add to an existing group** in the **Group Action** box.
15. Select the *group name* you created in **step 9** above from the **Group Name** box.
16. Click **OK**. The Add to an Existing Group pop-up window displays telling you successfully added a group to another group.
17. Click **OK**. The group is no longer displayed in the Group Work Area because it is now part of the group you created in **step 9**.
18. Repeat **steps 12** through **17** for as many groups that you want to add to the new group.

As previously stated, you cannot perform tasks on grouped groups. They can only be performed on the group that contains the individual CPC images. You can get access to this group or the individual images in the group using either of these methods:

- Double-click the grouped icon in the Groups Work Area. This opens up the groups that are nested in the preceding group. Continue double-clicking each nested group until the group that contains the individual CPC images is displayed, or
- Open the workplace pop-up menu
  1. Right-click on any empty area in the workplace. This opens the workplace pop-up menu.
  2. Point to **Groups** to open its cascaded menu. Continue selecting each cascaded menu until the individual group that contains the CPC images that you want to perform an action on is displayed and click that item.

Chapter 4. Error recovery

This section describes the tasks from the **CPC Recovery** task list typically needed to attempt to recover from hardware or software errors. 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.

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. An image represents a logical partition, while the CPC is activated.

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 11, “Processor and storage operations,” on page 11-1 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. 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. Log onto the support element on the hardware management console through **Single Object Operations** in advanced operator, system programmer, or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
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 object locking for disruptive tasks on an object” on page 2-18.
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. Log onto the support element on the hardware management console through **Single Object Operations** in advanced operator, system programmer, or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
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 object locking for disruptive tasks on an object" on page 2-18.

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 resets 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. An image represents either:

- A central processor complex (CPC)
- A logical partition (LPAR).

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. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, or service representative user role (see "Establishing a support element console session from a Hardware Management Console" on page 1-2).
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 object locking for disruptive tasks on an object” on page 2-18.

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, Click **Yes** to perform the reset normal.

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

   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. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
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 object locking for disruptive tasks on an object” on page 2-18.
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, Click **Yes** to perform the reset clear.

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

   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*.You can have up to four Load types: Normal, Clear, SCSI, and SCSI dump.

For daily or routine loading of images, it is recommended that you customize activation profiles to specify how you want to load images, and then use a profile

with the **Activate** task to perform all the operations necessary to make an image operational, including loading it with a control program.

Load (except for a coupling facility image) causes a program to be read from a designated device and initiates the execution of that program. On the support element workplace, *images* support operating systems, so images are your targets for loads. An image represents a logical partition, while the CPC is activated.

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

To perform a load:

1. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
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 object locking for disruptive tasks on an object” on page 2-18.
6. Drag and drop the image on the **Load** task to start it.
7. On the Load window:
   a. Use the controls to identify the operating system you want to load, and to indicate how you want to perform the load.
   b. Click **OK** to perform the load using the information you provided.

      The Load Task Confirmation window is displayed.
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, click **Yes** to perform the load.

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

   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 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. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
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 object locking for disruptive tasks on an object” on page 2-18.
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 Dynamic page to establish the hardware support required to use dynamic input/output (I/O) configuration.
   c. Use the Options page to set the operating environment and enable or disable the global input/output (I/O) priority queuing for the CPC.
   d. Use the CP/SAP page to select a CP/SAP configuration to optimize the performance of the CPC.
9. Select **Perform power-on reset** to perform the power-on reset using the information you provided in the window.
10. Click **Power-on reset** to perform the power-on reset.

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

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.

Use the online Help for more information on performing a power-on reset.

Installing software from a CD-ROM, DVD or FTP server

This task allows you to install system software or utility programs from a CD-ROM/DVD or from an FTP server. You can specify only one software source.

Note: The installation of some software, such as certain levels of z/VM, requires you to not remove the CD-ROM, DVD from the Hardware Management Console's drive until directed. Refer to the installation instructions that come with your software for more information.

To install software from a CD-ROM/DVD or FTP server:

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see "Establishing a support element console session from a Hardware Management Console" on page 1-2).
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, DVD, or Server** task that you will start.
4. Open **Groups** from the **Views** area.
5. Open a group that contains the CPC.
6. Drag and drop the CPC on the **Load from CD-ROM, DVD, or Server** task to start it.

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

   The Load from CD-ROM, DVD, 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.
9. Click **Continue**

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

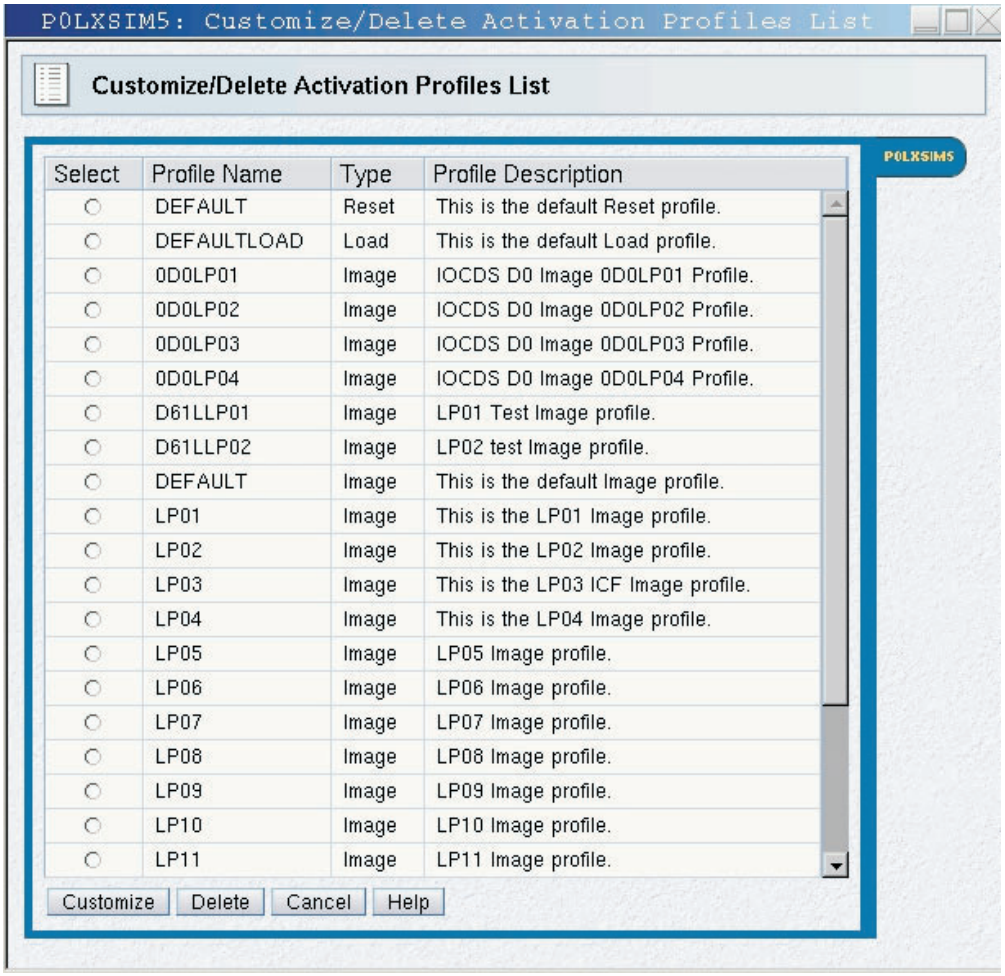
    The progress window indicates the duration and elapsed time of the program loaded.
12. Click **OK** to close the window when the task completes successfully.

Chapter 5. Settings for system operations

This section describes the tasks from the **CPC Operational Customization** task list 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.

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.
- 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, 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 activation.
  - 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 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 image profiles included in it.

Other options for using profiles

You can customize load profiles and image profiles. After you use a reset profile to activate the central processor complex (CPC), you can use individual load profiles or image profiles as follows:

- 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.
- 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 one or more image profiles. A reset profile includes an image profile by referencing its unique profile name. While you are customizing a reset profile, you have the option of customizing the image profiles included in it. You can also customize load profiles and image profiles individually. 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.

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 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.

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 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" on page 5-4.

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. 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 5-31.

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 activate the CPC, then load them with operating systems.

- See “Activating CPCs” on page 5-7, “Activating logical partitions” on page 5-16, and “Loading operating systems” on page 5-27.

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. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2). 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. Click **Customize** to open the selected reset profile.

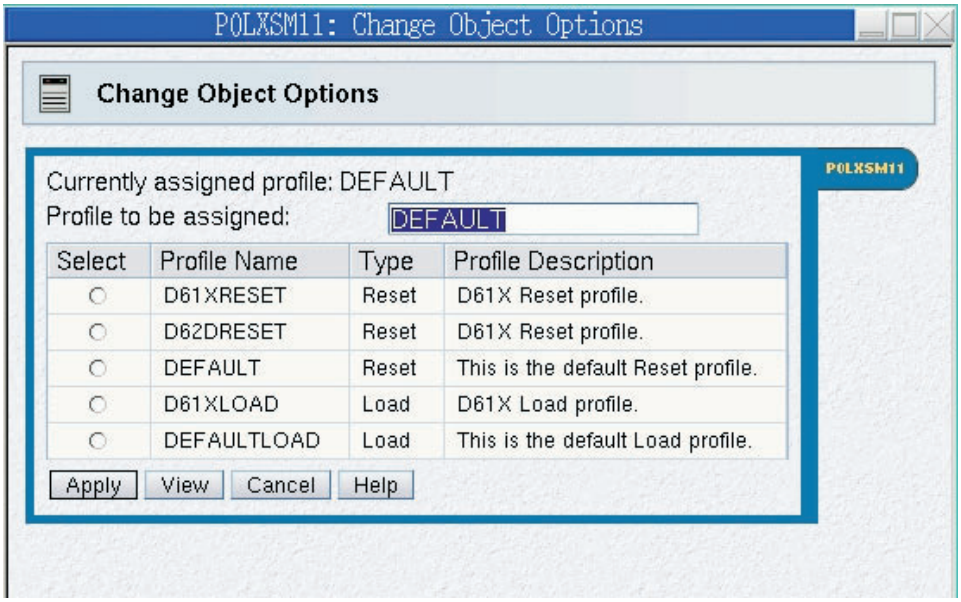
   After you start the task, use the online Help for more information about the control.

Checking the CPC's assigned activation profile: You can assign a 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 check and change a CPC's 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. Click **Change options**.



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. 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.

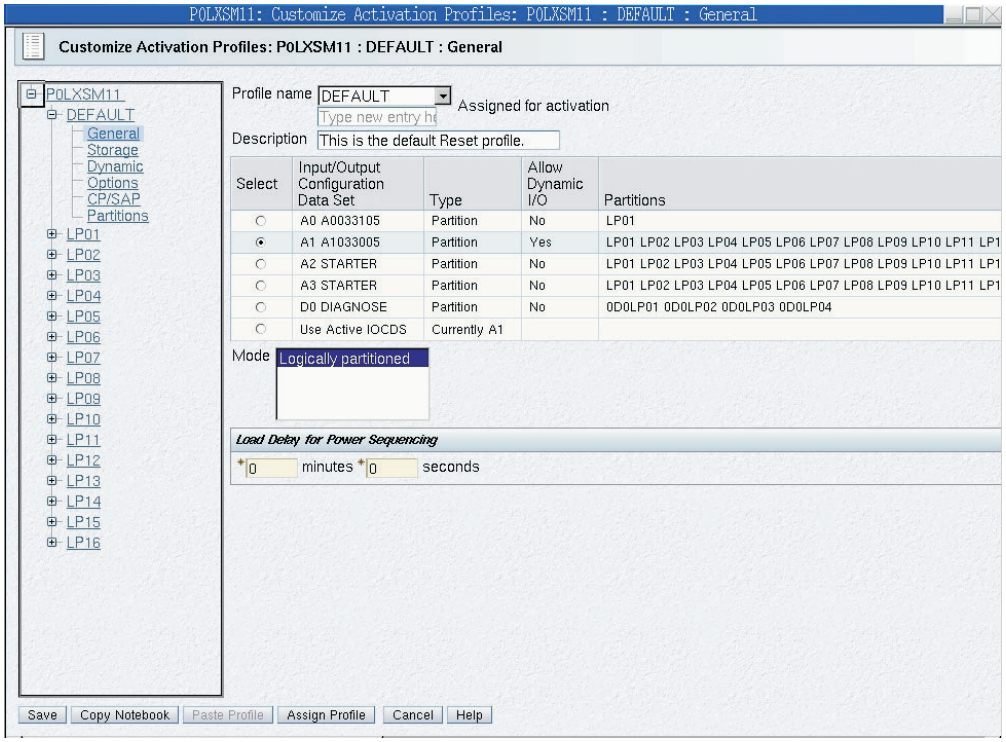
   Note: The list includes all the reset profiles and load profiles that can be assigned to the CPC.
7. If the assigned profile's type is **Reset**, then no further action is required.
8. Otherwise, the assigned profile's type is **Load**. If you want to assign the CPC a reset profile, use the window to select and save a reset profile.

   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 the windows that are organized as pages in a notebook.

The pages are identified in a profile tree view on the left side of the window with a description label. If the reset profile activates the CPC with multiple images, the profile tree view list the names of each image section with the identifying name. The information in each section is used to activate a single object either the CPC or a logical partition.



To use the profile tree view to open each page on the window:

- Click on the description label for each page within a section of the profile you want to open.
- Click on the '**+**' for each image to get a list of pages in the section of the profile.
- To save the changes made, click **Save**.
- To close the window, click **Cancel**.

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.

To create a new reset profile:

1. Open a reset profile.

   For more information, see "Opening a reset profile" on page 5-4.
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 window.
6. To create a new profile from the template, select **Editable value** at the bottom of the drop-down list
7. Enter a unique name for the new profile in the **Profile name** field.
8. To save the profile with the new name, click **Save**.

   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. To assign the reset profile as the CPC's activation profile, click **Assign 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. To save the reset profile and close it, click **Save**.

Activating CPCs

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

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. 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.

To customize a reset profile to support operating the CPC :

1. Open a reset profile.

   For more information, see "Opening a reset profile" on page 5-4.

2. Select the General page.
3. Select from the **Input/Output Configuration Data Set** list an IOCDS that defines the logical partitions you want to activate.

   Notes:

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

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

Use the online Help for more information.

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.

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” 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 5-4.
2. Select the General page.

   Use the online Help for more information.
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
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. 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. 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 z/OS® and OS/390® operating systems.
- The dynamic I/O configuration facility of some z/VM and 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 5-4.
2. Select 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."
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
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 5-4.
2. Select the General page.
3. Enter 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.

Use the online Help for more information.

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.

Changing the hardware I/O definition requires performing another power-on reset, and changing the software I/O definition requires loading the software again. 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 z/OS and OS/390 or other operating system that supports dynamic I/O.
  - Written using the DYN option of the input/output configuration program (IOCP) utility of a z/VM and 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."
- Dynamic I/O must be enabled for a logical partition.

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 5-4.
2. Select 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** column displays **Yes** to indicate an IOCDS supports dynamic I/O.
4. Select 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.

Use the online Help for more information on Dynamic I/O.

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. After a power-on reset of the CPC is performed, changing its operational capabilities and characteristics requires performing another power-on reset.

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. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see "Establishing a support element console session from a Hardware Management Console" on page 1-2). 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 any group that contains 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 **Enabled** or **Disabled**, indicates the current setting.
   b. While dynamic I/O is enabled, select **Disabled** to change the setting to disabled.
   c. Or while dynamic I/O is disabled, select **Enabled** to change the setting to enabled.
   d. Click **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 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 5-4.

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: If you intend to activate a CPC, 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 initial logical or reserved processors” on page 5-21.

Changing the CP/SAP allocation without performing a power-on reset: You can reassign your system CP/SAP allocations to optimize performance of applications without performing a power-on reset of the CPC. Changing the CPs to SAPs requires reassignment of the current licensed internal code. You must ensure the CPs being converted to SAPs can be deconfigured and are not dedicated.

To reassign or restore the CP/SAP allocation:

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2). 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 **Change CP/SAP Allocation** 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 **Change CP/SAP Allocation** task to start it.

   This displays the Change CP/SAP Allocation window.

7. Use the spin buttons to change or restore the CP/SAP allocation for the CPC.
8. Click **Perform the Updates** to activate the changes.

   Use the online Help for more information on using the window to change or restore the CP/SAP allocations.

Planning for a fenced book:

The reset profile you use to activate a central processor complex (CPC) can determine how the available system processors would be assigned when a hardware problem occurs with one of the system books that cause the book to be fenced or become unavailable for use.

Note: To display this Fenced page, select **Display fenced book page** on the CP/SAP page.

To customize a reset profile to let the CPC determine the processor assignment:

1. Open a reset profile.

   For more information, see “Opening a reset profile” on page 5-4.
2. Select the Fenced page.
3. Locate the Processor Assignment group box.
4. Select the **Determined by the system** radio button.

To customize a reset profile to set a processor assignment by the user:

1. Open a reset profile.

   For more information, see “Opening a reset profile” on page 5-4.
2. Select the Fenced page.
3. Locate the Processor Assignment group box.
4. Select the **Determined by the user** radio button.
5. Type the values in the **Value Used when Book is Fenced** field.

Use the online Help for more information about using it.

Enabling or disabling the global input/output (I/O) priority queuing: The reset profile you use to activate a CPC can enable or disable the global input/output (I/O) priority queuing.

To customize a reset profile for enabling or disabling global input/output (I/O) priority queuing:

1. Open a reset profile.

   For more information, see “Opening a reset profile” on page 5-4.
2. Select the Options page.
3. Locate the **Enable global input/output (I/O) priority queuing** check box. Then either:
   - Mark the check box to enable global input/output priority queuing. The check box displays a check mark when you mark it.
   - Or unmark the check box to disable global input/output priority queuing. The check box becomes empty when you unmark it.

Use the online Help for more information about using it.

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 5-4.
2. Select 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.

Use the online Help for more information.

Setting processor running time: The reset profile you use to activate a central processor complex (CPC) can set whether you or the CPC determines the processor running time.

When the CPC is activated, 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 5-4.
2. Select 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 5-4.
2. Select 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, you can use the support element workplace to dynamically change its settings for processor running time. See “Logical partition controls” on page 8-3 for more information.

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) can also activate one or more logical partitions.

To customize a reset profile to activate logical partitions during CPC activation:

1. Open a reset profile.

   For more information, see “Opening a reset profile” on page 5-4.
2. If you have not already done so, customize the reset profile to activate the CPC. For more information, see “Supporting LPAR mode operation” on page 5-7.
3. Select 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, enter 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 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 5-4 or "Opening a logical partition's image profile" on page 5-32.
2. If you opened a reset profile, select the name of the logical partition from the profile tree on the left side of the window.
3. Select 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'3F'.

   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. *Coupling facility* and *Linux Only* 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 5-4 or "Opening a logical partition's image profile" on page 5-32.
2. If you opened a reset profile, select the name of the logical partition from the profile tree from the left side of the window.
3. Select 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 5-4 or “Opening a logical partition’s image profile” on page 5-32.
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 5-16.
   b. To customize the information used to activate the coupling facility logical partition, select the name of the logical partition from the profile tree on the left side of the window.
3. Select 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 (main storage)” on page 5-27.

Using internal coupling facility processors: If internal coupling facility processors are installed in the CPC, you can assign a coupling facility logical partition either central processors, internal 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 5-4 or “Opening a logical partition’s image profile” on page 5-32.
2. If you opened a reset profile, select the name of the logical partition from the profile tree on the left side of the window.
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 internal coupling facility processors
   b. Not dedicated internal coupling facility processors

c. Dedicated internal coupling facility processors and not dedicated central processors.
d. Dedicated and not dedicated internal coupling facility processors.

Note: There are other options for assigning processors to the partition that are available, but these other options DO NOT use Internal coupling facility.

7. Use the controls available to complete the logical partition assignment for the coupling facility logical partition.

Assign both internal 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 integrated facility for Linux processors: If integrated facility for Linux facility processors are installed in the CPC, you can assign an integrated facility for Linux logical partition either central processors or integrated facility for Linux processors.

To customize an activation profile to assign logical processors to an integrated facility for Linux logical partition:

1. Open a reset profile or open an image profile.

   For more information, see “Opening a reset profile” on page 5-4 or “Opening a logical partition’s image profile” on page 5-32.
2. If you opened a reset profile, select the name of the logical partition from the profile tree on the left side of the window.
3. Select the General page.
4. Select **LINUX Only** from the **Mode** list.
5. Select the Processor page.
6. Select the type of processors you want assigned to the integrated facility for Linux logical partition:
   a. Dedicated integrated facility for Linux
   b. Not dedicated integrated facility for Linux

   Note: There are other options for assigning processors to the partition that are available, but these other options DO NOT use Integrated Facility for Linux.
7. Use the controls available to complete the logical partition assignment for the integrated facility for Linux logical partition.

Using integrated facility for application processor: If integrated facility for application processors are installed in the CPC, you can assign an integrated facility for application logical partition either central processors or integrated facility for application processors.

To customize an activation profile to assign logical processors to an integrated facility for application logical partition:

1. Open a reset profile or open an image profile.

For more information, see “Opening a reset profile” on page 5-4 or “Opening a logical partition’s image profile” on page 5-32.

2. If you opened a reset profile, select the name of the logical partition from the profile tree on the left side of the window.
3. Select the General page.
4. Select **ESA/390** from the **Mode** list.
5. Select the Processor page.
6. Use the Logical Processor Assignments group box to:
   a. Select **Dedicated processors** and **Integrated facility for applications** if you want to assign *integrated facility for applications* to each logical partition.
   b. Select **Integrated facility for applications** to assign **not** dedicated *integrated facility for applications* to logical partitions when the logical partition is activated.
7. Use the controls available to complete the logical partition assignment for the integrated facility for application logical partition.

   Note: There are other options for assigning processors to the partition that are available, but these other options DO NOT use Integrated Facility Applications.

Using System z9 integrated information processors: If the System z9 integrated information processors are installed in the CPC, you can assign a System z9 integrated information logical partition either central processors or System z9 integrated information processor.

To customize an activation profile to assign logical processors to a System z9 integrated information logical partition:

1. Open a reset profile or open an image profile.

   For more information, see “Opening a reset profile” on page 5-4 or “Opening a logical partition’s image profile” on page 5-32.
2. If you opened a reset profile, select the name of the logical partition from the profile tree on the left side of the window.
3. Select the General page.
4. Select **ESA/390** from the **Mode** list.
5. Select the Processor page.
6. Use the Logical Processor Assignment group box to:
   a. Select **Dedicated processors** and **System z9 integrated information processor** if you want to assign *System z9 integrated information processors* to each logical partition.
   b. Select **System z9 integrated information processor** to assign **not** dedicated *System z9 integrated information processors* to logical partitions when the logical partition is activated.
7. Use the controls available to complete the logical partition assignment for the System z9 integrated information logical partition.

Setting WorkLoad Manager (WLM) controls: The activation profile you use to activate a logical partition can manage your defined capacity for a logical partition. See “Setting defined capacity” on page 5-27 to set defined capacity for logical partitions. WorkLoad Manager allows you to run all of your work concurrently while allocating system resources to the most work first. WorkLoad Manager constantly monitors your system, automatically adjusting the resource allocation as necessary.

Note: To customize Integrated Facility for Applications (IFAs) and System z9 Integrated Information Processors (zIIPs) you must select the processor type from the *Not Dedicated Processor Details* section prior to setting the processing weight values.

To customize an activation profile to allow WorkLoad Manager to manage logical partitions:

1. Open a reset profile or open an image profile.

   For more information, see “Opening a reset profile” on page 5-4 or “Opening a logical partition’s image profile” on page 5-32.
2. If you opened a reset profile, select the name of the logical partition from the profile tree on the left side of the window.
3. Select the General page.
4. Select **ESA/390** or **LINUX Only** from the **Mode** list.
5. Select the Processor page.
6. Unmark the **Initial Capping** box.

   Note: You cannot mark the **Initial Capping** box if the **Enable WorkLoad Manager** is enabled. You must unmark it to allow Initial Capping to be marked.
7. Mark the **Enable WorkLoad Manager** check box to enable WorkLoad Manager.

   A check box displays a check mark when you mark it.
8. Enter the processing weight values for the logical partition that you want to be managed by WorkLoad Manager.

Assigning initial logical or reserved processors: The activation profile you use to activate a logical partition can assign it initial logical or reserved processors.

An initial logical processor is the processor resource defined to operate in a logical partition as a physical central processor. Initial logical processors are the processors a control program uses to perform jobs for the logical partition.

Reserved processors can be defined at partition activation time, but not used during partition activation. The reserved processor is not available when the system is activated, but can become available during concurrent central processor (CP) upgrade.

To customize an activation profile to assign initial 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 5-4 or “Opening a logical partition’s image profile” on page 5-32.
2. If you opened a reset profile, select the name of the logical partition from the profile tree on the left side of the window.
3. Select the Processor page.
4. Enter the number of initial logical processors to assign to the logical partition or the number of reserved processors.

   Note: You can only reserve integrated facility for applications (IFA) processors prior to installation.
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 8-3 for more information.

Using the Crypto Express2 feature: The activation profile you use to activate a logical partition can prepare it for running software products that utilize the Crypto Express2 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 X2 coprocessor or X2 accelerator. This is accomplished by selecting from the Usage Domain Index and the Cryptographic Candidate list.
- Load it with an operating system, such as z/OS, that supports using cryptographic functions.
- Install the CP Assist for Cryptographic Facility (CPACF) DES/TDES Enablement feature if planning to use ICSF.

For more information about the cryptographic feature, see “The Crypto Express2 Feature” on page 9-15.

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 5-4 or “Opening a logical partition's image profile” on page 5-32.
2. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
3. Select the General page.
4. Select **ESA/390** , **ESA/390 TPF**, or **LINUX Only** from the **Mode** list.
5. Select **Crypto** from the profile tree view on the left side of the window. Use the controls on the Crypto page to indicate whether and how you want the logical partition to use the cryptographic functions and facilities.

   Notes:

   a. If you intend to use the Integrated Cryptographic Service Facility (ICSF), see “Using the z/OS Integrated Cryptographic Service Facility (ICSF)” 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) Workstation feature” on page 5-23 for additional instructions for customizing the Crypto page.

   c. After activating logical partitions customized to use X2 coprocessors and X2 accelerators, you can use the support element workplace to view the settings of the cryptographic controls set on the Crypto page of their activation profiles. See “Viewing logical partition cryptographic controls” on page 8-4 for more information.
6. 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 “Loading operating systems” on page 5-27.

Using the z/OS Integrated Cryptographic Service Facility (ICSF): The z/OS Integrated Cryptographic Service Facility (ICSF) is a program product that provides

secure, high-speed cryptographic services in the operating environment. You can use ICSF services for all logical partitions that are customized for using X2 coprocessors and X2 accelerators.

Note: Some functions of ICSF may fail if you do not have the CP Assist for Cryptographic Functions (CPACF) DES/TDES Enablement feature installed. See the *ICSF Application Programmer's Guide* or the *ICSF System Programmer's Guide* for complete information.

The activation profile you use to activate a logical partition can prepare it for using ICSF services. Customize the activation profiles when installing the CP Assist for Cryptographic Functions (CPACF) DES/TDES Enablement feature.

To customize an activation profile for a logical partition to use the ICSF services :

1. Customize a reset profile or image profile to configure the logical partition access to the cryptographic facilities and functions.

   For more information, see "Using the Crypto Express2 feature" on page 5-22
2. Select the Crypto page again.
3. If you have not already set the logical partition's controls, set them now:
   a. Select a usage domain index for the logical partition to use for cryptographic functions from the **Usage domain index** list. More than one number should be selected from the **Usage domain index** when z/VM operating environment is running in the logical partition with other guests (for example, Linux) requiring access to the cryptographic hardware.

      Note: The cryptographic number, selected from the Cryptographic Candidate List, coupled with the usage domain index must be unique for each active partition.
4. Select from the Online List the number which specifies the coprocessors to be brought online at partition activation. For each number selected in the Online List, the corresponding number in the Candidate List must be selected.

Using the Trusted Key Entry (TKE) Workstation feature: A Trusted Key Entry (TKE) is a workstation application supported by ICSF to allow an alternative method of securely loading cryptographic keys (DES and PKA master keys and operational keys). A unique set of cryptographic keys is maintained for each domain index within the cryptographic facility. Only one partition can perform TKE functions at a time. The logical partition with this control is referred to as the TKE host. The other partitions that receive key updates from the TKE host are referred to as the TKE targets.

The activation profile you use to activate a logical partition can prepare it for being a TKE host or TKE target.

To use a TKE workstation to manage requests for secure information or commands to a specific X2 coprocessor, permission must be given. See "Changing permission for TKE commands" on page 9-18.

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 Crypto Express2 feature" on page 5-22.
2. Select the Crypto again.
3. If you have not already set the logical partition's controls, set them now:

a. Select a usage domain index for the logical partition to use for cryptographic functions from the **Usage domain index** list. It must be the same as the usage domain index set for the logical partition in the ICSF installation options data set.

   Note: The cryptographic number, selected from the Cryptographic Candidate List, coupled with the usage domain index must be unique for each active partition.

4. Select from the Online List the number which specifies the coprocessors to be brought online at partition activation. For each number selected in the Online List, the corresponding number in the Candidate List must be selected.
5. 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.

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.

A logical partition has access to only its own performance data. 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 5-4 or “Opening a logical partition’s image profile” on page 5-32.
2. If you opened a reset profile, select the page tab that displays the name of the logical partition.
3. Select 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 8-1 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 5-4 or “Opening a logical partition’s image profile” on page 5-32.
2. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
3. Select 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 8-1 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 z/OS and OS/390 operating systems.
- The dynamic I/O configuration facility of some z/VM and VM operating systems.

Input/output configuration control must be enabled for the logical partition that 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 5-4 or “Opening a logical partition’s image profile” on page 5-32.
2. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
3. Select 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 8-1 for more information.

Using the automatic reconfiguration facility (ARF): The automatic reconfiguration facility (ARF) is supported by z/OS and OS/390. 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*, SB10-7036 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.

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 5-4 or “Opening a logical partition’s image profile” on page 5-32.
2. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
3. Select 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 8-1 for more information.

Allocating storage: The activation profile you use to activate a logical partition can allocate its storage.

Allocating central storage (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 5-4 or “Opening a logical partition’s image profile” on page 5-32.
2. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
3. Select 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.

Setting I/O priority queuing values: The activation profile you use to activate a logical partition can control the I/O priority queuing assignment of logical partitions.

To customize an activation profile for I/O priority queuing:

1. Open a reset profile or open an image profile.

   For more information, see “Opening a reset profile” on page 5-4 or “Opening a logical partition’s image profile” on page 5-32.
2. If you opened a reset profile, select the page tab that displays the name of the logical partition.
3. Select the Options page.
4. Use the controls to set minimum and maximum I/O priority queuing values.

Setting defined capacity: The activation profile you use to activate a logical partition can control the defined capacity for a logical partition. A defined capacity is the portion of your processor resources you order from IBM.

Your defined capacity can be associated with:

- A license software product. You specify a defined capacity for a product on the product certificate.
- An LPAR. You specify a defined capacity for an LPAR using the appropriate LPAR controls. A defined capacity applies to the entire LPAR, no matter how many applications it contains.

To customize an activation profile to set defined capacity:

1. Open a reset profile or open an image profile.

   For more information, see “Opening a reset profile” on page 5-4 or “Opening a logical partition’s image profile” on page 5-32.
2. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
3. Select the Options page.
4. Enter the defined capacity value for your logical partition.

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 is a central processor complex (CPC) activated in a logical partition.

To customize an activation profile to load an operating system during an object's activation:

1. Open an applicable activation profile:
   - 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 5-4 or "Opening a logical partition's image profile" on page 5-32.

     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 5-17.
2. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
3. Select 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.

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 *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 activation profile:
   - Open a reset profile or open its image profile.

     For more information, see "Opening a reset profile" on page 5-4 or "Opening a logical partition's image profile" on page 5-32.

     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 5-17.
   - Or open a load profile.

     For more information, see "Opening a load profile" on page 5-36.
2. If you opened a reset profile, select the name of the logical partition from the profile tree on the left side of the window.

3. Select the Load page.

   Note: If you opened a load profile, the Load page is the first and only page.
4. Enter the load address in the **Load address** field.
5. Enter 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 must be activated on a CPC that supports dynamic I/O configuration. 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 z/OS and OS/390 operating systems.
- The dynamic I/O configuration facility of some z/VM and 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 activation profile:
   - Open a reset profile or open its image profile.

     For more information, see “Opening a reset profile” on page 5-4 or “Opening a logical partition’s image profile” on page 5-32.

     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 5-17.
   - Or open a load profile.

     For more information, see “Opening a load profile” on page 5-36.
2. If you opened a reset profile and the object is a logical partition, select the name of the logical partition from the profile tree on the left side of the window.
3. Select the Load page.

   Note: If you opened a load profile, the Load page is the first and only 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.

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 activation profile:
   - Open a reset profile or open its image profile.

     For more information, see “Opening a reset profile” on page 5-4 or “Opening a logical partition’s image profile” on page 5-32.

     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 5-17.
   - Or open a load profile.

     For more information, see “Opening a load profile” on page 5-36.
2. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
3. Select the Load page.

   Note: If you opened a load profile, the Load page is the first and only page.
4. Enter the time limit, from 60 to 600 seconds, in the **Time-out value** field.

Setting SCSI attributes: The activation profile you use to load an image can set the SCSI parameters used to perform the load.

The *Worldwide port name* is the number identifying the Fibre Channel port of the SCSI target device. This field contains the 64-bit binary number designating the port name, represented by 16 hexadecimal digits.

The *Logical unit number* is the number of the logical unit as defined by FCP. This field contains the 64-bit binary number designating the unit number of the FCP I/O device, represented by 16 hexadecimal digits. This field is required for SCSI IPL and SCSI dump.

The *Boot program selector* is a decimal value number specifying the program to be loaded from the FCP-load device during SCSI IPL or SCSI dump. Valid values range from 0 to 30.

The *Boot record logical block address* is the load block address field represented by 16 hexadecimal characters, designating the logical-block address of a boot record on the FCP-load device. If no block address is specified, the logical-block address of the boot record is assumed to be zero.

The *OS specific load parameters* is a variable number of characters to be used by the program that is loaded during SCSI IPL or SCSI dump. This information will be given to the IPLed operating system and will be ignored by the machine loader. The IPLed operating system has to support this.

To customize an activation profile to set the SCSI parameters:

1. Open an activation profile:
   - Open a reset profile or open its image profile.

     For more information, see “Opening a reset profile” on page 5-4 or “Opening a logical partition’s image profile” on page 5-32.

     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 5-17.
   - Or open a load profile.

For more information, see “Opening a load profile” on page 5-36.

2. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
3. Select the Load page.

   Note: If you opened a load profile, the Load page is the first and only page.
4. Enter the worldwide port name in the **Worldwide port name** field.
5. Enter the logical unit name in the **Logical unit number** field.
6. Enter the boot program number in the **Boot program selector** field.
7. Enter the boot record logical block address in the **Boot record logical block address** field.
8. Enter the OS specific load number in the **OS specific load parameters** field.

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 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. For more information, see “Supporting LPAR mode operation” on page 5-7 and the other topics that follow “Activating CPCs” on page 5-7.

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.

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.

Optionally, you can customize the image profile to also load the logical partition during activation.

Notes:

1. Initially activating a CPC requires customizing and using a reset profile. For more information, see “Supporting LPAR mode operation” on page 5-7 and the other topics that follow “Activating CPCs” on page 5-7.
2. 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 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. Starting the task is referred to also as *opening an image profile*.

To open a logical partition's image profile:

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
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. Click **Customize**.

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.

In addition, whenever you start the task for customizing the logical partition's activation profiles, it opens the logical partition's assigned activation profile. After you start the task, you can customize its assigned activation profile. If its assigned activation profile is a load profile, you can also create new load profiles or open and customize any other existing load profiles.

For example, to customize the image profile for a logical partition, its assigned activation profile must be its image profile. You can check, and change if necessary, the logical partition's assigned activation profile before you begin customizing its profiles.

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. Click **Change options**.

   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. 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.

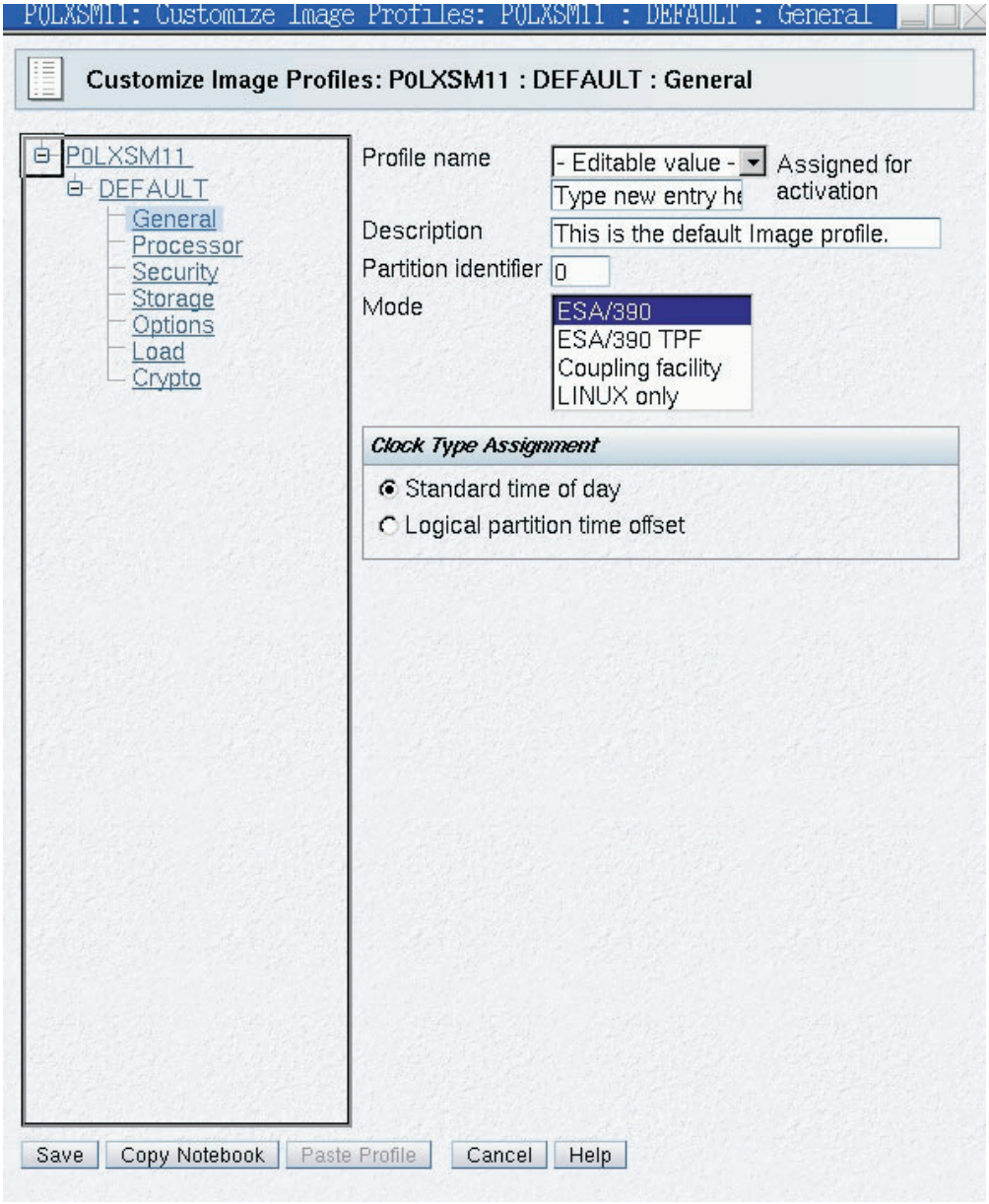
   Note: The list includes the logical partition's image profile and all the load profiles that can be assigned to the logical partition.
8. If the assigned profile's type is **Image**, then no further action is required.

   Whenever you start the task for customizing the logical partition's activation profiles, you will be able to customize the logical partition's image profile.
9. If the assigned profile's type is **Load**, you will be able to customize only load profiles.

   To assign the logical partition its image profile instead, use the window to select and save the image profile.

Navigating the image profile network: An image profile includes information for activating a logical partition.

Opening an image profile displays its information on the window organized in a profile tree view.



The pages are identified in a profile tree view on the left side of the window with a description label. The description label for each page is a general description of the information on the page.

To use the profile tree view to turn to a different page of the image profile:

- Click on description label in the profile tree view that you want to open.
  A window opens to that page of the image profile.
- To save the changes made, click **Save**.
- To close the window, click **Cancel**.

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

You can use the default image 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 image profiles, you can use them as templates for creating more new profiles.

To create a new image profile:

1. Open a image profile.

   For more information, see “Opening a logical partition’s image profile” on page 5-32.
2. Select the General page.

   The **Profile name** field identifies the image profile you opened. It will be used as a template for the new image profile.
3. To use a different image 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 image profiles. The image profile named DEFAULT is the default image profile provided by IBM.
5. Select from the list the name of the image profile you want to use as a template.

   This opens the selected image profile. Its information replaces the previous profile’s information on the pages of the notebook.
6. To create a new profile from the template, select **Editable value** at the bottom of the list
7. Enter a unique name for the new profile in the **Profile name** field.
8. Click **Save** to save the profile with the new name.

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

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. Click **Save** to save the image profile and close it.

customizing image profiles: The best way to customize an image profile is to go through the image profile window, 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 window. It provides additional information about each page and its controls.

The online Help is meant to assist you while you are actually customizing an image profile. It explains the purpose of each page and its controls, and how to customize them to activate a logical partition the way you want it activated.

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.

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.

Note: Initially activating a logical partition requires customizing the reset profile that activates the CPC. For more information, see “Activating CPCs” on page 5-7, and the topics that follow “Activating logical partitions” on page 5-16.

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. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
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. Click **Customize**.

   This opens the selected load profile. Its information replaces the previous profile's information on the notebook page.

Use the online Help for more information.

Choosing a CPC load type: normal, clear, SCSI, or SCSI dump: The activation profile you use to load a central processor complex (CPC) can perform either a normal, clear, SCSI, or SCSI dump load.

To customize an activation profile to choose a CPC load type:

1. Open a load profile.

   For more information, see "Opening a load profile" on page 5-36.
2. 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.
   - Select **SCSI** to perform a SCSI load (from certain types of channels), which clears main storage during the load.
   - Or select **SCSI dump** to perform a SCSI dump (to do a standalone dump from a SCSI IPL type of device).

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 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 activation profile:
   - Open a load profile.

     For more information, see "Opening a load profile" on page 5-36.
2. Select the Load page.

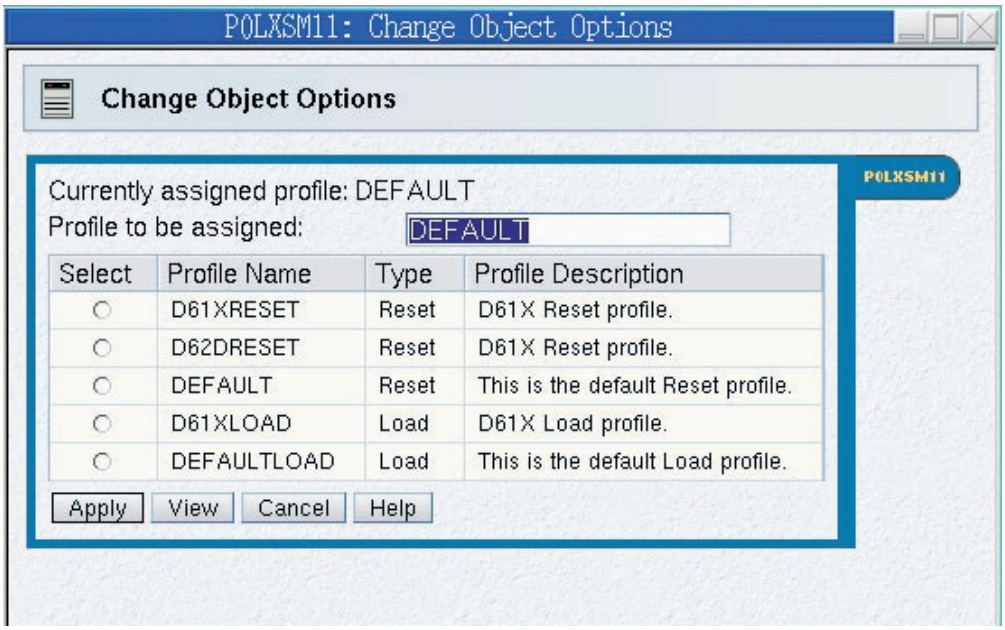
   Note: If you opened a load profile, the Load page is the first and only page.
3. Locate the **Load type** controls. Select **Normal** to perform a normal load, which performs the load without clearing main storage.
4. Mark the **Store status** check box.

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.

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.

Whenever you start the task for customizing the object's activation profiles, it opens the object's assigned activation profile. After you start the task, you can create new profiles or open and customize any other existing profiles *of the same type* as the assigned activation profile.

For example, to customize load profiles for a CPC, its assigned activation profile must be a load profile. You can check, and change if necessary, an object's assigned activation profile before you begin customizing its profiles.



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. 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. Click **Change options**.

   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. 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.
8. If the assigned profile's type is **Load**, then no further action is required.

   Whenever you start the task for customizing the object's activation profiles, you will be able to customize any load profile.
9. Otherwise, if the assigned profile's type is not **Load**, but is **Reset** or **Image** instead, you will be able to customize only the same type of profiles for the object.

   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 5-36.
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, select **Editable value** at the bottom of the list
5. Enter a unique name for the new profile in the **Profile name** field.
6. Click **Save** 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.

customizing load profiles: The best way to customize a load profile is to go through the one-page load profile window, 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 window.

The online Help is meant to assist you while you are actually customizing a load profile. It explains the purpose of the page and its controls, and how to customize them to load a central processor complex (CPC) or logical partition the way you want it loaded.

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. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, or service representative user role (see "Establishing a support element console session from a Hardware Management Console" on page 1-2).
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 click **View**.

This opens the selected activation profile.

Use the online Help for more information.

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, click **Change options**.
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 click **Save**.

   This sets the selected profile as the object's assigned activation profile, and returns to the object details window.
10. Click **Save** 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. You can customize a reset profile for a complete activation of the CPC.

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.

To assign the CPC a reset profile for activating it:

1. Create a group with the CPC for activating it:
   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 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.
- And 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, 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.

So, 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.

Then 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.

To enable or disable automatic activation:

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
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 any group that contains 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. Click **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). You must use the CPC's support element 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:

- 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.
- Accessing external time source for the CPC.

  This operation automates the task you perform manually by using the **System (Sysplex) Time** 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. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
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 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 **Customize Scheduled Operations** task to start it.

   Select a menu from the menu bar.
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. The CPC TOD clock is synchronized automatically to either the support element TOD clock or a time synchronization source.

Synchronizing the CPC TOD clock to a time synchronization source

A *Sysplex Timer* is a device that provides a time source to the time-of-day (TOD) clocks of Central Processor Complexes (CPCs) attached to it and the operating systems or control programs running on that server (CPC). A feature called an *External Timer Reference (ETR)* installed in the CPC provides two ETR attachment facility (EAF) ports for attaching Sysplex Timers. Both ports may attach the same Sysplex Timer, or each port may attach a separate Sysplex Timer when configured with 9037 Expanded Availability.

An ETR network consists of one Sysplex Timer or coupled Sysplex Timers (Expanded Availability), and the links from this source to the system. Each system has two ETR attachment facility (EAF) ports which can be connected by a link to the Sysplex Timer.

Server Time Protocol (STP) is a time synchronization architecture designed to provide the capability for multiple servers (CPCs) to maintain time synchronization with each other and to form a Coordinated Timing Network (CTN). STP is designed for servers (CPCs) that have been configured to be in a Parallel Sysplex or a sysplex (without a Coupling Facility), as well as servers (CPCs) that are not in a sysplex, but need to be time synchronized. STP is designed as a message-based protocol allowing time keeping information to be sent between servers (CPCs) and Coupling Facilities (CFs) over InterSystem Channel-3 (ISC-3) links configured in peer mode, Integrated Cluster Bus-3 (ICB-3) links, or Integrated Cluster Bus-4 (ICB-4) links.

While the CPC is attached to an operational Sysplex Timer or is using Server Time Protocol (STP), and if the CPC's operating or control program supports using the Sysplex Timer or Server Time Protocol (STP) as a time source:

- The Sysplex Timer or Server Time Protocol (STP) is used as a time source for the CPC TOD clock.
- The CPC TOD clock maintains clock synchronization with the Sysplex Timer or Server Time Protocol (STP). When the Sysplex Timer is the time source, the CPC TOD clock steps at the same rate as the Sysplex Timer. When STP is the time source, the CPC TOD clock continuously steers the TOD to the correct time.
- The CPC TOD clock is automatically synchronized to the Sysplex Timer or Server Time Protocol (STP) whenever the time or date at the Sysplex Timer or at the Current Time Server of an STP-only Coordinated Timing Network is changed.

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:

- If the CPC does not or cannot use a Sysplex Timer or Server Time Protocol (STP) 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.
- If the CPC uses a Sysplex Timer or Server Time Protocol (STP) as a time source, changing the time or date at the Sysplex Timer or at the Current Time Server in an STP-only Coordinated Timing Network automatically synchronizes the CPC TOD clock to the new time.
- 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.
  - The support element TOD clock is updated with local time adjustments (daylight saving time offset, leap seconds offset, and time zone offset) when they occur, if it is synchronized with the CPC TOD clock.
  - 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 or Server Time Protocol (STP) as a time source for the CPC is intended to prevent manually setting the support element TOD clock.

If the CPC does not or cannot use a Sysplex Timer or Server Time Protocol (STP) as a time source, you can manually set the support element TOD clock. See "Setting the support element time-of-day clock manually" on page A-15.

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 in use 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, 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. So 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:

- For each logical partition defined but *not* activated during CPC activation, 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 5-1.
- For information about allocating storage for a logical partition, see "Allocating storage" on page 5-26.

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.

Precise estimates of the HSA size vary according to several conditions, including:

- The CPC model and engineering change (EC) level.
- Operating the CPC increases the HSA size. 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.

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.

To review the current storage allocations:

1. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer or service representative user role (see "Establishing a support element console session from a Hardware Management Console" on page 1-2). 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 any group that contains 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 top of the window identify its pages. Select a page tab to display that page.
   - The first page of the window displays information about storage installed and allocated for the CPC. Its page tab is labelled: Base system storage allocation.
   - If the CPC is activated, the window includes a second tab 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 window 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 any group that contains 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. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer or service representative user role (see "Establishing a support element console session from a Hardware Management Console" on page 1-2). 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 any group that contains the CPC from the **Groups Work Area**.
6. Drag and drop the CPC on the **Storage Information** task to start it. The window displays the current storage allocation of the CPC and its logical partitions.
7. Page tabs along the top of the window identify its pages. Select the page tab labelled Base system storage allocation, if necessary, to display that page.
8. Locate the Installed Storage Details group box on the page.
9. Add the storage amounts displayed in the following fields in the group box:
   - **Central storage**
   - **Expanded storage**
   - **Base hardware system area (HSA)**

   The sum is the degraded storage amount.

Use the online Help for more information about using the window to review the current storage allocations.

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. Furthermore, 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 5-6.
2. 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.

  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 5-6.
  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 5-26.
  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, 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 5-26.
  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.

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. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2). 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 **System Activity 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 **System Activity Profiles** task to start it.

   This opens the Customize System Activity window.

   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.”

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, Customize System Activity Profile, by clicking **Cancel**. 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 for which 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 5-52.

   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 click **Customize**.

   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.
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.

   Note: Central processors (CPs) include the general processors, internal coupling facility processors, integrated facility for Linux processors, and integrated facility for application processors.

   Change one or more activity lines to:

   - Define the particular system resources you want to monitor.
   - Set conditions for which 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 click **OK** 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. Click **OK**.

      This opens 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.
   e. Select the radio button that describes the particular system resource you want to monitor, then click **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.
   g. Click **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 clicking **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 click **OK** 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**.

b. From the list of activity lines, select the line you want to modify with the option you selected.

c. Click **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, enter in the **Description** field a brief description of the types of activity the profile can be used to monitor.

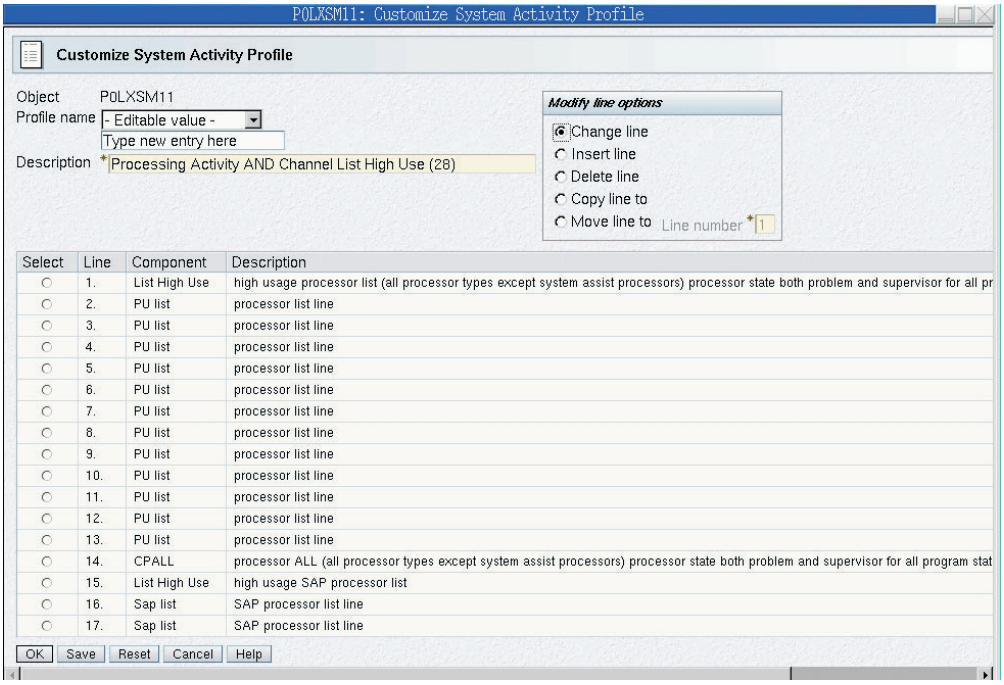
      Note: Providing a profile description is recommended. Whenever a list of system activity profiles is opened, either to work with the profiles or to start system activity analysis, profile names *and* descriptions are listed to help you distinguish between the different profiles and their purposes.

   b. Click **Save** 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 5-52.

This opens the Customize System Activity Profiles List window. Its page lists the CPC's system activity profiles, and it provides controls 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 click **Customize**.

   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, select **Editable value** at the bottom of the drop-down list.
4. Enter a new, unique name for the new profile in the **Profile name** field.
5. Customize any other information in the profile as needed. For instructions, see "Customizing a system activity profile" on page 5-52.
6. Click **Save** 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

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.

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. You can assign the CPC other active profiles as needed, to choose in advance the system activity you want to monitor.

To assign profiles for monitoring system activity:

1. Open a list of system activity profiles. For instructions, see "Opening a list of system activity profiles" on page 5-52.

   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.

   Note: The column displays **Active for HWMCA** to indicate the profile is assigned to the CPC for monitoring its activity. 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.

   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.
5. Click **Change status** 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 will use the active profiles.

Note: If system activity analysis of the CPC is already in progress, it will begin using the CPC's newly assigned active profiles shortly after their status is changed.

Exporting and importing profile data

This task allows you to export or import activation profiles or system activity profiles for the CPC to a diskette or to your hard drive. Exporting and importing profiles is necessary only when you intend to have your current system and support element replaced with a new system and support element. When a Capacity Backup Upgrade (CBU) is activated, more processors (CPs, SAPs, ICFs) are activated in the system. In most cases, this requires you to change your activation profiles to include these new processors in the next activation. Otherwise, the CP/SAP split in the reset profile and the number of dedicated CPs/ICFs and other processor options in the Image profile won't specify the correct options.

To export/import profile data:

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see "Establishing a support element console session from a Hardware Management Console" on page 1-2). 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 **Export/Import Profile 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 **Export/Import Profile Data** task to start it.

   The Export/Import Profiles window displays.
7. Select from the options to export/import your activation profiles or system activity profiles for the CPC to a DVD-RAM or hard drive.
8. Click **OK**.

   Use the online Help for more information about exporting/importing profile data.

Chapter 6. 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).

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.

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 6-3 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 A-13.
- "Performing Problem Analysis of optical errors" on page A-13.

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 a DVD-RAM 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, DVD-RAM and diskettes remain eligible sources. 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. 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" 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 a DVD-RAM 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. 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, DVD-RAM and diskettes remain eligible destinations. If you intend to *schedule an operation* for transmitting service data regularly and automatically, the IBM Service Support System is the only eligible destination. 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" 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. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see "Establishing a support element console session from a Hardware Management Console" on page 1-2).
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 **Groups 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.
8. To enable remote service:
   a. Check **Enable remote service**.

      The check mark displays 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. Identify the Customer Service Center Telephone Number 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.
9. To enable automatic service calling, check **Authorize automatic service call reporting**.

   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.
10. Click **OK** to save the settings and close the window.

Use the online Help for more information about using the window to customize the settings.

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. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see "Establishing a support element console session from a Hardware Management Console" on page 1-2).
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 **Customer Information** task that you will start.
4. Open **Groups** from the **Views** area.
5. Drag and drop the CPC on the **Customer Information** task to start it.

   The Customize Customer Information window displays.
6. Proceed through each tabbed window for your administrator, system, and account fields.
7. Click **Save** to save the information and close the notebook.

Use the online Help for more information about using the page to customize the information.

Chapter 7. System testing, problem determination, and service

This section describes the 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.

When in service, the CPC status displayed on its Details window will be **Service** and no other status will be reported by the CPC until service status is disabled. The background of the support element workplace also displays **Service** while service status is enabled. During a service action, status changes (for example, no power) that would normally cause an execution due to an unacceptable status will not cause an exception when the status is service.

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. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
2. Open the **Task List** from the **Views** area.
3. Open **Service** from the **Task List Work Area**.

   The Service task list contains the **Service Status** 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 **Service Status** task to start it.

   This displays the **Service Status** window.
7. Select one or more objects using the check boxes.
8. Point to **Options** from the menu bar and then click **Enable service status**, **Disable service status**, or **Display error message** to enable or disable service status or display error messages, respectively
9. Click **Save** to save your changes.
10. Click **Yes** when you are ready to save your changes.

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 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. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, or service representative user role (see "Establishing a support element console session from a Hardware Management Console" on page 1-2).
2. Open the **Task List** from the **Views** area.
3. Open **Service** from the **Task List Work Area**.

   The Service task list contains the **Checkout Tests** task that you will start.
4. Open **Groups** from the **Views** area.
5. 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 object locking for disruptive tasks on an object" on page 2-18.
6. Drag and drop the CPC on the **Checkout Tests** task to start it.

   This displays the Checkout Tests window.
7. Click **Run test** 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 6-3 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 3-7 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. 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.
- 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 window. Its page lists the CPC's hardware messages, and it provides controls 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 click **Details**.

   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, click **Request service** 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.
   - 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. 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. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, or system programmer user role (see "Establishing a support element console session from a Hardware Management Console" on page 1-2).
2. Open the **Task List** from the **Views** area.

3. Open **Service** from the **Task List Work Area**.

   The Service task list contains the **Perform Problem Analysis** 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 **Perform Problem Analysis** task to start it.
7. 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. 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. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
2. Open the **Task List** from the **Views** area.
3. Open **Service** from the **Task List Work Area**.

   The Service task list contains the **Report a Problem** 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 **Report a Problem** task to start it.
7. Select the type of the problem you have from the list provided and enter a description of the problem in the **Problem Description** box.

   Note: If you are just testing problem reporting, select **Test automatic problem reporting** and enter *This is just a test* in the **Problem Description** box.
8. Click **Request Service**.

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 a DVD-RAM 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. 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 6-3 for instructions for enabling remote service.

To send service data to IBM:

1. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, or service representative user role (see "Establishing a support element console session from a Hardware Management Console" on page 1-2).
2. Open the **Task List** from the **Views** area.
3. Open **Service** from the **Task List Work Area**.

   The Service task list contains the **Transmit Service 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 Service Data** task to start it.
7. 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. Collecting and storing information is often referred to as *dumping data*.

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. Like other types of service data, sending dump data to IBM is necessary only when dump data is requested by IBM.

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 that 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 7-8 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 data, the CPC must be power-on reset.
2. To dump coupling facility logical partition dump data, the CPC must be power-on reset, and a logical partition must be activated in coupling facility mode.
3. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
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” on page 7-8.
9. Use the window's controls to select the type of dump you want to perform, then click **OK** 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. 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. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see "Establishing a support element console session from a Hardware Management Console" on page 1-2).
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 click **Delete** to delete them.

   Otherwise, if you only wanted to check the type, time, and date of previously dumped data, click**Cancel** to end the task *without* deleting the previously dumped data.

Dumping SCSI IPL data

SCSI IPL machine loader data is stored automatically by the support element of the central processor complex (CPC). The first 32 MB of storage in the targeted logical partition is gathered and sent to IBM.

Like other types of service data, SCSI IPL machine loader data assist IBM in servicing the CPC. Like other types of service data, sending SCSI IPL machine loader data to IBM is necessary only when dump data is requested by IBM.

To dump SCSI IPL machine loader data:

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
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 Machine Loader Data** 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 dump SCSI IPL on an image can be considered disruptive. If the CPC image is locked, unlock it. See “Setting object locking for disruptive tasks on an object” on page 2-18
6. Drag and drop the CPC on the **Dump Machine Loader Data** task to start it.

   The Dump SCSI IPL Loader Data Confirmation window displays.
7. Click **Yes** to perform the dump.

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 service is 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.

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. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
2. Open the **Task List** from the **Views** area.
3. Open **Service** from the **Task List Work Area** area.

The Service task list contains the **View Service History** task that you will start.

4. Open **Groups** from the **Views** area.
5. Open the **CPC** group from the **Groups Work Area**.

   This open the CPC Work Area. The area contains the target CPC.
6. Drag and drop the CPC on the **View Service History** task to start it.
7. Use the Service History window to select a menu item from the following:

   View

   Problem summary
   Displays detailed information about the selected problem including machine type, model, and serial number information.

   Problem analysis panels
   Redisplays the Problem Analysis (PA) windows that were created when the selected problem was originally reported.

   Repair information
   Displays repair information for the selected problem.

   Exit Ends the task.

   Close

   Selected problem
   Changes the current status of the selected problem to be closed.

   All problems
   Changes the current status of all open problems to be closed.

   Sort

   By date
   Lists problems in the order of the dates on which problems occurred, starting with the most recent problem.

   By system name
   Lists problems by the alphabetical order of the names of the objects on which they occurred.

   By status
   Lists all open problems, followed by all closed problems.

Use the online Help for more information about the problem and service information on it.

Offloading Virtual RETAIN® Data to the HMC DVD

This task allows you to copy problem data onto a hardware management console DVD media when there is no external connections for your hardware management console to send problem data.

To offload Virtual RETAIN data to the HMC DVD:

1. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer,

access administrator, or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).

2. Open the **Task List** from the **Views** area.
3. Open **Service** from the **Task List Work Area** area.

   The Service task list contains the **Offload Virtual Retain Data to HMC DVD** 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 **Offload Virtual Retain Data to HMC DVD** task to start it.

   The Virtual Retain Data Offload window displays.
7. Select a problem number from the listbox in the window.

   A formatted DVD must be loaded in the hardware management console DVD drive.
8. Click **OK** to initiate the offload.

   This offload process takes approximately 4 to 6 minutes to complete.

   Use the online Help for more information on offloading RETAIN data.

Checking the STI status

This task allows you to view the state and status of the primary Self Timing Interface (STI) and chain links and to display which PCHID/CSS.CHPID are controlled by the selected STI.

To check STI status:

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user mode (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
2. Open the **Task List** from the **Views** area.
3. Open **Service** from the **Task List Work Area** area.

   The Service task list contains the **STI Status Control** 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 **STI Status Control** task to start it.

   The STI Status Control window displays.
7. Click **OK** to close the window.

   Use the online Help for more information on STI status.

Chapter 8. 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. After the CPC is activated, 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.

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.

View LPAR Cryptographic Controls
Use this task to view the settings that determine how logical partitions use the cryptographic functions of the Crypto Express2 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 5-1
- Tips for activating logical partitions:
  - "Controlling access to performance data" on page 5-24
  - "Controlling I/O configuration changes" on page 5-24
  - "Authorizing control of other logical partitions" on page 5-25
  - "Controlling use of reconfigurable channel paths" on page 5-26

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. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see "Establishing a support element console session from a Hardware Management Console" on page 1-2).
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 any group that contains the CPC 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 object locking for disruptive tasks on an object" on page 2-18.
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

   Use the online Help for more information about changing logical partition security.
7. Use the check boxes to change the logical partitions' security settings, then use the controls to indicate what you want to do with the new settings.

   Use the online Help for more information about changing logical partition security.

   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, how they are assigned as either dedicated or shared processor resources, and the processing weights of logical partitions. The settings control how a partition is workload managed and whether software pricing is to change based on the number of defined capacity.

Processor running time
: These CPC settings control how its logical partitions' 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 5-1
- "Assigning initial logical or reserved processors" on page 5-21
- "Setting processor running time" on page 5-15
- "Setting defined capacity" on page 5-27
- "Setting WorkLoad Manager (WLM) controls" on page 5-20

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. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
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 object locking for disruptive tasks on an object” on page 2-18.
6. Drag and drop the CPC on the **Change LPAR Controls** task to start it.

   This displays the Change Logical Partition Controls window.
7. Depending on the physical processors installed in your system (CPs, ICFs, IFLs, IFAs, and zIIPs), select the processor assignment tab to display the processor assignment window. Each processor assignment 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 defined capacity weights and current weight. Workload manager (WLM) the current, minimum, and maximum processing weight.
   - The CPC’s settings for processor running time.
8. Use the controls to change the control settings of the logical partitions or the CPC, then proceed to indicate what you want to do with the new settings.
9. 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 processing weights of logical partitions that share central processors (and whether they are capped).
   - A logical partition to be workload managed with minimum and maximum weight values to set.
   - Defined capacity values for software pricing.
   - The CPC’s settings for processor running time.

Use the online Help for more information about changing logical partition controls.

Viewing logical partition cryptographic controls

You can use the support element workplace to start the task for viewing the cryptographic controls of each active logical partition on the central processor complex (CPC). Logical partition’s cryptographic controls are:

Control domain index numbers
This number identifies the cryptographic domains the logical partition uses for remote secure administration functions.

Usage domain index numbers
This number identifies the usage domains the logical partition uses for cryptographic functions.

Cryptographic Candidate List
These numbers identify which X2 coprocessor or X2 accelerator are assigned to the partition by the partition activation.

Cryptographic Online List
These numbers identify which X2 coprocessor or X2 accelerator were brought online at the partition activation.

Logical partition's initial cryptographic controls are established by the activation profile used to activate the logical partition. See "Getting ready to operate the system: customizing activation profiles" on page 5-1 for more information about customizing activation profiles for establishing a logical partition's initial cryptographic controls:

To review cryptographic settings:

1. The Crypto Express2 feature must be installed.
2. At least one activated logical partition must have at least one X2 coprocessor or X2 accelerator assigned to it.
3. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see "Establishing a support element console session from a Hardware Management Console" on page 1-2).
4. Open the **Task List** from the **Views** area.
5. Open **CPC Operational Customization** from the **Task List Work Area**.

   The CPC Operational Customization task list contains the **View LPAR Cryptographic Controls** task that you will start.
6. Open **Groups** from the **Views** area.
7. Locate any group that contains the CPC from the **Groups Work Area**.
8. Drag and drop the CPC on the **View LPAR Cryptographic Controls** task to start it.

   This displays the View LPAR Cryptographic Controls window. The window includes a tabbed window for each logical partition that can be activated on the CPC.

Use the online Help for more information about what its current setting means.

Setting the system time offset

The Logical partition system time offset provides for the optional specification of a fixed system time offset (specified in days, hours, and quarter hours) for each logical partition activation profile. The offset, if specified, will be applied to the time that a logical partition will receive from an External Time Source. This support can be used to address the following customer environment:

- *Multiple local time zones with a single sysplex timer (or sysplex timer network).*
  It is sometimes necessary to run multiple parallel sysplexes with different local time and run with the time set to GMT=LOCAL. This causes the results returned in the store clock (STCK) instruction to reflect local time. With logical partition system time offset support, logical partitions on each CPC in a Parallel Sysplex® that need to do this can specify an identical system time offset that will shift the ETR time in the logical partition sysplex members to the desired local time. Remaining logical partitions on the CPCs, as well as logical partitions on other CPCs or CPCs in basic mode, can continue to participate in current date production parallel sysplexes utilizing the sysplex timer(s) with the time provided by the External Time Source.

To customize the image profile for the system time offset:

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer user mode (see "Establishing a support element console session from a Hardware Management Console" on page 1-2).
2. Open an activation profile customized for activating a CPC.
3. Select **Logical partition system time offset** in the Clock type assignment box
4. Select the Time Offset from the window tree view to set the offset and to choose how you want it applied when the logical partition's clock is set.
5. Click **Save**.
6. Activate the CPC.

Use online Help to guide you through completion of this task.

Enabling I/O Priority Queuing

This task allows you to enable or disable I/O priority queuing for the system. Enabling the I/O priority queuing allows the system to specify a priority to be associated with an I/O request at start subchannel time. See "Enabling or disabling the global input/output (I/O) priority queuing" on page 5-14 to customize the reset profile for the CPC.

To enable or disable the I/O priority queuing:

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see "Establishing a support element console session from a Hardware Management Console" on page 1-2).
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 I/O Priority Queuing** 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: Enabling or disabling the input/output priority settings on a CPC can be considered disruptive. If the CPC is locked, unlock it. See "Setting object locking for disruptive tasks on an object" on page 2-18.
6. Drag and drop the CPC on the **Enable I/O Priority Queuing** task to start it.

This displays the Enable Input/Ouput (I/O) Priority Queuing window.

7. Select **Enable** to activate the I/O priority queuing or select the **Disable** to deactivate the I/O priority queuing.
8. Click **Save** to save the setting.

Use online Help to guide you through completion of this task.

Changing LPAR I/O Priority Queuing

This task allows you to review or change the minimum or maximum input/output (I/O) priority queuing value assignments of logical partitions. These values are passed on to the I/O subsystem for use when queuing decisions with multiple requests. You can dynamically (new settings take effect without customizing profiles or activating objects) change the minimum and maximum input/output (I/O) priority queuing values. See “Setting I/O priority queuing values” on page 5-27 to customize the activation profile for each logical partition.

To change LPAR I/O priority queuing:

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
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 I/O Priority Queuing** 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 the input/output priority settings on a CPC can be considered disruptive. If the CPC is locked, unlock it. See “Setting object locking for disruptive tasks on an object” on page 2-18.
6. Drag and drop the CPC on the **Change LPAR I/O Priority Queuing** task to start it.

   This displays the Change Logical Partition Input/Output (I/O) Priority Queuing window. The window lists the I/O priority queuing values for logical partitions defined by this IOCDS.
7. Use the window to dynamically change the minimum and maximum I/O priority queuing values.

   Note: If global input/output I/O priority queuing is **Enabled**, changes made for the minimum or maximum values will take effect immediately. If the global value is **Disabled**, changes will be saved by the system, but will not take effect until the global value is changed to **Enabled**.
8. Select a control to indicate what you want to do with the new setting.

Use online Help to guide you through completion of this task.

Chapter 9. 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 tasks you can use to get or change information that describes or defines the CPC configuration.

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. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer or service representative user role (see "Establishing a support element console session from a Hardware Management Console" on page 1-2).
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 the **CPC** group 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 click **Details**.

   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*, SB10-7037.
- 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*, SB10-7040.

Defining the I/O configuration using the stand-alone IOCP

You can use the support element workplace to start the support processor input/output configuration program (IOCP) available with the support element of the central processor complex (CPC).

To start the stand-alone IOCP:

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see "Establishing a support element console session from a Hardware Management Console" on page 1-2).
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 **Images** group from the **Group Work Area**.
6. Drag and drop the selected image 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 lists the input/output configuration data sets (IOCDSs) currently stored on the CPC's support element.

Determining PCHIDs assignments to channels

This task allows you to display the physical locations of all the installed and configured physical channels and the assigned physical channel identifier (PCHID) mapping. The CSS.CHPID associated with the PCHID and a description of the channel hardware type are displayed. The CSS.CHPID identifies the channel subsystem that the CHPID belongs to. You can view the front and back details of a specific cage. An action to write the view to a diskette allows you to print the cage view.

To view the channel to PCHID assignments:

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
2. The central processor complex (CPC) must be power-on reset.
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 **Channel to PCHID assignment** task that you will start.
5. Open **Groups** from the **Views** area.
6. Open the **CPC** group from the **Groups Work Area**.
7. Drag and drop the CPC on the **Channel to PCHID assignment** task to start it.

   The Channel to PCHID assignment window displays.
8. Use the **Options** or **Search** menu bar to perform tasks.

From the **View** menu bar on the Channel to PCHID assignment window, you can:
- Sort by Channel Location
- Sort by Cage and PCHID Number
- Sort by Card Type and PCHID Number
- Sort by Book-Jack-MBA
- Sort by Channel State
- Sort by PCHID Number
- Sort by Configured CSS.CHPIDs
- View Cage Details

From the **Search** menu bar on the Channel to PCHID assignment window, you can:
- SEARCH PCHID
- SEARCH CSS.CHPID

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.

Preparing Enhanced Book Availability

Use this option to prepare your system for Enhanced Book Availability on a targeted book. This option is a prerequisite to the Perform Enhanced Book Availability option and will determine the readiness of the system for the targeted book. The configured processors and the in-use memory will be evaluated for the evacuation from the targeted book to the unused resources available on the remaining books within the system configuration.

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
2. Open the **Task List** from the **Views** area.
3. Open **Groups** from the **Views** area.
4. Open the **CPC** group from the **Groups Work Area**.
5. Open **CPC Configuration** from the **Task List Work Area**.

   The CPC Configuration task list contains the **Perform Model Conversion** task that you will start.
6. Drag and drop the CPC on the **Perform Model Conversion** task to start it.

   The Model Conversion window displays.
7. Select **Hardware upgrades**.
8. Select **Prepare for Enhanced Book Availability** from the list.

Use the online Help for more information about the display fields and list.

Performing Enhanced Book Availability

Use this option to concurrently perform the Enhanced Book Availability on the targeted book that was previously prepared. This option allows for the evacuation of system resources from the targeted book, removal of the book, removal of memory hardware, addition of new memory hardware, reinstallation of the targeted book, and finally the restoration of the targeted book into the system configuration.

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
2. Open the **Task List** from the **Views** area.
3. Open **Groups** from the **Views** area.
4. Open the **CPC** group from the **Groups Work Area**.
5. Open **CPC Configuration** from the **Task List Work Area**.

   The CPC Configuration task list contains the **Perform Model Conversion** task that you will start.
6. Drag and drop the CPC on the **Perform Model Conversion** task to start it.

   The Model Conversion window displays.
7. Select **Hardware upgrades**.
8. Select **Perform Enhanced Book Availability** from the list.

Use the online Help for more information about the display fields and list.

Displaying Previous Prepare Enhanced Book Availability Results

Use this option to view the results from the last execution of the Prepare for Enhanced Book Availability.

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
2. Open the **Task List** from the **Views** area.
3. Open **Groups** from the **Views** area.
4. Open the **CPC** group from the **Groups Work Area**.
5. Open **CPC Configuration** from the **Task List Work Area**.

   The CPC Configuration task list contains the **Perform Model Conversion** task that you will start.
6. Drag and drop the CPC on the **Perform Model Conversion** task to start it.

   The Model Conversion window displays.
7. Select **Hardware upgrades**.
8. Select **Display Previous Prepare Enhanced Book Availability Results** from the list.

Use the online Help for more information about the display fields and list.

Testing Capacity Backup feature using password panel

The Capacity Backup (CBU) feature provides the ability to temporarily increment the capacity of your processors, using Licensed Internal Code (LIC), in the event of an unforeseen loss of substantial server computing capacity at one or more of your eligible site. CBU can concurrently add CPs, ICFs, IFLs, IFAs, and zIIPs to an existing configuration when other servers are experiencing unplanned outages. This ability is provided under a special IBM contract called the ″IBM Customer Agreement Attachment for Capacity Backup Upgrade.″ For more information on the CBU feature, see the*Capacity on Demand User's Guide*.

CBU is offered with the System z9 EC and z9 BC to provide reserved emergency backup processor capacity for unplanned situations where you lost capacity in another part of your enterprise and want to recover by adding the reserved capacity on a designated System z9 EC and z9 BC.

CBU is the quick, *temporary* activation of Central Processors (CPs), for up to 90 days, when you lose processing capacity due to an emergency or disaster/recovery situation.

The Test Capacity Backup feature is only a test and is not to be used for a temporary upgrade. The test can be active for up to 10 days and can be undone any time during that time. This is counted as one test being used.

Note: If you are not sure of your CBU status, see“Viewing the CBU feature information” on page 9-10

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
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 **Perform Model Conversion** 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 **Perform Model Conversion** task to start it.

   The Model Conversion window displays.
7. Select **Capacity Backup (CBU)** from the list
8. Select **Test Capacity Backup feature using password panel** if your system has the CBU feature enabled and you want to test the CBU feature.
9. Click **Continue**.
10. Write down the **PU Serial Number** and **PU Detailed DATA** from the **Capacity Backup (CBU) Activation Authorization** panel. You must contact IBM for the correct password based on the Processing Unit data displayed. There are five 10 day tests allowed per CBU feature prior to executing a REAL CBU upgrade. Consult your contract with IBM or contact your IBM account representative to determine the number of test allowed each year and when you will be billed for activations.

If you get a message **The requested upgrade failed due to missing or invalid CBU data**, the CBU feature is not installed.

Use the online Help for more information about the display fields and list.

Testing the Capacity Backup feature using IBM service support system

The Test Capacity Backup feature is only a test and is not to be used for a temporary upgrade. The test can be active for up to 10 days and can be undone any time during that time. This is counted as one test being used.

Note: If you are not sure of your CBU status, see“Viewing the CBU feature information” on page 9-10

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
2. Verify Capacity Backup is enabled. See “Enabling Capacity Backup Services” on page A-12.
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 **Perform Model Conversion** task that you will start.
5. Open **Groups** from the **Views** area.
6. Open the **CPC** group from the **Groups Work Area**.
7. Drag and drop the CPC on the **Perform Model Conversion** task to start it.

   The Model Conversion window displays.
8. Select **Capacity Backup (CBU)** from the list

9. Select **Test Capacity Backup feature using IBM Service Support System** if your system has the CBU feature enabled and you want to test the CBU feature.

   Note: Once this option is selected an automatic validation is executed for authorization to activate the CBU feature. There are five 10 day tests allowed per CBU feature prior to executing a REAL CBU upgrade. Consult your contract with IBM or contact your IBM account representative to determine the number of test allowed each year and when you will be billed for activations.

Use the online Help for more information about the display fields and list.

Activating the Capacity Backup feature using password panel

Use this task if your system has the CBU feature enabled and you want a fast temporary upgrade activation.

Note: If you are not sure of your CBU status, see"Viewing the CBU feature information" on page 9-10

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see "Establishing a support element console session from a Hardware Management Console" on page 1-2).
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 **Perform Model Conversion** 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 **Perform Model Conversion** task to start it.

   The Model Conversion window displays.
7. Select **Capacity Backup (CBU)** from the list
8. Select **Activate Capacity Backup feature using password panel** if your system has the CBU feature enabled and you want to test the CBU feature.
9. Click **Continue**.
10. Write down the **PU Serial Number** and **PU Detailed DATA** from the **Capacity Backup (CBU) Activation Authorization** panel. You must contact IBM for the correct password based on the Processing Unit data displayed. After three unsuccessful attempts to enter the password, the CBU feature will no longer be available to the system. You must contact IBM for a new CBU record and its password. The activation will be in effect for 90 days starting with the data of the activation.

If you get a message **The requested upgrade failed due to missing or invalid CBU data**, the CBU feature is not installed.

Use the online Help for more information about the display fields and list.

Activating the Capacity Backup feature using IBM Service Support System

Use this task if you want to activate a real, 90-day Disaster Temporary Upgrade using the CBU feature using the IBM Service Support System (RETAIN).

Note: If you are not sure of your CBU status, see"Viewing the CBU feature information" on page 9-10

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see "Establishing a support element console session from a Hardware Management Console" on page 1-2).
2. Verify Capacity Backup is enabled. See "Enabling Capacity Backup Services" on page A-12.
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 **Perform Model Conversion** task that you will start.
5. Open **Groups** from the **Views** area.
6. Open the **CPC** group from the **Groups Work Area**.
7. Drag and drop the CPC on the **Perform Model Conversion** task to start it.

   The Model Conversion window displays.
8. Select **Capacity Backup (CBU)** from the list
9. Select **Activate Capacity Backup feature using IBM Service Support System** if your system has the CBU feature enabled and you want to test the CBU feature.

   Note: Once this option is selected an automatic validation is executed for authorization to activate the CBU feature. There are five 10 day tests allowed per CBU feature prior to executing a REAL CBU upgrade. Consult your contract with IBM or contact your IBM account representative to determine the number of test allowed each year and when you will be billed for activations.

Use the online Help for more information about the display fields and list.

Deactivation of the CBU configuration prior to expiration date

The **Undo Temporary Upgrade** restores the original system configuration. When you have activated the Capacity Backup (CBU) feature, the **Undo Temporary Upgrade** will end the CBU and return the system to its original base model. When you have activated either **Activate Capacity Backup feature using password panel** (90-day CBU) or **Activate Capacity Backup using IBM Service Support System** (90-day CBU), the CBU feature will no longer be available to the system after the **Undo Temporary Upgrade**. Now you must contact IBM for a new CBU record.

To do an Undo Temporary Upgrade:

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
2. Open the **Task List** from the **Views** area.
3. Open **Groups** from the **Views** area.
4. Open the **CPC** group from the **Groups Work Area**.
5. Open **CPC Configuration** from the **Task List Work Area**.

   The CPC Configuration task list contains the **Perform Model Conversion** task that you will start.
6. Drag and drop the CPC on the **Perform Model Conversion** task to start it.

   The Model Conversion window displays.
7. Select **Undo Temporary Upgrade**.
8. Follow the directions on the screen until **Completed** displays. Please read all messages thoroughly.
9. Open the **Daily** tasks list from the **Task List Work Area**.

   The Daily task list contains the **Activate** task that you will start.
10. Drag and drop the CPC on the **Activate** task to start it.

    Verify the correct Activation Profile is being used.
11. Right click on the CPC and select CP from the pop-up menu and verify that the correct number of CPs are defined.
12. Create another good BACKUP CRITICAL DATA on the Hardware Management Console.

    Use the online Help for more information about the display fields and list.

Deactivation on Expiration Date

The CBU function is enabled with a built in 90 day expiration time period. When the machine nears the expiration date:

- Warning messages start five days prior to the expiration date.
- Warning messages will appear on the Hardware Management Console and Support Element.
- Warning messages will continue for two days after expiration date. At this point the machine will **call home** to alert IBM service.
- If no action is taken to perform a normal deactivation, the following occurs:
  - At this point the microcode will automatically degrade the performance of each CP to approximately 10-20% of the present CBU model. This is a concurrent action that keeps the machine operating, but at the slower performance value.
  - This is an immediate operation (see “Restore Machine to Original Model after Automatic Deactivation”).
  - Reactivation of the CBU configuration is not possible. To reactivate, you must obtain a new CBU record from IBM via a reordable feature code.

Restore Machine to Original Model after Automatic Deactivation

To restore the machine to the original model after the automatic deactivation, perform the normal deactivate prior to expiration date procedure. See “Deactivation of the CBU configuration prior to expiration date” on page 9-8

Viewing the CBU feature information

You can use this task to view the status of either your activated CBU feature upgrade or a test of CBU upgrade. Depending on whether you have activated or tested an upgrade, the information displayed indicates:

- If the CBU is installed on your system
- If the CBU is activated for testing
- The date the CBU was activated
- The date the CBU will expire
- How many CBU tests are remaining.
- Whether the activated CBU is a TEST CBU or UPGRADE CBU
- If the system is enabled for CBU
- Additional resources for installing the CBU feature.

To view the CBU information:

1. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, access administrator, or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
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 CBU feature information** 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 **View Capacity Backup feature information** task to start it.

   The View Capacity Backup feature information Confirmation window displays.
7. Click **Continue** to view the status of the CBU feature data.

   Use the online Help for more information about viewing CBU feature information.

Customer Initiated Upgrade (CIU)

Customer Initiated Upgrade (CIU) gives you the capability to initiate a processor upgrade using the Resource Link™ web site at: *www.ibm.com/servers/resourcelink*. The CIU feature allows concurrent upgrades for processors (CPs, IFLs, ICFs, and IFAs) and memory dynamically and non-disruptively.

The Resource Link Web site produces the interface that allows you to order a dynamic CIU upgrade order for your server. Using this interface you can create, cancel, and view the CIU upgrade order. You can also view the history of orders that were placed through this interface. To retrieve and apply your CIU, you will need a registered user ID. For more information, see the *Capacity on Demand User’s Guide*

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).

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 **Perform Model Conversion** 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 **Perform Model Conversion** task to start it.

   The Model Conversion window displays.
7. Select **Customer Initiated Upgrade (CIU)**.
8. Select the option you want from the list to retrieve and apply customer initiated upgrades.

Viewing the On/Off Capacity on Demand (On/Off CoD) feature information

The On/Off Capacity on Demand (On/Off CoD) feature is used to temporarily increase CPs and IFLs concurrently and non-disruptively. You can use this task to view the current state of the Customer Initiated Upgrade (CIU) and the current activation data of the installed On/Off CoD feature.

To view the On/Off CoD feature information:

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
2. Open the **Task List** from the **Views** area.
3. Open the **CPC Configuration** from the **Task List Work Area**.

   The CPC Configuration task list contains the **View On/Off CoD feature information** 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 **View On/Off CoD feature information** task to start it.

   The View On/Off CoD feature information window displays.

   Use the online Help for more information about viewing On/Off CoD feature information.

Time Synchronization features

A *Sysplex Timer* is a device that provides a times source to the time-of-day (TOD) clocks of Central Processor Complexes (CPCs) attached to it and the operating systems or control programs running on that server (CPC). A feature called an *External Timer Reference (ETR)* installed in the CPC provides two ETR attachment facility (EAF) ports for attaching Sysplex Timers. Both ports may attach the same Sysplex Timer, or each port may attach a separate Sysplex Timer when configured with 9037 Expanded Availability.

An ETR network consists of one Sysplex Timer or coupled Sysplex Timers (Expanded Availability), and the links from this source to the system. Each system has two ETR attachment facility (EAF) ports which can be connected by a link to the Sysplex Timer.

Server Time Protocol (STP) is a time synchronization architecture designed to provide the capability for multiple servers (CPCs) to maintain time synchronization with each other and to form a Coordinated Timing Network (CTN). STP is designed for servers (CPCs) that have been configured to be in a Parallel Sysplex or a sysplex (without a Coupling Facility), as well as servers (CPCs) that are not in a sysplex, but need to be time synchronized. STP is designed as a message-based protocol allowing timekeeping information to be sent between servers (CPCs) and Coupling Facilities (CFs) over InterSystem Channel-3 (ISC-3) links configured in peer mode, Integrated Cluster Bus-3 (ICB-3) links, or Integrated Cluster Bus-4 (ICB-4) links.

There are two types of CTNs supported by STP:

1. *Mixed CTN* is a timing network that contains a collection of servers and has at least one STP-configured server stepping to timing signals provided by the Sysplex Timer. The CTN ID must be a valid STP network ID and the ETR network ID must be in the range of 0 to 31.
2. *STP-only CTN* is a timing network that contains a collection of servers configured to be in STP timing mode. None of the servers in an STP-only CTN can be in ETR timing mode.

The feature(s) you have installed on the server (CPC) determines what options are available for the System (Sysplex) Time task.

- If only the ETR cards are installed, the System (Sysplex) Time window displays the current configuration and the status of the ETR Attachment Facility (EAF) ports that allow you to synchronize to the Sysplex Timers for your Central Complex (CPC). The following available tab options are:
  - ETR Configuration
  - ETR Status.
- If both the ETR features are installed and the Server Time Protocol (STP) feature enabled, the System (Sysplex) Time window displays the following available tab options:
  - Timing Network
  - Network Configuration
  - ETR Configuration
  - ETR Status
  - STP Configuration
  - STP Status.
- If only the Server Time Protocol (STP) feature is installed, the System (Sysplex) Time window displays the following available tab options:
  - Timing Network
  - Network Configuration
  - STP Configuration
  - STP Status.

Use the online help if you need additional information about the **System (Sysplex) Time** task. You can also go to Resource Link, *http:/www.ibm.com/servers/*

resourcelink click **Education** in the Navigation bar, under **System z9** click **z9 EC (formerly z9-109)**, and select **Introduction to Server Time Protocol (STP)**.

Setting up time synchronization

Use the System (Sysplex) Time task to setup time synchronization for a server (CPC) using the Sysplex Timer and/or the Server Time Protocol (STP).

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user mode (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
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 **System (Sysplex) Time** 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 **System (Sysplex) Time** task to start it.

   The System (Sysplex) Time window displays. Depending on the features you have installed and enabled, use the appropriate tabs that appear at the top of the window:

Use the online help if you need additional information about the **System (Sysplex) Time** task. You can also go to Resource Link, *http:/www.ibm.com/servers/resourcelink* click **Education** in the Navigation bar, under **System z9** click **z9 EC (formerly z9-109)**, and select **Introduction to Server Time Protocol (STP)**.

Timing Network

The Timing Network window displays the overall timing information for the ETR network or Coordinated Timing Network (CTN) including the current date and time, local offsets, and general network information. The information displayed is identical on each server in the same ETR network or CTN.

In an STP-only CTN adjustments can be made for the management of time, leap seconds, and time zones. These adjustments are available on every server in the STP-only CTN but are only enabled on the Current Time Server to ensure all time and offset adjustments are done at the server providing time information to all members of the STP-only CTN. Any changes that are made are sent to the Current Timer Server (CPC) or the CPC being set up to be the Current Time Server. From there they are distributed throughout the timing network. Depending on the state of the coordinated timing network and the role of the server (CPC) in the Coordinated Timing Network (CTN) the following adjustments can be made:

- **Adjustment Steering...** allows you to view detailed steering information for an entire STP-only CTN that indicates the amount of time the clock needs to be adjusted. Each server (CPC) is gradually adjusting its clock by steering towards the new Coordinated Server Time (CST).

  Adjustment steering could be the result of the following:

  – Setting the time manually on the console

  - Dialing out to the External Time Source via the Hardware Management Console
  - Migrating from an STP-only CTN to a Mixed CTN.
- **Adjust Time...** allows you to make a slight adjustment to current Coordinated Server Time (CST). Clicking **Access External Time Source** allows you to get the adjustment amount fron an external time source (if one is set up) or manually enter an amount.

  Note: The External Time Source (ETS) is set by using the **Customize Outbound Connectivity** task on the hardware management console, then selecting the **External Time Source** tab. You can set up the modem to dial an ETS for CPCs that are participating in an STP-only CTN.
- **Adjust Leap Seconds...** allows you to display or change the current leap seconds to a new leap second offset and when that adjustment should happen.
- **Adjust Time Zone...**allows you to display or change the current time zone and daylight saving time. Clicking **Define...** allows you to set up a time zone not found in the list of time zones.

Network Configuration

The Network Configuration window allows you to manage or view the STP-only CTN configuration and any configuration in progress including migration from an STP-only CTN to a Mixed CTN. The changes are sent to the Current Time Server (CPC) or the CPC being set up to be the Current Time Server. The changes are then distributed throughout the network. The Network Configuration window allows you to:

- **Initialize Time...** to set up initial time values (leap second offset, time zone, or date and time) for a CPC that will act as the Current Time Server for a CTN.
- **Deconfigure** to deconfigure the Preferred Time Server, Backup Time Server, and Arbiter.

  Note: This action is extremely disruptive and should only be done in order to shut down your STP-only CTN.
- **Cancel Migration to Mixed CTN** if you decide not to proceed with the migration of an STP-only CTN to a Mixed CTN.

ETR Configuration

If ETR features are installed on your server (CPC), the ETR Configuration window allows you to set the configuration for the ETR attachment facility (EAF) ports to synchronize your Sysplex Timer. Configuration changes made only affect this particular server (CPC). They are not applied to an entire timing network. The ETR Configuration window allows you to:

- Set the configuration for the ETR Attachment Facility (EAF) ports to synchronize your Central Processor Complex (CPC) to your Sysplex Timer.
- Configure your CPC to participate in a Mixed CTN by specifying an ETR network ID.
- Migrate your CPC from a Mixed CTN to an STP-only CTN by removing the ETR network ID.
- Remove the ETR network ID to no longer be part of an ETR network or Mixed CTN.

ETR Status

If the ETR cards are installed on your server (CPC), the ETR Status window displays the configuration and operational state of the ETR connections as viewed

by the server (CPC). Any modifications that need to be done to the ETR configuration, such as setting the ETR network ID and ETR Unit IDs must be done using the Sysplex Timer console.

STP Configuration

The STP Configuration window allows you to do the following:

- Configure this server (CPC) or remove it from participating in a Mixed CTN.
- Configure this server (CPC) or remove it from participating in an STP-only CTN

Configuration changes made only affect this particular CPC. They are no applied to an entire timing network.

Note: When a CPC does not have the ETR feature installed, a decimal number from 0 to 31 can be specified in the ETR network ID portion of the CTN ID so that the CPC can participate in a Mixed CTN.

STP Status

The STP Status window displays the following STP status information for a specific CPC:

- *Timing state* indicates the timing state the CPC is operating in. If it has a value of anything other than Synchronized then the server is not actively participating in an ETR network or CTN.
- *Usable clock source* indicates whether a usable STP-clock source is available in order to synchronize the server TOD.
- *Timing mode* indicates the timing mode of your server (CPC) within the ETR network or CTN.
- *Stratum level* indicates the hierarchy of this server within the timing network. A stratum level of 0 indicates the server has no time source.
- *Maximum timing stratum level* indicates how far a CPC can be from the active Stratum 1 and still be in a synchronized state
- *Active STP* indicates the level of STP facility code currently active on the server (CPC).
- *System Information* identifies the CPCs that are directly attached to the CPC for STP purposes. The CPC's coupling links that are initialized to transport STP messages are listed using the PCHID addresses and are grouped according to the system that is directly attached to the links. Additionally, the stratum level, active STP version, and maximum STP version for each directly attached system is shown.
- *Local Uninitialized STP links* identifies the possible coupling links defined in the IODF that may be used by this server to exchange STP messages.

The Crypto Express2 Feature

The Crypto Express2 Feature is an orderable feature.

- The Crypto Express2 Feature works with the Integrated Cryptographic Service Facility (ICSF) and the IBM Resource Access Control Facility (RACF®) (or equivalent software products) in an z/OS or OS/390 operating environment to provide data privacy, data integrity, cryptographic key installation and generation, electronic cryptographic key distribution, and personal identification number (PIN) processing. The Crypto Express2 Feature is 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.

- The Crypto Express2 Feature works with the Integrated Cryptographic Service Facility (ICSF) in an z/OS or OS/390 operating environment to provide support for RSA (PK) cryptographic operations. The Crypto Express2 Feature is used 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.

Working with the Crypto Express2 feature

Use the support element to monitor the X2 coprocessors and X2 accelerators by loading their configuration data during CPC activation.

To work with the Crypto Express2 feature:

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
2. The Crypto Express2 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 Configuration** task that you will start.
5. Open **Groups** from the **Views** area.
6. Open the **CPC** group from the **Groups Work Area**.
7. Drag and drop the CPC on the **Cryptographic Configuration** task to start it.

The Cryptographic Configuration window lists the X2 coprocessors and X2 accelerators installed in the CPC and provides controls for working with them.

Configuring and monitoring the Crypto Express2 feature

Upon completing the configuration and initialization of the Crypto Express2 feature, you can monitor and manage it by:

- Checking the status of the X2 coprocessors or X2 accelerators.
- Testing the random number (RN) generators of the X2 coprocessors.
- Zeroizing the X2 coprocessors.
- Indicate whether you want TKE commands permitted for the X2 coprocessors.
- Import and activate a UDX for any X2 coprocessor installed in your system.
- Select a crypto configuration type for your system.

Checking status for the Crypto Express2 feature

You can use the support element workplace to monitor the status of the Crypto Express2.

To check the status of the Crypto Express2 feature:

1. Start the **Cryptographic Configuration** task for working with X2 coprocessors and X2 accelerators. For instructions, see “Working with the Crypto Express2 feature”

The Cryptographic Configuration window lists the X2 coprocessors and X2 accelerators installed in the CPC and provides controls for working with them.

Note: The Crypto Express2 has completed its initialization when the status indicates *Configured*. After initialization is complete, you need to refresh the Cryptographic Configuration window. If initialization is ongoing, you may need to refresh the Cryptographic Configuration window to see the current status until *Configured* is indicated.

2. Select from the list the X2 coprocessors or X2 accelerators that you want more information for.
3. Click **View Details**.

   The Cryptographic Details window displays information on the selected X2 coprocessors or X2 accelerator.

Testing the RN generator

Each X2 coprocessor includes a random number (RN) that may be used as a key for encryption. Testing a RN generator verifies whether the numbers it generates are sufficiently random.

Ordinarily, a RN generator is tested automatically when it is initialized. But you can use the support element workplace at any time to manually test a RN generator.

You can select to run a RN generator test on individually selected X2 coprocessors or run a test on all X2 coprocessors.

To test a X2 coprocessor's RN generator:

1. A power-on reset of the CPC must be complete.
2. The X2 coprocessor must be online and assigned to a logical partition.
3. Log onto the support element in the system programmer or service representative user mode.
4. Start the **Cryptographic Configuration** task for working with X2 coprocessors. For instructions, see "Working with the Crypto Express2 feature" on page 9-16

   The Cryptographic Configuration window lists the X2 coprocessors and X2 accelerators installed in the CPC, and provides push buttons for working with them.

   To manually test a specific X2 coprocessor:

   - Select from the list a configured X2 coprocessor that you want to test.
   - Click **Test RN Generator** to test it.

     A message is displayed to indicate the results of the test.

   To manually run the test on **all** X2 coprocessors:

   - Click **Test RN Generator on All X Coprocessors** to test it.

     A message is displayed to indicate the results of the test.

Zeroizing X2 coprocessors manually

Zeroizing a X2 coprocessor clears all configuration data and cryptographic keys by resetting them to binary zeroes.

Attention: Zeroizing one or all X2 coprocessor clears its configuration data and clears all cryptographic keys. Zeroizing all also erases configuration data from the support element hard drive (for example, UDX files). X2 coprocessors should be zeroized manually only when absolutely necessary, typically when X2 coprocessors configuration data must be erased completely.

For example:

- You must zeroize X2 coprocessors prior to selling or transferring ownership of the CPC.
- A service representative may zeroize X2 coprocessors prior to upgrading the CPC, if required.
- You may want to zeroize X2 coprocessors if, in an emergency, it is the only way to maintain the security of encrypted data.

To manually zeroize X2 coprocessors:

1. A power-on reset of the CPC must be complete.
2. The X2 coprocessor must be online and assigned to a logical partition.
3. Start the **Cryptographic Configuration** task for working with X2 coprocessors. For instructions, see “Working with the Crypto Express2 feature” on page 9-16

   This displays the Cryptographic Configuration window. The window lists the X2 coprocessors and X2 accelerators installed in the CPC, and provides controls for working with them.

   To manually zeroize a specific X2 coprocessors:

   - Select from the list the configured X2 coprocessor you want to zeroize.
   - Click **Zeroize** to zeroize the selected X2 coprocessor.

     A Zeroize Warning window is displayed to notify you of the consequences for clearing the configuration data.
   - Click **Zeroize** to confirm your request to zeroize the selected X2 coprocessor.

   To manually run zeroize on all X2 coprocessors:

   - Click **Zeroize All X Coprocessors** to zeroize all the X2 coprocessors and erase configuration data from the support element hard drive.

     A Zeroize Warning window is displayed to notify you of the consequences for zeroizing all the X2 coprocessors.
   - Click **Zeroize All** to confirm your request to zeroize them.

   A message is displayed to indicate the results of the function.

Changing permission for TKE commands

The TKE workstation can manage secure functions of a specific Crypto Express2 feature only if permission is given. If permission is denied, all requests for information or commands to a specific X2 coprocessor from the TKE workstation will not be allowed. You can use the support element to dynamically permit or deny TKE commands to the X2 coprocessor from the TKE workstation.

To permit or deny TKE commands:

1. A power-on reset of the CPC must be complete.
2. The X2 coprocessor must be online and assigned to a logical partition.
3. Start the **Cryptographic Configuration** task for working with X2 coprocessors. For instructions, see “Working with the Crypto Express2 feature” on page 9-16

   The Cryptographic Configuration window lists the X2 coprocessors and X2 accelerators installed in the CPC and provides controls for working with them.
4. Select from the list the X2 coprocessors that you want to view or modify TKE command permission.
5. Click **TKE Commands**.

   The TKE Commands Configuration window displays information on the TKE commands for the selected X2 coprocessors.

6. Locate the Permit TKE Commands check box. Then either:
   - Mark the check box to permit TKE commands. The check box displays a check mark when you mark it.
   - Or unmark the check box to deny TKE commands. The check box becomes empty when you unmark it.
   - Click **OK** to change the permission.

   Use the online Help for more information on TKE commands configuration.

Selecting a crypto type configuration

The Crypto Express2 feature can be configured to run as a X2 coprocessor or X2 accelerator. The Crypto Express2 must be deconfigured prior to changing the crypto configuration type. If you select **Accelerator**, you can zeroize the selected X2 coprocessor by indicating **Zeroize the Coprocessor** on the Crypto Type Configuration window.

To select a crypto type configuration:

1. A power-on reset of the CPC must be complete.
2. The X2 coprocessor or X2 accelerator must be online and assigned to a logical partition.
3. Start the **Cryptographic Configuration** task for working with X2 coprocessors and X2 accelerators. For instructions, see “Working with the Crypto Express2 feature” on page 9-16

   The Cryptographic Configuration window lists the X2 coprocessors and X2 accelerators installed in the CPC and provides controls for working with them.
4. Select from the list the X2 coprocessors or X2 accelerator that you want to change the crypto type configuration.
5. Click **Crypto Type Configuration**.

   The Crypto Type Configuration window displays information on the selected Crypto Express2.
6. Select a crypto type configuration for the Crypto Express2.
7. Zeroize the X2 coprocessor when selecting an X2 accelerator crypto type.
8. Click **OK** to change the crypto type configuration.

Use the online Help for more information on crypto type configuration.

Configuring the User Defined Extensions (UDX)

The UDX allows you to add customized operations to the X2 coprocessor installed. The UDX provides the capability to develop your own UDX Segment 3 image file and load your custom Segment 3 image file onto one or more X2 coprocessors. To view the Segment 3 details, click **View Details** on the Cryptographic Configuration window. The Segment 3 image file is built and loaded onto a DVD-RAM using a Windows NT workstation. For more information on building a UDX Segment 3 image file go to the following Web site at:

- *http://www.ibm.com/security/cryptocards*
- Click on **Library** on the navigation bar.

To configure for User Defined Extension (UDX):

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
2. The Crypto Express2 feature must be installed, and the CPC must be power-on reset to activate the UDX. Otherwise, to import a UDX file:
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 Configuration** task that you will start.
5. Open **Groups** from the **Views** area.
6. Open the **CPC** group from the **Groups Work Area**.
7. Drag and drop the CPC on the**Cryptographic Configuration** task to start it.

   The Cryptographic Configuration window lists the X2 coprocessor and X2 accelerators installed in the CPC and provides controls for working with them.
8. Click **UDX Configuration** to configure the X2 coprocessors for UDX.

   The UDX Configuration window displays detailed information for the X2 coprocessor configured for UDX capability and provides controls for working with them.
9. Insert the UDX DVD-RAM into the hardware management console diskette drive.
10. Click **Import** to import the UDX file from the DVD-RAM to the support element hard drive.

    The Import window displays.
11. Click **OK**.
12. Click **Activate** to load the UDX data to the X2 coprocessor.

Use the online Help for more information on UDX configuration.

Releasing a X2 Coprocessor or X2 Accelerator

If a Crypto Express2 card is removed from the system, this task allows you to break the association of the cryptographic number and the card serial number. This is necessary because the cryptographic number assigned to that card continues to be associated with the card’s serial number, unless the card is released, preventing reuse of the cryptographic number.

This task also allows you to view X2 coprocessor and X2 accelerator configuration of:

- All installed cards with their X2 coprocessor and X2 accelerator assignment, crypto number, card location, and PCHID.
- All fenced cards.

To release a cryptographic number from the card serial number:

1. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer,

access administrator, or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).

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 **Cryptographic 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 **Cryptographic Management** task to start it.

   The Cryptographic Management window list the cryptographic number assignments in the current system configuration.
7. Select the cryptographic number to be released from the card serial number list.
8. Click **Release**.

   The Cryptographic Management window confirms the cryptographic number you selected to be released.
9. Click **Confirm**.

   A message is displayed to indicate the release was successful.

Releasing NPIV port names

N_Port Identifier Virtualization (NPIV) for Fibre Channel Protocol (FCP) channels allows sharing of a single physical FCP channel among operating system images. Use this task to:

- Display all N_Port Identifier Virtualization (NPIV) port names that are currently assigned to FCP subchannels.
- Release all port names that had previously been assigned to FCP subchannels and are now locked
- Release a subset of the port names that had previously been assigned to FCP subchannels and are now locked.

To enable the NPIV mode for selected channel paths see “Enabling NPIV mode” on page 13-6.

To release NPIV port names:

1. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
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 **NPIV - Config** 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 **NPIV - Config** task to start it.

   The FCP Channel - FCP NPIV Port Names window displays.

Use the Online Help for more information on releasing a NPIV port name.

Chapter 10. 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.

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 a DVD-RAM 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. Mirror data from the primary support element to the alternate support element.
6. Operate the system to determine whether it is operating correctly and satisfactorily with the new internal code changes.
7. **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. See"Defining clonable internal code levels" on page 10-18 for more information on distributing internal code levels to multiple systems. 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.

The operations that can be scheduled on the support element are:

Accept internal code changes
: Schedules an operation to make activated internal code changes a permanent working part of the licensed internal code of the selected CPC.

Activate
: Makes the installed code changes operational in place of their corresponding licensed internal code. Activating the changes does not permanently modify the internal code and they may be removed until the time that they are accepted. Activating internal code changes that are not concurrent may cause the support element(s) to reload its licensed internal code without warning. If no licensed internal code changes are installed, the CPC will be activated with the current licensed internal code.

Deactivate
: Stops the operating system, deallocates resources, clears associated hardware and powers off the CPC.

Install internal code changes/Activate
: Schedules an operation for installing and activating internal code changes retrieved for the selected CPCs.

Remove internal code changes/Activate
: Schedules an operation for removing and activating internal code changed installed for the selected CPCs.

Retrieve internal code changes
Schedules an operation to copy internal code changes from a remote service support system to the support element hard disk.

Access external time source
Schedules an operation to obtain data from an external time source for the purpose of synchronizing the time of the selected servers (CPCs) that are participating in a Server Time Protocol (STP) Coordinated Timing Network (CTN).

Transmit system availability data
Sends service data generated by the selected object to IBM. This data is used to ensure a high level of availability.

To schedule operations for managing internal code changes:

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
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 **Customize 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 **Customize Scheduled Operations** task to start it.

   This opens the Customize Scheduled Operations window. It provides controls for scheduling operations.
7. After you start the task, request help for the controls or the window for additional information about using them to schedule operations for managing internal code changes.

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.

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. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see "Establishing a support element console session from a Hardware Management Console" on page 1-2).
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 object locking for disruptive tasks on an object" on page 2-18.
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.
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 click **OK** 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.

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. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user mode (see “Establishing a support element console session from a Hardware Management Console” on page 1-2). 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 10-5.

   This opens the Change Internal Code window. It lists a radio button for each task available for working with internal code changes.
3. Select **Accept installed changes that were activated** from the list, then click **OK**.

   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 click **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 click **Accept** to begin the process of accepting all installed changes that were activated.
6. Wait until a message indicates the process is complete.

   Click **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.

At least one of the following sources will be available to you for retrieving internal code changes:

Retrieve code changes from DVD-RAM to the support element
: Select this source when IBM has delivered the internal code changes to you on a DVD-RAM.

Retrieve code changes from the IBM support system to the support element
: Select this source when IBM has notified you that the new internal code changes are available through the IBM Service Support System, and if the support element is configured and enabled for communicating with it.

Retrieve code changes from FTP site to the support element
: Select this source to copy internal code changes from an FTP site to the support element.

To retrieve internal code changes:

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
2. Start the task for working with internal code changes. For instructions, see “Starting a task for changing internal code” on page 10-5.

   This opens the Change Internal Code window. It lists a radio button for each task available for working with internal code changes.
3. Select **Retrieve internal code changes** from the list, then click **OK**.

   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 click **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 click **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.

   Click **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.

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.

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. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see "Establishing a support element console session from a Hardware Management Console" on page 1-2).
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 10-5.

   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 click **OK**.
5. Select the radio button that describes the operation and internal code changes for which you want dependencies checked, then click **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, click **OK** to close the window.

Use the online Help for more information for any radio button and the operation it describes and the dependency checking it performs.

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. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2). 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 10-5.

   This opens the Change Internal Code window. It lists a radio button for each task available for working with internal code changes.
3. Select **Install and activate changes that were retrieved** from the list, then click **OK**.

   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 click **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 window to select the type of changes you want to install and activate, then click **Install and activate** 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.

   Click **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. This makes the previous change levels operational. 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. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user mode (see “Establishing a support element console session from a Hardware Management Console” on page 1-2). 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 10-5.

   This opens the Change Internal Code window. It lists a radio button for each task available for working with internal code changes.
3. Select **Remove and activate changes** from the list, then click **OK**.

   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 click **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 window to select the type of changes you want to remove and activate, then click **Remove and activate** to continue.
6. Review the information on the confirmation window and follow the instructions to begin the process.
7. Wait until a message indicates the process is complete.

Click **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 install, or activate them. Deleting the changes allows them to be retrieved again. Retrieving the changes again may correct the problem that caused the errors.

To delete internal code changes:

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2). One or more internal code changes must currently be retrieved 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 10-5.

   This opens the Change Internal Code window. It lists selections for each task available for working with internal code changes.
3. Select **Delete retrieved changes that were not installed** from the list, then click **OK**.

   This opens the Select Internal Code Changes window. It lists options for deleting either all or specific installed changes that were retrieved.
4. To delete *all* changes that are currently retrieved but not installed, select **All internal code changes**, then click **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 click **Delete** to begin the process of deleting all changes that are retrieved but not installed.
6. Wait until a message indicates the process is complete.

   Click **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.

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. When changes for continuous usage channels are installed, a hardware message is displayed explaining which types of channels need to be configured off and on again to activate the changes. To stop channel activity, you can either:

- Use an operating system facility to end channel activity.
- Use tasks from the Channel 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.

Machine type, **Machine model number**, **Machine serial number**, and **CPC identifier** identify the selected CPC.

Internal Code Change Information lists the part number, engineering change (EC) number and state levels of each set of licensed internal code associated with the support element

Licensed internal code controls many of the operations available on the support element. Internal code changes may provide new operations, or correct or improve existing operations.

The part number and EC number are assigned to a set of licensed internal code by IBM product engineering. The numbers identify the licensed internal code and its purpose.

If a set of licensed internal code is modified, its EC number is supplemented with a state level. A state level distinguishes between different versions of the same set of licensed internal code.

To view internal code change information:

1. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, access administrator, or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
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.
7. Select the internal code information you want and then click **Details...** to view the additional information about this internal code.

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 a DVD-RAM 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, DVD-RAM and FTP remain eligible sources. 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. 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 6-3 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. 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. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
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 of the next activation, click once on the check box to mark it.
   b. While the setting is disabled of the next activation, 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. Click **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. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).

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 setting is enabled, **Disable authorization status for next activation** box is empty.

      Disable the setting at the next activation, click once on the check box to mark it.
   b. While the setting is disabled, **Disable authorization status for next activation** box displays a check mark.

      To enable the setting at the next activation, click once on the check box to unmark it.
   c. Click **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.

   Note: The new setting is saved, but it will not become the current setting until the next activation of the CPC.

Defining clonable internal code levels

The **Define Clonable Internal Code Levels** task allows you to define internal code levels to save and send to RETAIN. The defined clonable internal code levels from a system are saved with an identifying name and password and sent to RETAIN, then later retrieved using the hardware management console to bring another system to the identical internal code level. The Define Clonable Internal Code Levels window displays a list of all clonable internal code levels that have been defined. Click **Details...** to display the engineering change numbers and levels associated with a selected defined clonable internal code level. You can use the **Define Clonable Internal Code Levels** task to:

- Create a new defined clonable internal code level to be saved and sent to RETAIN
- Replace an existing defined clonable internal code level with an updated level and send to RETAIN
- Delete an existing defined clonable internal code level that is no longer needed.

Note: The Define Clonable Internal Code Levels window displays the machine serial number for the support element. You will need this machine serial number when retrieving the clonable level definition data from the hardware management console.

To define a clonable internal code level:

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
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 **Define Clonable Internal Code Levels** 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 **Define Clonable Internal Code Levels** task to start it.

The Define Clonable Internal Code Levels window includes push buttons to perform tasks when working with defining a clonable internal code level. You can use the window to:

1. Type an identifying alphanumeric name and alphanumeric password of 1 to 8 characters in the **Name** and **Password** entry fields. Then, click **Create** to save a clonable internal code level to send to RETAIN.
2. Select a defined internal code level from the list to be replaced, then click **Replace** to replace the selected existing defined internal code level with an updated level to send to RETAIN.
3. Select a defined clonable internal code level from the list that is no longer needed, then click **Delete** to delete the existing defined clonable internal code level.

Use the online Help for more information on defining clonable internal code levels.

Performing an alternate support element action

This task allows you to perform the following actions for the primary/alternate support elements:

- Forcing mirroring of data prior to switching support elements
- Querying whether a switch between support elements can take place
- Switching support elements.

One support element is used for the primary, the other as the alternate. The primary support element is used for all hardware service. The alternate support element has a special workplace window with limited tasks available.

Forcing an immediate mirroring of the primary support element to the alternate support element

Notes:

1. Mirroring is suppressed if the support element has service status enabled.
2. Mirroring is suppressed if the alternate support element was loaded with a different CD-ROM from the primary support element.
3. Mirroring is suppressed if the alternate support element is fenced because of an automatic switch.

4. The primary support element is scheduled for automatic mirroring at 10 a.m. and 10 p.m. each day with a one-hour window for starting the operation. A record is added to the support element's event log to indicate the outcome of the operation.

This action mirrors support element data for the central processor complex (CPC). Mirroring support element data copies it from the CPC's primary support element to its alternate support element. By regularly mirroring support element data, you can help ensure that the alternate support element looks and works the same as the primary support element in case you need to switch to the alternate support element (for example, because of a hardware failure on the primary support element).

Ordinarily, support element data is mirrored automatically each day or when you install internal code changes through single step internal code changes, but you can use this action to mirror support element data immediately, at any time, and for any reason. The following are examples of when you would want to mirror support element data instead of waiting for the automatic mirroring default times:

- Licensed internal code changes
- Input/output configuration data set (IOCDS) changes
- Hardware configuration definition (HCD) changes
- Dynamic I/O changes
- Dynamic load address and parameter changes
- LPAR data
- Profile changes
- Lockout disruptive tasks
- Scheduled operations

To mirror the primary support element data:

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see "Establishing a support element console session from a Hardware Management Console" on page 1-2).
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 **Alternate Support Element** 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 **Alternate Support Element** task to start it.

   This opens the Alternate Support Element window.
7. Select the **Mirror the Primary Support Element data to the Alternate Support Element** radio button.
8. Click **OK** to perform the action.

Use the online Help for more information on the alternate support element actions.

Querying switch capabilities between support elements

The query switch capability action provides a quick check of the communication path between the support elements, the status of the automatic switch action, and their status. You can use this action before attempting a switch to the alternate support element or for checking the status of the automatic switch action.

To query switch capabilities:

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
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 **Alternate Support Element** 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 **Alternate Support Element** task to start it.

   This opens the Alternate Support Element window.
7. Select the **Query Switch capabilities** radio button.
8. Click **OK** to perform the action.

Use the online Help for more information on the alternate support element actions.

Switching to the alternate support element

You can use this action to switch to the alternate support element when the primary fails. When the manual switchover action is started, the system checks that all internal code levels are the same and that the CPC is activated. If the switch can be made concurrently, the necessary files are passed between the support elements, and the new primary support element is rebooted. If a disruptive switch is necessary, the CPC will be deactivated before completing the switch.

There are several conditions, when in progress, that will prevent a switchover:
- A mirroring task
- An internal code update
- A hard disk restore
- An engineering change.

The system automatically attempts a switchover for the following conditions:
- Primary support element has a serious hardware problem
- Primary support element detects a CPC status check
- Alternate support element detects a loss of communications to the primary over both the service network and the customer’s LAN.

Note: To disable the automatic switchover, See “Enabling automatic support element switchover” on page A-12.

To switch to the alternate support element:

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
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 Alternate Support Element 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 **Alternate Support Element** task to start it.

   This opens the Alternate Support Element window.
7. Select the **Switch the Primary Support Element and the Alternate Support Element** radio button.
8. Click **OK** to perform the action.

Use the online Help for more information on the alternate support element actions.

Chapter 11. Processor and storage operations

This section describes tasks from the **CP Toolbox** task list you can use to monitor and control the operation and storage of specific central processors (CPs) in the central processor complex (CPC).

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).
- 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. Generally, stopping processors for an image is effective only when the image and processors are operating.

To stop processors for an image:

1. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, or service representative user roles (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
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. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
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.
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.

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).
- 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. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
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. 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).
- Logical processors that support the images of logical partitions activated in operating modes other than coupling facility mode.

To restart a processor:

1. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).

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 object locking for disruptive tasks on an object” on page 2-18.
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 click **OK** 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, click **OK** to perform the restart.

    This begins the restart; a message displays when it is completed.
12. Click **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).
- Logical processors that support the images of logical partitions activated in operating modes other than coupling facility mode.

To interrupt a processor:

1. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
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.

   This immediately performs the operation; 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 condition 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.

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. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer user role (see "Establishing a support element console session from a Hardware Management Console" on page 1-2).
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 task that you can start:

   - **Stop on CP Address Match**
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 CPs in the work area. The area contains the target CPs.
8. Drag and drop a CP on a task to start it.

   The 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.

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)
- Access registers 0-15
- Prefix
- 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).
- 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. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, or service representative user role (see "Establishing a support element console session from a Hardware Management Console" on page 1-2).
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. Click **OK** to close the message when the operation completes successfully.

   Otherwise, if the operation does not complete successfully, follow the directions in the message to determine the problem and how to correct it.

Chapter 12. Channel operations

This section describes tasks from the **Channel Operations** task list you can use to monitor and control the operation of specific channels, identified with a physical channel identifier (PCHID). A channel path (CSS.CHPID) is associated with a physical channel identifier (PCHID).

Configuring channel paths on or off

Configure on and *configure off* are channel operations you can use to control whether channel paths (CSS.CHPIDs) are online or on standby in the active input/output (I/O) configuration. You can use the **Channel Operations** task list to configure channel paths (CSS.CHPIDs), associated with a specific physical channel identifier (PCHID), on and off. A channel path is identified with a CSS.CHPID. The CSS.CHPID is a single-digit number that identifies the channel subsystem followed by a decimal point followed by a two-digit number that identifies the channel path. See Chapter 13, “CHPID operations,” on page 13-1 for more information on configuring CSS.CHPIDs on and off.

To use the workplace to configure channel path’s on or off:

1. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2). The CPC must be power-on reset.
2. Open the **Task List** from the **Views** area.
3. Open **Channel Operations** from the **Task List Work Area**.

   The Channel Operations task list contains the **Configure On/Off** task that you will start.
4. Locate the channel, identified with a physical channel identifier (PCHID), that you want to configure on or off.
5. Open **Groups** from the **Views** area.
6. Open the **CPC** group, or any group that contains the CPC.
7. Right click on the target CPC object.
8. Select the **Channels** menu choice from the pop-up menu.

   This displays the Channel’s Work Area.
9. Select the channel, identified with a physical channel identifier (PCHID), that you want to configure on or off.
10. Drag and drop the selected channel on the **Configure On/Off** task to start it.

    This displays the Configure On/Off window. The window lists the CSS.CHPIDs, current state, target state, and messages associated with the channel you selected.
11. Initially, each channel’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 changing path 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 path you want to configure on or off, click **Apply** to make each channel path's new target state its current state.

Configuring reconfigurable channel paths in LPAR mode

When the central processor complex (CPC) is power-on reset, 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. 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 that 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.

It is recommended 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 12-1.
  2. Use the **Release** task to release the channel paths that are isolated. For instructions, see "Releasing reconfigurable channel paths" on page 12-3.
  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 12-4.

Releasing reconfigurable channel paths

Release is a channel operation you can use to free reconfigurable channel paths (CSS.CHPIDs), associated with a physical channel identifier (PCHID), from their assignment to isolated logical partitions.

Channel paths that are both reconfigurable and isolated are eligible for being released. You can use the Channel's 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. For more information on releasing channel paths, see "Releasing reconfigurable channel paths" on page 13-2

To release channel paths:

1. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, or service representative user role (see "Establishing a support element console session from a Hardware Management Console" on page 1-2).
2. The central processor complex (CPC) must be power-on reset.
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 **Channel Operations** from the **Task List Work Area**.

   The Channel 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 **Channels** menu choice.

    This displays the Channel's Work Area. The area contains the target channels. Channels are identified with a physical channel identifier (PCHID).
12. Select the reconfigurable channel paths you want to release.
13. Drag and drop the selected channels on the **Release** task.
14. Click **Release** from the confirmation window to confirm your request to release the selected channels.

    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 (CSS.CHPIDs). The icon label for a reconfigurable channel path displays **Reconfigurable**.

To reassign a channel path:

1. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
2. The central processor complex (CPC) must be power-on reset.
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 **Channel Operations** from the **Task List Work Area**.

   The Channel 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 **Channels** menu choice from the pop-up menu.
9. Select *one* reconfigurable channel, identified with a physical channel identifier (PCHID), that you want to reassign.
10. Drag and drop the selected channel 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, then click **Reassign**.
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 service on or off for channels

Service on and *Service off* are channel operations you can use to control whether channels, identified with physical channel identifiers (PCHIDs) are on standby in, or reserved from, the active input/output (I/O) configuration:

- A channel 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 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, which removes it from the active I/O configuration, allows running diagnostic tests on the channel without disturbing other channels being used by the system. Setting service on for a channel can be used also to remove failing channels from the I/O configuration so subsequent power-on resets will not attempt to initialize the failing channels.

If you have experience using other systems, setting service on or off for channels may have been referred to as taking channels in and out of single channel service (SCS), for which you may have used an SCS command with IN and OUT parameters.

To set service on and off for a channel:

1. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2). The CPC must be power-on reset.
2. Open the **Task List** from the **Views** area.
3. Open **Channel Operations** from the **Task List Work Area**.

   The Channel 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. Right click on the CPC to open its pop-up menu.
7. Select the **Channels** menu choice.
8. Select the channel, identified with a physical channel identifier (PCHID), that you want to set service on or off.
9. Drag and drop the selected channel on the **Service On/Off** task to start it.
10. Initially, each channel’s current state and target state are the same. Use the Service On/Off window controls to change the target states of the channel that you want to set the service state on or off:
    - If the current state of a channel is **Reserved**, toggle its target state to **Standby** if you want to set service off for the channel.
    - If the current state of a channel is **Standby**, toggle its target state to **Reserved** if you want to set service on for the channel.

If you attempt to change the target state of a channel that cannot have service set on or off, a message is displayed in the **Messages** list column to indicate changing the channel's state is not allowed. Double-click on the message for more information about why the channel state cannot be changed.

11. When you finish changing the target states of the channels for which you want to set service on or off, click **Apply** to make each channel's new target state its current state.

Setting the channel LED on

Show LED is a channel operation you can use to find the location of the jack and card slot in a cage. The light emitting diode (LED) is located below each card slot and near each jack in the cages that support attachment hardware. You can use this task for channel problem determination.

To set the show LED on:

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see "Establishing a support element console session from a Hardware Management Console" on page 1-2). The CPC must be power-on reset.
2. Open the **Task List** from the **Views** area.
3. Open **Channel Operations** from the **Task List Work Area**.

   The Channel Operations task list contains the **Show LED** 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 **Channels** menu choice.
8. Select the channel, identified with a physical channel identifier (PCHID), that you want the LED on for.
9. Drag and drop the selected channel on the **Show LED** task to start it.

   The Show LED window displays the PCHID for the LED that is on.
10. Click **OK** to turn the LED off.

Performing channel problem determination

You can use the Channels 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 physical channel identifier (PCHID), 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. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2). The CPC must be power-on reset and the image must be activated.
2. Open the **Task List** from the **Views** area.
3. Open **Channel Operations** from the **Task List Work Area**.

   The Channel Operations task list contains the **Channel Problem Determination** 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 channels. Channels are identified with a physical channel identifier (PHCID).
7. Right click on the CPC to open its pop-up menu.
8. Select the **Channels** menu choice.
9. Select the channels that you want to perform channel problem determination.
10. Drag and drop the selected channel on the **Channel Problem Determination** task to start it.

    The Partition Selection window lists the logical partitions which problem determination can be performed.
11. Select from the list the logical partition that you want to perform problem determination.
12. Click **OK**.

    The Channel Problem Determination window lists the types of problem determination information you can get for the selected channel.

    Note: The channel 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.
13. Select the radio button beside the type of problem determination information you want, then click **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’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 Channels Work Area to locate channels that have definition errors. The icon label for any channel that has a definition error displays **Definition error** for its status. After locating a channel that has a definition error, perform channel problem determination to determine the channel's exact definition error.

To determine a channel's exact definition error:

1. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, or service representative user role (see "Establishing a support element console session from a Hardware Management Console" on page 1-2).
2. The CPC must be power-on reset, the image must be activated, and the status displayed for the channel must be **Definition error**.
3. Start the **Channel Problem Determination** task for *one* channel that has a definition error. See "Performing channel problem determination" on page 12-6 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.
4. Select the **Analyze Channel Information** radio button, then click **OK**.

   This displays the Analyze Channel Information window. The window displays channel information for the selected channel path.
5. Click **Error details**.

   This displays a message that describes the selected channel's exact definition error.

   Note: **Error details** is *not* available if the status displayed for the selected channel is *not* **Definition error**.

Working with the Open Systems Adapter (OSA)-Express

The Open Systems Adapter (OSA)-Express is an integrated hardware feature that provides direct connection to clients on Local Area Networks (LAN). Each OSA-Express channel can be shared among all images in a single CSS of the server. This is referred to as the Multiple Image Facility (MIF), sharing of channels across logical partitions.

For more detailed information on OSA-Express, refer to *zSeries Open Systems Adapter-Express Customer's Guide and Reference*.

An OSA-Express can be a channel type of OSE, OSD, or OSC. An OSC channel is an OSA Integrated Console Controller (OSA-ICC). For more information on OSA-ICC, refer to the *zSeries Open Systems Adapter-Express Integrated Console Controller User's Guide*.

Using Advanced Facilities for OSA-Express Channels

You can use the Support Element workplace to open a facility for monitoring, operating, and customizing an OSA-Express channel. To work with an OSA-Express channel:

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2). The CPC must be power-on reset.
2. Open the **Task List** from the **Views** area.
3. Open **Channel Operations** from the **Task List Work Area**.

   The Channel Operations list contains the **Advanced Facilities** 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 **Channels** menu choice from the pop-up menu. This displays the Channel’s Work Area.
8. Select the OSA-Express channel that you want to work with.

   The OSA-Express channel is represented by the channels icon in the Channels Work Area.
9. Drag and drop the selected OSA-Express channel on the **Advanced Facilities** task.

   This displays the **Standard Channel Advanced Facilities** window.
10. The **Standard Channel Advanced Facilities** window displays a list of actions you can take for the selected channel path. The list of tasks includes the following:
    - Card specific advanced facilities
    - View code level
    - Card Trace/Log/Dump Facilities
    - Reset to default
11. If you select the **Card specific advanced facilities** radio button, click **OK**.
12. The **Advanced Facilities** window displays a list of actions you can take for the selected channel. Depending on the channel and hardware type installed on your system, the list of tasks can include several of the following:

    Enable/disable ports
    : Displays to enable or disable the LAN ports for the selected OSA-Express channel.

    Query port status
    : Displays the LAN port record of each LAN port on the selected OSA-Express channel. A LAN port record displays the port identifier, indicates whether the port is enabled or disabled, indicates whether the port is in support element control mode, and indicates the source of the command that disabled the port if the port becomes disabled while it is in support element control mode.

    Run port diagnostics
    : Displays *normal* and *wrap plug test* diagnostic type choices for the selected OSA-Express channel.

    View port parameters
    : Displays a subset of the industry-standard port parameters of LAN

ports on the selected OSA-Express channel. LAN port parameters describe the characteristics and control the operations of a LAN port.

View code level
Displays the internal code level for the selected OSA-Express channel.

Display or alter MAC address
Displays the medium access control (MAC) addresses of the ports on the selected OSA-Express channel. A MAC address identifies a port as a destination and source of information it receives and transmits, respectively, on the LAN.

Set card mode
Displays the speed and mode selections to set for the identified port of the selected OSA-Express channel.

Display client connections
Displays the active client connections for the selected OSA-Express channel.

Display active sessions configuration
Displays the active sessions configuration for the selected OSA-Express channel.

Display active server configuration
Displays the active TCP/IP connection configuration information for the selected OSA-Express channel.

Panel configuration options
Displays the edit session configuration for the selected OSA-Express channel. This includes a list of the sessions that are configured on each session.

Manual configuration options
Displays the configuration options you can manually work with for the selected OSA-Express channel.

Activate configuration
Displays the activate session configuration for the selected OSA-Express channel.

Display activate configuration errors
Displays the activate configuration errors, if any exist.

Debug utilities
Displays debug utility options you can work with for the selected OSA-Express channel.

13. Select the task that you want to start, then click **OK**.
14. After starting a task, use the online Help for more information to complete the task.

Chapter 13. CHPID operations

This section describes tasks from the **CHPID Operations** task list you can use to monitor and control the operation of specific channel paths with channel path identifiers (CSS.CHPIDs) defined in the input/output (I/O) configuration of the central processor complex (CPC). The CSS.CHPID is a single-digit number that identifies the channel subsystem followed by a decimal point followed by a two-digit number that identifies the channel path.

Configuring channel paths on or off

Configure on and *configure off* are CHPID 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. 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. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2). 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 images which you want to configure the 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:

   Each logical partition is an image. Locate an image if you want to work only with channel paths defined for a specific logical partition.
5. Open **Groups** from the **Views** area.
6. Open the **Images** group, or any group that contains the image.

7. Right click on the target image object to which the target channel paths are defined.
8. 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.
9. Select the channel paths you want to configure on or off.
10. 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 CSS.CHPID, current state, target state, and messages for each channel path you selected.
11. 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.
12. When you finish changing the target states of the channel paths you want to configure on or off, click **Apply** to make channel path's new target state its current state.

Releasing reconfigurable channel paths

Release is a CHPID 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 8-1.

Reconfigurable channel paths assigned to an isolated logical partition do not become available to other logical partitions when they are configured off. 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 CHPID's 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. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
2. The central processor complex (CPC) must be power-on reset.
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 **Images** group, or any group that contains the image.
10. Right click on the target image object to which the target channel paths are defined.
11. Select the **CHPIDs** menu choice from the pop-up menu.

    This displays the object’s CHPID’s 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. Click **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.

Setting the channel LED on

Show LED is a CHPID operation you can use to find the location of the jack and card slot in a cage. The light emitting diode (LED) is located below each card slot and near each jack in the cages that support attachment hardware. You can use this task for channel problem determination.

To set the show LED on:

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2). 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 **Show LED** 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 target image object to which the target channel paths are defined.
7. Select the **CHPIDs** menu choice from the pop-up menu.

   This displays the object's CHPID's Work Area. The area contains the target channel paths.
8. Select the channel path you want the LED on for.
9. Drag and drop the selected channel path on the **Show LED** task to start it.

   The Show LED window displays the CSS.CHPID for the LED that is on.
10. Click **OK** to turn the LED off.

Performing channel problem determination

You can use the CHPID's 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 CSS.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. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, or service representative user role (see "Establishing a support element console session from a Hardware Management Console" on page 1-2). The CPC must be power-on reset and the image must be activated.
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 for which 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. Each logical partition is an 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 for which 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 CSS.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 click **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. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, or service representative user role (see "Establishing a support element console session from a Hardware Management Console" on page 1-2).
2. The CPC must be power-on reset, the image must be activated, 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 12-6 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 click **OK**.

   This displays the Analyze Channel Information window. The window displays channel information for the selected channel path.

5. Click **Error details**.

   This displays a message that describes the selected channel path's exact definition error.

   Note: **Error details** is *not* available if the status displayed for the selected channel path is *not* **Definition error**.

Enabling NPIV mode

Use this task to enable NPIV mode for selected channel paths. When NPIV mode is enabled for selected logical partitions, the system provides a virtual FCP channel for each s390 device definition for a FCP channel in the active Input/Output configuration.

Note: The channel paths must be configured offline to enable NPIV mode.

To set the NPIV configuration:

1. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, or service representative user mode (see "Establishing a support element console session from a Hardware Management Console" on page 1-2).
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 **NPIV - On/Off** 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 **NPIV - On/Off** task to start it.

   The NPIV Mode On/Off window displays.

Use the online Help for more information on enabling the NPIV mode.

Chapter 14. Crypto service operations

This section describes tasks from the **Crypto Service Operations** task list you can use to monitor and control the operation of specific crypto defined in the configuration of the central processor complex (CPC).

Configuring crypto on or off

Configure on and *configure off* are crypto service operations you can use to control whether crypto are online or standby in the active configuration:

- A crypto is *online* while configured on. It is in the active configuration and it can be used.
- A crypto is *standby* while configured off. It is in the active configuration but it cannot be used until it is configured on.

You can use the support element workplace to configure crypto 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 crypto, the operating system running in any image that owns or shares the crypto is not notified, and the next operation from the operating system to the crypto causes an error. When using z/OS operating environment, deactivate the crypto through ICSF before configuring off crypto.

Note: To determine when crypto initialization has completed after a configure on of a crypto, see “Checking status for the Crypto Express2 feature” on page 9-16

To use the workplace to configure a crypto on or off:

1. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2). The CPC must be power-on reset and the logical partitions must be activated.
2. Open the **Task List** from the **Views** area.
3. Open **Crypto Service Operations** from the **Task List Work Area**.

   The Crypto Service Operations task list contains the **Configure On/Off** task that you will start.
4. Locate the images which you want to configure the crypto on or off. One or more images is created during a power-on reset of the CPC and the active configuration is established during partition activation.
   - Each logical partition is an image. Locate the CPC if you want to work with *all* crypto in all active partitions. Locate an image if you want to work only with crypto defined for a specific logical partition.
5. Open **Groups** from the **Views** area.
6. Open the **Images** group, or any group that contains the image.
7. Right click on the target image which the target crypto are defined.

8. Select the **Crypto** menu choice from the pop-up menu.
   The area contains the target crypto.
9. Select the crypto you want to configure on or off.
10. Drag and drop the selected crypto on the **Configure On/Off** task to start it.
    This displays the Configure On/Off window. The window lists the crypto, current state, target state, and messages for each crypto you selected.
11. Initially, each crypto's current state and target state are the same. Use the window's controls to change the target states of the crypto you want to configure on or off:
    - If the current state of a crypto is **Online**, toggle its target state to **Standby** if you want to configure off the crypto.
    - If the current state of a crypto is **Standby**, toggle its target state to **Online** if you want to configure on the crypto path.

    Note: If you attempt to change the target state of a crypto that cannot be configured on or off, a message is displayed in the **Messages** list column to indicate changing the crypto state is not allowed. Double-click on the message for more information about why the crypto state cannot be changed.
12. When you finish changing the target states of the crypto you want to configure on or off, click **Apply** to make each crypto new target state its current state.

Setting service on or off for crypto

Service on and *Service off* are crypto service operations you can use to remove from or add back in crypto, identified with physical channel identifiers (PCHIDs), in the active configuration:

- A crypto is *standby* while service is set off. It is in the active configuration but it cannot be used until it is configured on. It will remain in the active configuration until service is set on.
- A crypto is *reserved* while service is on. It is not in the active configuration and cannot be used. It will remain out of the active configuration until service is set off.

Setting service on for a crypto, which removes it from the active configuration, allows running diagnostic tests on the crypto without disturbing other crypto being used by the system. Setting service on for a crypto can be used also to remove failing crypto from the configuration so subsequent power-on resets and partition activations will not attempt to initialize the failing of crypto.

If you have experience using other systems, setting service on or off for crypto may have been referred to as taking channels 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 service on and off for crypto.

To set crypto service on and off:

1. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2). The CPC must be power-on reset.
2. Open the **Task List** from the **Views** area.
3. Open **Crypto Service Operations** from the **Task List Work Area**.

   The Crypto Service 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 crypto:
7. Right click on the CPC to open its pop-up menu.
8. Select the **Crypto** menu choice.
9. Select the crypto, identified with a physical channel identifier (PCHID), that you want to set service on or off.
10. Drag and drop the selected crypto on the **Service On/Off** task to start it.
11. Initially, each crypto’s current state and target state are the same. Use the Service On/Off window controls to change the target states of the crypto that you want to set the service state on or off:
    - If the current state of a crypto is **Reserved**, toggle its target state to **Standby** if you want to set service off for the crypto.
    - If the current state of a crypto is **Standby**, toggle its target state to **Reserved** if you want to set service on for the crypto.

    If you attempt to change the target state of a crypto that cannot have service set on or off, a message is displayed in the **Messages** list column to indicate changing the crypto state is not allowed. Double-click on the message for more information about why the crypto state cannot be changed.
12. When you finish changing the target states of the crypto that you want to set service on or off, click **Apply** to make each crypto’s new target state its current state.

Performing crypto problem determination

You can use the Crypto Work Area to determine the state and status of specific crypto in the central processor complex (CPC). The label for each crypto’s icon includes it crypto, state, and status. When you need more detailed information, you can use the support element workplace to perform problem determination. Perform problem determination to get information for a crypto.

To perform crypto problem determination:

1. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2). The CPC must be power-on reset and the partition must be activated.
2. Open the **Task List** from the **Views** area.

3. Open **Crypto Service Operations** from the **Task List Work Area**.

   The Crypto Service Operations task list contains the **Channel Problem Determination** task that you will start.
4. Locate the image that owns or shares the crypto for which you want to perform crypto problem determination. One or more images is created and the active configuration is established during a power-on reset of the CPC.
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 crypto is defined to open its pop-up menu.
8. Select the **Crypto** menu choice from the pop-up menu.
9. Select *one* target crypto that you want to perform crypto problem determination.
10. Drag and drop the selected crypto on the **Channel Problem Determination** task to start it.

    The Channel Problem Determination window lists the Analyze Channel Information problem determination you can get for the selected crypto.
11. Select the radio button beside the type of problem determination information, then click **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 crypto's problem determination information is displayed.

Identifying crypto 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. Cryptos are not defined in the I/O configuration, but are defined when they are installed. A *crypto definition error* occurs when:

- The definition of a crypto conflicts with the definition of a channel in the I/O configuration.

You can use the Crypto Work Area to locate crypto that have definition errors. The icon label for any crypto that has a definition error displays **Definition error** for its status. After locating crypto that have a definition error, perform crypto problem determination to determine the crypto's exact definition error.

To determine a crypto's exact definition error:

1. Log onto the support element on the hardware management console through **Single Object Operations** in advanced operator, system programmer, or service representative user mode (see "Establishing a support element console session from a Hardware Management Console" on page 1-2).
2. The CPC must be power-on reset, the image must be activated, and the status displayed for the crypto must be **Definition error**.
3. Start the **Channel Problem Determination** task for *one* crypto that has a definition error. See "Performing channel problem determination" on page 12-6 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 crypto.
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 crypto.

5. Click **Error details**.

   This displays a message that describes the selected crypto's exact definition error.

   Note: **Error details** is *not* available if the status displayed for the selected crypto is *not* **Definition error**.

Using advanced facilities for crypto

You can use the support element workplace to open a facility for monitoring, operating, and customizing a crypto. To work with a crypto:

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see "Establishing a support element console session from a Hardware Management Console" on page 1-2). The CPC must be power-on reset.
2. Open the **Task List** from the **Views** area.
3. Open **Crypto Service Operations** from the **Task List Work Area**.

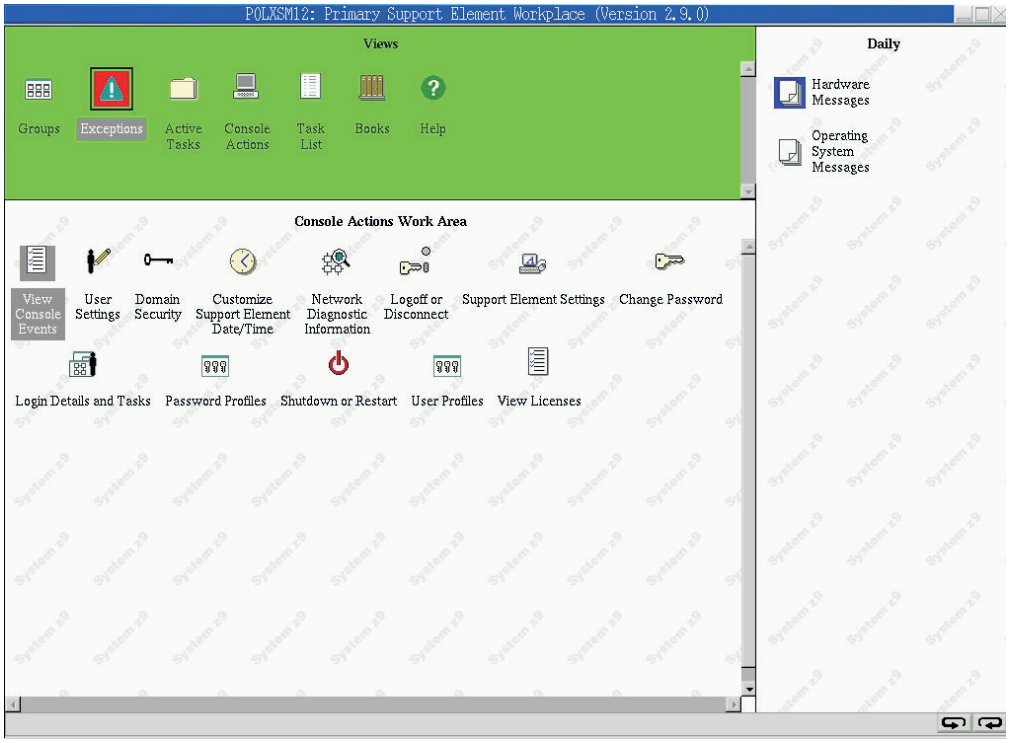
   The Crypto Service Operations list contains the **Advanced Facilities** task that you will start.
4. Open **Groups** from the **Views** area.
5. Open the **CPC** group, or any group that contains the CPC.
6. Right click on the CPC.
7. Select the **Crypto** menu choice from the pop-up menu. This displays the CPC's in the work area.
8. Select the crypto that you want to work with.

   The crypto is represented by the crypto icon in the Crypto Service Work Area.
9. Drag and drop the selected crypto on the **Advanced Facilities** task.

   This displays the **Standard Channel Advanced Facilities** window.
10. The **Standard Channel Advanced Facilities** window displays a list of actions you can take for the selected crypto. The list of tasks include:
    - View code level
    - Card Trace/Log/Dump Facilities
11. Select the task that you want to start, then click **OK**.

Console Actions

This section describes the tasks from the **Console Actions** task list that you can use to access information, monitor and operate the support element console, and customize console settings.



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 roles. The access administrator user role is used to set up user identifications and passwords, and allow access to a particular user role of operation. The system programmer user role 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.

Changing your Password

Use this task to change your password for logging on the support element console.

To change your support element logon password:

1. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer,

or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).

2. Open the **Console Actions** from the Views area.
3. Open **Change Password** from the Console Actions Work Area.

   The Change Password window is displayed
4. Enter your current password and your new password twice, the latter time to confirm it.
5. Click **OK** to change your password.

Use the online Help for more information on completing this task.

Customizing your Password Profiles

Use this task to create, customize, or verify the password rules assigned to the system users. There are three default password rules that you can choose from if you do not want to create your own. They are: basic, strict, and standard.

To customize a password profiles:

1. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
2. Open the **Console Actions** from the Views area.
3. Open **Password Profiles** from the Console Actions Work Area.

   The Password Profiles window is displayed
4. You can either create new rules for a password or modify existing ones.
5. Click **OK** once you have defined the password properties to save the settings.

Use the online Help for more information on completing this task.

Customizing your User Profiles

Use this task to manage your system users that log onto the support element console. This task enables you to add, remove, copy, or modify user profiles using the default user roles on the support element console. A user profile consists of a user ID (user identification), password, managed resource roles, and task roles.

The user ID and password are used to verify a user’s authorization to log on the support element console. The user ID can be 4 to 32 characters in length and can be a combination of letters (a-z) and numbers (0-9), The password is determined by the password rule that is chosen for the user ID. The default choices are *basic*, *strict*, and *standard*; however, other rules may also be available if they were defined in the **Password Profiles** task. All of these rules have their own set of specifications for assigning a password. Your Access Administrator determines what password rule is appropriate for you.

The user ID also includes managed resource roles and task roles. You can choose from a list of available default managed resource and task roles.

The default managed resource roles include:

- All Managed Objects

- Limited Managed Objects

The default task roles include:
- Access Administrator Tasks
- Advanced Operator Tasks
- Operator Tasks
- Service Representative Tasks
- System Programmer Tasks

To customize a user profile:

1. Log onto the support element on the hardware management console through **Single Object Operations** in access administrator user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
2. Open the **Console Actions** from the Views area.
3. Open **User Profiles** from the Console Actions Work Area.

   The User Profiles window is displayed.
4. Select the type of user ID you want to customize.
5. If you are creating a new user ID, point to User on the menu bar.
6. Click **Add** when the menu is displayed. The Add User window is displayed.

   If the user ID already exists in the window, select the user ID from the list and then point to **User** on the menu bar. When the menu is displayed, click **Modify**. The Modify User window is displayed.
7. Compare or change the fields in the window.
8. Click **OK** when you have finished.

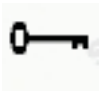
Use the online Help for more information on completing this task.

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.

The domain name and password of the console authorize its communication with the objects in its domain. They prevent unauthorized sources attached to the same local area network (LAN) from communication with other objects.

To define the domain security:



1. Log onto the support element on the hardware management console through **Single Object Operations** in access administrator or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
2. Open the **Console Actions** from the Views area.

3. Open **Domain Security**.

Use the online Help for more information on completing this task.

Monitoring the support element

You can view console events, network diagnostic information, security logs, and other information that the support element monitors.

Viewing console events

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.

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.

When an event occurs, the date and time occurs and a brief description of the event are recorded in the **Console Event Log**. This information is listed on the View Console Events window under the **Date**, **Time**, and **Console Event** headings, respectively.

Initially, all events are listed. The events are displayed in descending order, from the most recent event to the oldest event

Use the options in **View** on the menu bar to change to a different time range, or to change how the events display in the summary.

To view console events:

1. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, access administrator, or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
2. Open the **Console Actions** from the **Views** area.
3. Open **View Console Events** from the **Console Actions Work Area**. The View Console Events window is displayed.

Use the online Help for more information on viewing console events.

Viewing Network Diagnostic Information

You can use the support element workplace to start the task to view network diagnostic information on your support elements network protocols.

This task lets you view information concerning the networking configuration on this support element console. There are tabs (Interfaces, Address, Routes, ARP, Sockets, TCP, UDP, IP, ICMP, and Native Connections) to scroll through for information.

To view your network diagnostic information:

1. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, access administrator, or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
2. Open the **Console Actions** from the **Views** area.
3. Open **Network Diagnostic Information** from the **Console Actions Work Area**. The Network Diagnostic Information window is displayed.
4. Select a Network Diagnostic Information tab to view information.

   Use the online Help for more information on viewing the network diagnostic information.

Pinging the TCP/IP address

To ping a TCP/IP address:

1. Open the **Network Diagnostic Information** window.
2. Select the Ping tab.
3. Enter the TCP/IP address to ping.
4. Click **Ping**.

Viewing security logs

You can use the support element workplace to start the console action for viewing security logs for the CPC. The support element automatically keeps a default security log of security events that occur while the support element application is running

To view security logs:

1. Log onto the support element on the hardware management console through **Single Object Operations** in system programmer or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
2. Open the **Console Actions** from the **Views** area.
3. Open **View Security Logs** from the **Console Actions Work Area**. The View Security Logs window is displayed.

4. The window displays the **Security Event** and the **Date** and **Time** the security log is created. Use the menu bar to open a security log or search a security log by data or event.
5. If you need to view a security event log that is not displayed. Click **Show Earlier Events** or **Show Later Events**.

Use the online Help for more information on reviewing the console events.

Customizing support element settings

You can customize console settings to 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. 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. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, access administrator, or service representative user role (see "Establishing a support element console session from a Hardware Management Console" on page 1-2).
2. Open the **Console Actions** from the **Views** area.
3. Open **User Settings** from the **Console Actions Work Area**. The window displays the support element console's current settings.
4. Select the **Colors and Patterns** tab.
5. To check the color currently set for a status, select the status term from the list labelled **Conditions**.

   This highlights the color, in the **Color** list, currently set for the status.

   Notes:

   a. To use black and white patterns instead of colors for indicating unacceptable statuses, check **Use patterns instead of colors**. A check mark displays when you mark it.
6. To change the color set for a status:
   a. Select the status term from the **Conditions** list.
   b. Select the color from the **Color** list.
   c. Click **Apply**.
7. When you finish changing the colors set for indicating unacceptable statuses, click **Close**.

Use the online Help for more information on using the window to change the console's colors set for indicating unacceptable statuses.

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. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer, access administrator, or service representative user role (see "Establishing a support element console session from a Hardware Management Console" on page 1-2).
2. Open the **Console Actions** from the **Views** area.
3. Open **User Settings** from the **Console Actions Work Area**.

   The window displays the support element console's current settings
4. Select the **Colors and Patterns** page tab.
5. To check the color currently set for a summarized system status, select a condition from the list labelled **Conditions**.

   This highlights the color, in the **Color** list, currently set for the summarized system status.

   Notes:

   a. To use black and white patterns instead of colors for summarized system statuses, check **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 the condition from the **Conditions** list.
   b. Select the color from the **Color** list.
   c. Click **Apply**.
7. When you finish changing the colors set for summarized system statuses, click **Close** from the window.

Use the online Help for more information on changing the console's colors set for summarized system status.

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. Log onto the support element on the hardware management console through **Single Object Operations** in operator, advanced operator, system programmer,

access administrator, or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).

2. Open the **Console Actions** from the **Views** area.
3. Double-click on the **User Settings** console action to start it.

   The pages display the support element console’s current settings.
4. Click on the **Colors and Patterns** tab.
5. To check the color currently set for a message indicator, select either **Hardware Messages** or **Operating System Messages** from the list labelled **Conditions**.

   This highlights the color, in the **Color** list, currently set for the message indicator.

   Notes:

   a. To use black and white patterns instead of colors for message indicators, check **Use patterns instead of colors**. A check mark displays when you mark it.
6. To change the color set for a message indicator:
   a. Select either **Hardware Messages** or **Operating System Messages** from the **Conditions** list.
   b. Select the color from the **Color** list.
   c. Click **Apply**.
7. When you finish changing the colors set for message indicators, click **Close**.

Use the online Help for more information on using the window to change the console’s colors set for message indicators.

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. This task allows you to enable or disable an SNMP agent and set up a community name file and event notification information for an SNMP agent. For more information see *Application Programming Interfaces*. An online copy of this book is available under the Books icon in the Views area of your Support Element Console workplace.

To change your Application Programming Interface:

1. Log onto the support element on the hardware management console through **Single Object Operations** in access administrator user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
2. Open the **Console Actions** from the Views area.
3. Open **Support Element Settings** from the Console Actions Work Area.

   The Support Element Console Settings Work Area is displayed.
4. Open the **Customize API Settings** task from the Support Element Settings Work Area.

The Customize API Settings window is displayed.

Use the online Help for more information on completing this task.

Customizing Network Settings

This task allows you to view the current network information for the Support Element Console and to change the network settings as shown in the following list. Network settings changes are applied after a network restart, no reboot is needed for updated setting to take effect.

Identification
Contains the host name and domain name of the Support Element Console.

Console name
Your Support Element Console user name, the name that identifies your console to other consoles on the network. This is the short host name, for example: seibm1.

Domain name
An alphabetic name that Domain Name Services (DNS) can translate to the IP address, For example, DNS might translate the domain name 222.example.com to 198.105.232.4 (The long host name consists of console name plus a period plus a domain name, for example: seibm1.endicott.ibm.com.) Definition

Console description
This is for customer use only. An example might be: Main Support Element Console for customer finance.

LAN Adapters
A summarized list of all (visible) LAN adapters. You can select any of these and click **Details...** to launch a window allowing you to change addressing, routing, and other LAN adapter characteristics.

Name Services
The Domain Name Services (DNS) and domain suffix values.

Routing
Routing information and default gateway information. The latter includes

Default Gateway Information
The Gateway Address is the route to all networks. The Default gateway address (if defined) informs each personal computer or other network device where to send data if the target station does not reside on the same subnet as the source.

You can assign a specific LAN to be the Gateway device or you can choose ″any.″

Enable 'routed'
Indicates whether to start the routed daemon.

To customize the network settings:

1. Log onto the support element on the hardware management console through **Single Object Operations** in access administrator user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
2. Open the **Console Actions** from the Views area.
3. Open **Support Element Settings** from the Console Actions Work Area.

   The Support Element Console Settings Work Area is displayed.
4. Open the **Customize Network Settings** task from the Support Element Settings Work Area.

   The Customize Network Settings window displays to allow you to view or change settings.

   Note: If you change network settings, these are applied when you restart the network; you are not required to reboot.

Use the online Help for more information on completing this task.

Customizing Product Engineering Access

Use this task to verify or change the settings authorizing IBM Product Engineering (PE) local or remote access to the support element console.

With access authority, IBM Product Engineering can log on the support element console in an exclusive user identification 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 console.

Use this task to control whether the support element console accepts the Product Engineering user identification and password for logging on.

To customize the product engineering access:

1. Log onto the support element on the hardware management console through **Single Object Operations** in access administrator user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
2. Open the **Console Actions** from the Views area.
3. Open **Support Element Settings** from the Console Actions Work Area.

   The Support Element Console Settings Work Area is displayed.
4. Open the **Customize Product Engineering Access** task from the Support Element Settings Work Area.

   The Customize Product Engineering Access window displays to allow you to view or change settings.

Use the online Help for more information on completing this task.

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 and z/OS Processor Operations Component (SA OS/390 and z/OS 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.

Ordinarily, 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. Log onto the support element on the hardware management console through **Single Object Operations** in advanced operator, system programmer, access administrator, or service representative user role (see "Establishing a support element console session from a Hardware Management Console" on page 1-2).
2. Open the **Console Actions** from the **Views** area.
3. Double-click on the **Support Element Settings** console action in the Console Actions Work Area to start it.

   This displays the Support Element Settings Work Area.
4. Double-click on the **Customize Console Services** console action in the Support Element Settings Work Area.
5. Locate the Exclusive Control choice from the Customize Console Services. It lists choices for enabling or disabling the exclusive control service. The selected choice indicates the current setting of the service.

6. Select a different choice to change the setting, click **OK** to save the setting and close the window.

Use the online Help for more information on the exclusive control service.

Enabling automatic support element switchover

You can use the support element workplace to control whether the support element is to be automatically switched to the alternate support element.

To enable or disable automatic support element switchover:

1. Log onto the support element on the hardware management console through **Single Object Operations** in advanced operator, system programmer, access administrator, or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
2. Open the **Console Actions** from the **Views** area.
3. Double-click on the **Support Element Settings** console action in the Console Actions Work Area to start it.

   This displays the Support Element Settings Work Area.
4. Double-click on the **Customize Console Services** console action in the Support Element Settings Work Area.
5. Locate the Automatic SE Switchover choice from the Enable Support Element Console Services window. It lists choices for enabling or disabling Automatic SE switchover. The selected choice indicates the current setting of the service.
6. Select **Enabled** or **Disabled**, then click **OK** to save the setting.

Use the online Help for more information on the automatic SE switchover.

Enabling Capacity Backup Services

You can use the support element workplace to control whether to test or temporarily upgrade the CBU feature via the IBM service support system.

To enable or disable capacity backup:

1. Log onto the support element on the hardware management console through **Single Object Operations** in advanced operator, system programmer, access administrator, or service representative user role (see “Establishing a support element console session from a Hardware Management Console” on page 1-2).
2. Open the **Console Actions** from the **Views** area.
3. Double-click on the **Support Element Settings** console action in the Console Actions Work Area to start it.

   This displays the Support Element Settings Work Area.
4. Double-click on the **Customize Console Services** console action in the Support Element Settings Work Area.

5. Locate the Capacity Backup choice from the Customize Console Services window. It lists choices for enabling or disabling Capacity Backup. The selected choice indicates the current setting of the service.
6. Select **Enabled** to activate the CBU feature via the IBM service support system.
7. CLick **OK** to save the setting.

Use the online Help for more information on the capacity backup.

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.

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.

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

Only a Hardware Management Console can analyze optical errors for *integrated* support elements. A Hardware Management Console analyzes optical errors for a support element if:

- The Hardware Management Console is configured as a Problem Analysis Focal Point.
- The support element's CPC is defined to the Hardware Management Console.
- And the Hardware Management Console's *Optical and I/O Error Analysis setting* is enabled.

See *Hardware Management Console Operations Guide* for instructions for enabling or disabling a Hardware Management Console's optical and I/O error analysis setting.

Performing Problem Analysis on System I/O errors

Some system I/O devices, mostly tape and DASD products, report errors to the local operating system as they occur. The operating system may record the errors in its error recording data set and may also report the problem to the support element.

If there are no hardware management consoles that have the Problem Analysis Focal Point function enabled (by enabling Optical and I/O Error Analysis setting), then the support element problem analysis function will analyze the error report and possibly report it as a hardware message.

If there is a hardware management console that has the Problem Analysis Focal Point function enabled and the support element is configured to it, then the I/O error reports will be forwarded to that hardware management console for analysis and potential reporting under the Optical Network and System I/O message icon.

Either the support element or the hardware management console may determine that the I/O error needs to be reported to the service representative and will automatically initiate the report, if so configured.

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 Sysplex Timer or Server Time Protocol (STP) 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.
- If the CPC uses a Sysplex Timer or Server Time Protocol (STP) as a time source, changing the time or date at the Sysplex Timer or at the Current Time Server in an STP-only Coordinated Timing Network automatically synchronizes the CPC TOD clock to the new time.
- 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.
  - The support element TOD clock is updated with local time adjustments (daylight saving time offset, leap seconds offset, and time zone offset) when they occur, if it is synchronized with the CPC TOD clock.
  - 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 or Server Time Protocol (STP) as a time source for the CPC is intended to prevent manually setting the support element TOD clock.

If the CPC does not or cannot use a Sysplex Timer or Server Time Protocol (STP) as a time source, you can manually set the support element TOD clock.

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 when the CPC does not or cannot use a Sysplex Timer or Server Time Protocol (STP) as a time source.

To set the support element TOD clock:

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

   The work area contains the **Support Element Customize Date/Time** action that you will start.
2. Double-click on the **Support Element Customize Date/Time** console action to start it.

   The Customize Console Date and Time window displays the current date, time, and time-zone offset set for the support element TOD clock.
3. Click **Cancel** if no corrections are necessary.
4. Enter corrections, if needed, then click **Customize**.
5. Click **OK**.
6. Click **Refresh** to display the new changes.
7. Click **Cancel** to close the window.

Use the online Help for more information on setting the support element TOD clock.

Viewing Licensed Internal Code

You can use the support element workplace to start the console action for viewing the licensed internal code (LIC) that you have agreed to for this support element console. This list does not include program and code provided under separate license agreements. This task window appears after the initialization window or to view the license

To view licensed internal code:

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

   The work area contains the **View Licenses** task from the Console Actions Work Area.
2. Open **View Licenses** from the Console Actions Work Area.

   The View Licenses window is displayed.
3. Click on any of the license links to get more information.
4. Click **OK** when you are done.

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 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 described 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 laws:

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.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, or other countries, or both:

ESCON
IBM
Netfinity
OS/390
Parallel Sysplex
PR/SM
RACF
Resource Link
RETAIN
RMF
Sysplex Timer
System z9
S/390
z/OS
z/VM

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of 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 statements apply 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 Class A digital apparatus complies with Canadian ICES-003.

Avis de conformlté aux normes du ministère des Communications du Canada

Cet appareil numérique de la classe A est conform à la norme NMB-003 du Canada.

European Union (EU) Electromagnetic Compatibility Directive

This product is in conformity with the protection requirements of EU Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to European Standard EN 55022. The limits for Class equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

Warning: This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

EC Declaration of Conformity (In German)

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 89/336/EWG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der IBM gesteckt/eingebaut werden.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden: ″Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen.″

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem “Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)“. Dies ist die Umsetzung der EU-Richtlinie 89/336/EWG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) vom 18. September 1998 (bzw. der EMC EG Richtlinie 89/336) für Geräte der Klasse A.

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Konformitätserklärung nach Paragraf 5 des EMVG ist die IBM Deutschland GmbH, 70548 Stuttgart.

Informationen in Hinsicht EMVG Paragraf 4 Abs. (1) 4:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

update: 2004/12/07

People’s Republic of China Class A Compliance Statement

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may need to perform practical actions.

声　明

此为Ａ级产品，在生活环境中，
该产品可能会造成无线电干扰。
在这种情况下，可能需要用户对其
干扰采取切实可行的措施。

Japan Class A Compliance Statement

This product is a Class A Information Technology Equipment and conforms to the standards set by the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Korean Class A Compliance Statement

이 기기는 업무용으로 전자파적합등록을 한 기기이오니 판매자 또는 사용자는 이점을 주의하시기 바라며, 만약 잘못 판매 또는 구입하였을 때에는 가정용으로 교환하시기 바랍니다.

Taiwan Class A Compliance Statement

Warning: This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user will be required to take adequate measures.

警告使用者:
這是甲類的資訊產品，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。

台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

Index

A

B

C

D

E

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

Printed in USA

SC28-6858-01