System i

Managing Operations Console

System i

Managing Operations Console

Note

Before using this information and the product it supports, read the information in "Notices" on page 113 and the *IBM Systems Safety Information* manual, G229-9054.

Ninth Edition (September 2007)

Contents

Safety and environmental notices

Safety notices may be printed throughout this guide:

- **DANGER** notices call attention to a situation that is potentially lethal or extremely hazardous to people.
- **CAUTION** notices call attention to a situation that is potentially hazardous to people because of some existing condition.
- **Attention** notices call attention to the possibility of damage to a program, device, system, or data.

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 U.S. English source. Before using a U.S. English publication to install, operate, or service this 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 U.S. English publications.

Laser safety information

IBM® System i® models can use I/O cards or features that are fiber-optic based and that 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:
This product might contain one or more of the following devices: CD-ROM drive, DVD-ROM drive, DVD-RAM drive, or laser module, which are Class 1 laser products. Note the following information:

- **Do not remove the covers. Removing the covers of the laser product could result in exposure to hazardous laser radiation. There are no serviceable parts inside the device.**
- **Use of the controls or adjustments or performance of procedures other than those specified herein might result in hazardous radiation exposure.**

(C026)

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)

CAUTION:
Some laser products contain an embedded Class 3A or Class 3B laser diode. Note the following information: laser radiation when open. Do not stare into the beam, do not view directly with optical instruments, and avoid direct exposure to the beam. (C030)

Power and cabling information for NEBS (Network Equipment-Building System) GR-1089-CORE

The following comments apply to the IBM System i models that have been designated as conforming to NEBS (Network Equipment-Building System) GR-1089-CORE:

The equipment is suitable for installation in the following:

- Network telecommunications facilities
- Locations where the NEC (National Electrical Code) applies

The intrabuilding ports of this equipment are suitable for connection to intrabuilding or unexposed wiring or cabling only. The intrabuilding ports of this equipment *must not* be metallically connected to the interfaces that connect to the OSP (outside plant) or its wiring. These interfaces are designed for use as intrabuilding interfaces only (Type 2 or Type 4 ports as described in GR-1089-CORE) and require isolation from the exposed OSP cabling. The addition of primary protectors is not sufficient protection to connect these interfaces metallically to OSP wiring.

Note: All Ethernet cables must be shielded and grounded at both ends.

The ac-powered system does not require the use of an external surge protection device (SPD).

The dc-powered system employs an isolated DC return (DC-I) design. The DC battery return terminal *shall not* be connected to the chassis or frame ground.

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 recomienda a los propietarios de equipos de tecnología de la información (TI) que reciclen responsablemente sus equipos cuando éstos 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.

EU Only

Note: 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.

Battery return program

This product may contain sealed lead acid, nickel cadmium, nickel metal hydride, lithium, or lithium ion battery. 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.

For Taiwan: Please recycle batteries.

For the European Union:

Note: This mark applies only to countries within the European Union (EU).

Batteries or packaging for batteries are labeled in accordance with European Directive 2006/66/EC concerning batteries and accumulators and waste batteries and accumulators. The Directive determines the framework for the return and recycling of used batteries and accumulators as applicable throughout the European Union. This label is applied to various batteries to indicate that the battery is not to be thrown away, but rather reclaimed upon end of life per this Directive.

In accordance with the European Directive 2006/66/EC, batteries and accumulators are labeled to indicate that they are to be collected separately and recycled at end of life. The label on the battery may also include a chemical symbol for the metal concerned in the battery (Pb for lead, Hg for mercury and Cd for cadmium). Users of batteries and accumulators must not dispose of batteries and accumulators as unsorted municipal waste, but use the collection framework available to customers for the return, recycling, and treatment of batteries and accumulators. Customer participation is important to minimize any potential effects of batteries and accumulators on the environment and human health due to the potential presence of hazardous substances. For proper collection and treatment, contact your local IBM representative.

For California: Perchlorate Material - special handling may apply. See 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 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.

About this publication

This topic provides users with instructions on setting up the Operations Console, as well as for managing the console once it is configured. This topic also provides instructions for troubleshooting Operations Console problems.

For information about the accessibility features of this product, for users who have a physical disability, see "Accessibility features," on page 111.

Managing Operations Console

Operations Console is an installable component of iSeries® Access for Windows®. It allows you to use one or more PCs to access and control, either remotely or locally, console and control panel functions.

You can use Operations Console to manage i5/OS® in a partitioned or nonpartitioned environment. In a partitioned environment, you might want to use the Hardware Management Console (HMC) or the Advanced System Management Interface (ASMI) to access your hardware. If you plan to use Operations Console to manage a 270 or 8*xx* server, see the Operations Console information in the IBM i5/OS Information Center Web site at http://publib.boulder.ibm.com/iseries/ .

Operations Console uses 5250 emulation provided by either iSeries Access for Windows or IBM Personal Communications to emulate a console. To emulate a server control panel, Operations Console provides a graphical remote control panel or virtual control panel. Operations Console can use a local console on a network (LAN) or direct cable attachment to enable communications between a server and a PC.

Operations Console works well when the system has several partitions and requires high availability. In this type of environment, the HMC can be overwhelmed by multiple console windows. The Operations Console is able to distribute the consoles for these partitions over multiple PCs. If a problem occurs with Operations Console or console-related hardware, the HMC can be made the backup console and requires no extra effort to quickly retrieve a console.

Related concepts

Managing your server using the Hardware Management Console

Managing your server using the Advanced System Management Interface

Operations Console

PDF file for Capacity on Demand

You can view and print a PDF file of this information.

To view or download the PDF version of this document, select Capacity on Demand (about 730 KB).

You can also view or download these related topics:

- The System i and System p Operations Guide for the Hardware Management Console and Managed Systems Version 7 Release 3.1.0 contains information about the HMC Version 7 or greater.
- The Resource Link™ Web site at http://www.ibm.com/servers/resourcelink contains the complete POWER6 library.

The following topics contain information about the HMC Version 6 or lower:

- Managing your server using the Hardware Management Console (about 750 KB) contains information about how to manage your server using the HMC.
- Partitioning for AIX® (about 330 KB)
- Partitioning for Linux® (about 700 KB)
- Partitioning for i5/OS (about 960 KB)

Saving PDF files

To save a PDF on your workstation for viewing or printing:

1. Right-click the PDF link in your browser.
2. Click the option that saves the PDF locally.
3. Navigate to the directory in which you want to save the PDF.
4. Click **Save**.

Downloading Adobe Reader

You need Adobe Reader installed on your system to view or print these PDFs. You can download a free copy from the Adobe Web site (www.adobe.com/products/acrobat/readstep2.html)  .

Types of Operations Consoles

Review the types of consoles and connectivity options available to you, along with each option's advantages and disadvantages.

Depending on your environment, one connectivity option might work better than another. Review the following advantages and disadvantages of each Operations Console type and choose the best option for you.

"Local console directly attached to the server"
A local console directly attached to the server is a local PC installed with Operations Console that is directly attached to the server over an Operations Console cable.

"Local console on a network (LAN)" on page 3
A local console on a network (LAN) is a local PC installed with Operations Console that is indirectly connected to the server over a network.

Local console directly attached to the server

A local PC installed with Operations Console that is directly attached to the server over an Operations Console cable.

Use this type of connection if you need one console and are providing physical security for access to the console to manage your server. The following table lists some advantages and disadvantages for using this type of connection.

Table 1. Advantages and disadvantages: Local console directly attached to the server

Advantages	Disadvantages
• The administrator will have access to his console in the event of a network failure. With a local console on a network (LAN), a network failure will cause you to lose the ability to access your console. • You can use this PC to become the system console, to perform control panel functions, or both, provided that you have a virtual control panel connection (or LAN-like configuration supporting the remote control panel). For more information about the remote control panel, see Remote and virtual control panels. • The console can be securely placed behind locked doors in the server room.	• You must be located near the server to manage or access the console. • An Operations Console cable is required to support the Operations Console function. Remote control panel support must be provided using a method other than a direct cable. • This configuration does not support remote connections. • Only one local console that is directly attached is allowed per PC and per server or partition.

Local console on a network (LAN)

A local PC installed with Operations Console that is indirectly connected to the server over a network.

Use this type of connection if you need to manage multiple servers or partitions from one console and you have a secured network that you can configure your console on.

Table 2. Advantages and disadvantages: Local console on a network (LAN)

Advantages	Disadvantages
• You can configure a single PC to be the console for several different servers or partitions as long as they are connected to the network. • The administrator will not need to be located near the server to manage Operations Console. • Security features are available to protect your Operations Console connections. • Multiple PCs can be configured as the Operations Console to a server or partition, but only one can be active at a time.	• No console is available in the event that a network failure occurs unless a backup console is in place. It is recommended that you configure a local console that is directly attached, a twinaxial console, or HMC (if installed) for backup. For more information on the backup console, see Backup console for i5/OS. • Your server will need a separate LAN card to be used by Operations Console or other service tools. For more information on the hardware requirements, see Operations Console hardware requirements.

Related concepts

Remote and virtual control panels

Backup console for i5/OS

Related reference

Operations Console hardware requirements

Planning for your Operations Console configuration

Important planning considerations must be made to accommodate for an Operations Console for one or more servers. If you plan ahead, you can include additional features in your configuration.

General Operations Console considerations

Whether or not you have an HMC, there are several important items to consider when planning to use Operations Console for one or more servers.

Important: IBM System i models start counting logical partitions with the number 1 (even if it is the only partition) instead of a 0. For the console to connect correctly, your logical partitions must also begin numbering at 1 instead of 0. This is especially true if you rely on the BOOTP process to configure the server with its network data.

Read through the following considerations specifically for servers with and without a Hardware Management Console (HMC), and then the considerations for all servers.

Servers without an HMC

- Operations Console now defaults the first embedded Ethernet port as the default console port in systems not using an HMC. This includes the 5706/5707 adapters. However, the server will not check for the 5706/5707 adapter unless support for the default embedded Ethernet port has been disabled. Support for the default embedded Ethernet port is disabled in manufacturing for systems where the embedded ports do not exist, for example, the 9406-595. To disable support for the default embedded Ethernet port or 5706/5707 adapters, see Disabling support for the default embedded Ethernet port or 5706/5707 adapters.To disable support for the default embedded Ethernet port or 5706/5707 adapters, see “Disabling support for the default embedded Ethernet port or 5706/5707 adapters” on page 48.

- Servers without an HMC, and without an enabled embedded Ethernet port, will use the location of the console's adapter to determine the eligibility for a console. For more information, see "Systems without an HMC determine the console by adapter location" on page 5.
- Multiple console-supporting adapters on servers without an HMC, and without an enabled embedded Ethernet port, might interfere with console selection. For more information, see "Multiple console-capable adapters on systems without an HMC" on page 5.
- On servers without an HMC, when a LAN adapter is available for use as a console when another console connectivity (directly attached, for example) has been configured by location, and it has a valid configuration, then the system will activate this adapter for console or service tools server usage. For more information, see "Adapter activation when multiple console types are available" on page 5.
- If you have an IBM System i5® or eServer™ i5 520, 525, or 515 model, your system can have asynchronous adapters located in multiple slots simultaneously, including locating the 2793 asynchronous adapter in slot C4. This is possible only for systems that are not managed by an HMC and have an input/output adapter (IOA) that does not require an input/output processor (IOP). For more information, see "Selecting an individual asynchronous adapter location" on page 6.

Servers with an HMC

- Only an IOA can be tagged for console with an HMC. For more information, see "Tagging an IOA for console with an HMC" on page 6.
- Partitions require the **console** tag.
  - Operations Console (LAN) only requires the IOA tag for the **console** option in a profile of a partition.
  - Operations Console (Direct) requires both the **console** tag and the **Operations Console** tag to be specified. For more information, see "Tagging logical partitions for console with an HMC" on page 6.
- The **Operations Console** tag requires an IOA to be specified if you are using a directly connected console or a remote service connection. For more information, see "Tagging an IOA for console and Operations Console with an HMC" on page 6.

All servers

- The PCI 1 Gbps Ethernet TX IOA (5706), and PCI 1 Gbps Ethernet SX IOA (5707) do not require an IOP and are available for use with the Operations Console. For more information about these adapters, see "5706/5707 adapters" on page 7.
- The 2793 and 2742 asynchronous communications adapters no longer require an IOP.
- The PCI 1 Gbps Ethernet TX IOA (5706) and PCI 1 Gbps Ethernet SX IOA (5707) do not require an IOP and are available for use with the Operations Console. For more information about these adapters, see "5706/5707 adapters" on page 7.
- Only the configured console type is supported. For more information, see "Configured console type" on page 7.
- A dedicated adapter resource is no longer required to support a console. For more information, see "Dedicated adapter resource" on page 7.
- Do not place the console adapter with the same IOP that supports storage devices, if possible. For more information, see "Console adapter placement" on page 8.
- When planning for multiple LAN-connected PCs, designate one PC to be used as the console to your server or partition during a recovery installation. For more information, see "Designating a PC for recovery installations" on page 8.
- The alternate console is only relevant when the primary console is a twinaxial console. For more information, see "Alternate console" on page 8.
- The service tools server interface is automatically configured when Operations Console (LAN) is configured. For more information, see "Service tools server and Operations Console (LAN)" on page 8.

- Only Operations Console (LAN) can perform a takeover. For more information, see “Performing a takeover” on page 8.
- When Operations Console (LAN) is used in an environment with multiple LAN-connected PCs attempting to connect at the same time, the first successful connection will be the console. For more information, see “Multiple PCs connecting at the same time” on page 9.
- Coexistence between console types is allowed. For more information, see “Coexistence with multiple console types” on page 9.
- A maximum of 26 emulator sessions is available for each PC. For more information, see “Maximum active emulator sessions available for each PC” on page 9.
- Multiple consoles and multiple servers can be used. For more information, see “Multiple consoles and multiple servers” on page 9.
- Console activation is determined differently in D-mode. For more information, see “Console activation in D-mode” on page 10.

Systems without an HMC determine the console by adapter location

When a server is not managed by an HMC, and the embedded Ethernet port is disabled, the console-supporting hardware is required to be located in specific slot locations based on the server model. For Operations Console (LAN), there might be more than one location that can support a console. When more than one location is available for a server model, the locations are listed from highest priority to lowest priority when the console searches for console-capable hardware resources.

The console service functions (65+21) and the OPSCONSOLE macro have support to designate a particular adapter.

Also, the 5706/5707, 2793, or 2742 adapters are able to run without an IOP. If you do not want to use a 5706/5707 adapter for the console, you can disable this option by following the steps in ″Disabling support for the default embedded Ethernet port or 5706/5707 adapter″. You can also use the OPSCONSOLE macro or the console service functions (65+21) to disable this support. For more information on either of these options, see ″Using the OPSCONSOLE macro″ or ″Using the console service functions (65+21)″.

Multiple console-capable adapters on systems without an HMC

Multiple IOPs capable of supporting a console workstation can interfere with the selection of the LAN adapter that you want. Consider the following:

- The server attempts to use the first, or only, console IOA based on the current console type value.
- If your server model supports a second adapter location for LAN and has a LAN adapter installed, a problem with the first adapter might cause the server to use the second LAN adapter for the console, making it unavailable for use by i5/OS.

The console service functions (65+21) and the OPSCONSOLE macro have support to designate a particular adapter which solves these issues.

Adapter activation when multiple console types are available

When a server is not managed by an HMC, it is possible to have more than one console adapter available for activation. For example, the console type is set for Operations Console (LAN) and has a device connected that is the system console. If an Operations Console (Direct) adapter is also activated, the corresponding device can also connect at the same time. However, this device cannot become the console and only displays the Console Information Status window. Each of the adapters are dedicated to their designated function and are not available for use in i5/OS.

The console service functions (65+21) and the OPSCONSOLE macro have support to designate a particular adapter which solves these issues.

Selecting an individual asynchronous adapter location

If you have an IBM System i5 or eServer i5 520, 525, or 515 model, your system can have asynchronous adapters located in multiple slots simultaneously, including locating the 2793 asynchronous adapter in slot C4. Slot C4 allows an IOA that does not require an IOP. This is possible only for systems that are not managed by an HMC and have an input/output adapter (IOA) that does not require an input/output processor (IOP). For more information, see "Selecting an individual asynchronous adapter location."

You are able to select an individual asynchronous adapter for use with the console and remote service by using either a native macro or the console service functions (65+21). The console and remote service functions must all remain on a single asynchronous adapter. If you have a system that was shipped with Licensed Internal Code (LIC) prior to V5R4M5, you cannot select slot C4 for use with the console when using the 2793, but you can select slot C4 for use with remote service.

There is function to specify an external network (LAN) adapter when more than one may be eligible to support a console. This function is not available when the system is managed by an HMC or the embedded port is enabled.

Example: If you have an asynchronous adapter located in both C2 and C3 for use by Operations Console (Direct), you can choose to use either slot for console and remote service, without having to remove the asynchronous adapter from the other slot.

Tagging an IOA for console with an HMC

IBM System i5 and eServer i5 models with an HMC support tagging only at an IOA level. The advantage of this is you can specify the specific adapter to use for your console. If you need to change the console type, you can make the change without an IPL in most cases. For more information about how to change the console, see Changing consoles, interfaces, and terminals.

For more information about making console type changes without an IPL, see Changing console tags without an IPL.

Tagging logical partitions for console with an HMC

Consider the following when determining what to tag for Operations Console:

Operations Console (LAN)
If you use a LAN-based PC for your console, the only tag you need to set is for **console**.

Operations Console (Direct)
If you use a direct cable attached PC for your console, you need to specify the tag for **console** and **Operations Console**. The **Operations Console** tag is the equivalent of the former Electronic Customer Support (ECS) tag.

Tagging an IOA for console and Operations Console with an HMC

The **console** tag requires an IOA to be specified. The **Operations Console** tag is required if you are using a directly connected console, if you are configuring for a directly connected backup console, or if you are using an asynchronous communications adapter for remote service. Tagging the IOA allows you to select the specific adapter used for the Operations Console. Therefore, if multiple console-capable adapters exist in the IOP, only the selected console-capable adapter is used for the console. Tagging the IOA automatically sets the console type during the next activation following the partition profile update. An IPL will not read the changed partition profile.

You can use the HMC command window to specify the tag. This allows the change to be used immediately, although you might have to force the system to determine the new console in some instances. This can be performed using the same command window, using the OPSCONSOLE macro, or using the console service functions (65+21). For more information on how to change the console, see Changing consoles, interfaces, and terminals.

For more information about making console type changes without an IPL, see Changing console tags without an IPL.

5706/5707 adapters

The 5706/5707 adapters do not require an IOP and are supported with an Operations Console. When using these adapters, you can locate the LAN adapters in any of the remaining slots, specific to the adapter, on your server if your server supports this type of operation and is managed by an HMC. If the system is *not* managed by an HMC, the 5706/5707 LAN adapter must be located in one of the designated card locations that supports a local console on a network (LAN). Only the first port of this adapter can be used for the console. If you elect to use this adapter instead of the default embedded Ethernet port, you must disable the embedded port before the system can use the adapter. To disable support for the default embedded Ethernet port, see "Disabling support for the default embedded Ethernet port or 5706/5707 adapters" on page 48.

Configured console type

If no console type is specified, such as when a new partition is being created, the supporting hardware tagged by the HMC is used. If there is no HMC, then the console is determined by any eligible adapters by location. If more than one eligible adapter is found, then the first connected device determines the console.

In the case of a server without an HMC, then the console is determined by any eligible adapters by location. If more than one eligible adapter is found, then the first connected device determines the console. In the case of a server without an HMC, for example, if you use Operations Console (Direct) and you have a LAN adapter that is available to support a console, and has a valid configuration, then the console is the directly attached PC. However, the LAN adapter is started at IPL time and the connecting PC, one or multiple, displays the Console Information Status window. The option to take over the console displays NO and the message at the bottom of the screen indicates that this device is not the supported console type. The console service functions (65+21) and the OPSCONSOLE macro have support to designate a particular adapter which solves these issues.

Dedicated adapter resource

The service interface is a single adapter used for service tools. For a local console that is directly attached, if there is no network adapter selected, either by location or partition tagging, then this is the service interface. More commonly it is a network adapter to support either a local console on a network or the service tools server. In the case where there is a valid network adapter available, even if another console is selected and there is a valid service host name associated with the adapter, then this is the service interface. It can support a console, the service tools server, or both.

Occasionally the console is not connected using this network adapter, but the service tools server is configured to support the iSeries Navigator interface for hard disk drive configuration or similar functions. With i5/OS Version 6 Release 1, the service interface can be shared with an i5/OS line description, thus sharing the same interface. This works only when the 5706/5707 is supporting the service interface. It is possible to have a local console that is directly attached using a 2793 adapter, for example, and a 2849 network adapter configured for service tools server. Each adapter is dedicated to support its respective function and is not available in i5/OS.

Console adapter placement

Do not place your console adapter on the same IOP as storage devices. Having a dedicated IOP for the console adapter and one for the storage devices reduces possible connectivity problems. For example, during very heavy usage of storage devices, the console might appear to stop working temporarily. If this happens, it should resume operation shortly. If you must place the console adapter on shared resources, keep the other usages to a minimum for better console reliability. Also, enable the console option, **Allow console recovery and console can be taken over by another console** so the console automatically reconnects.

Designating a PC for recovery installations

By default, a system running i5/OS Version 6 Release 1 automatically manages service tools device IDs. The default number of service tools device IDs to be managed is 11, QCONSOLE plus ten automatically created service tools device IDs. Any recovery involving distribution media from IBM might reset the value to 10 in rare cases. You no longer need to know which PC is using the QCONSOLE service tools device ID.

Alternate console

In a partitioned environment, *alternate console* refers to a twinaxial console connected to a different IOA or IOP that is tagged as the alternate console. The **console** tag must also specify a twinaxial console. An alternative console gives you an added layer of protection because if the system detects a failure of the primary console during an attended IPL, it automatically tries the alternate console's tagged resource. It is important to remember that tagging the same resource as the console and alternate console can result in an inability to select a console at all. For more information on using Operations Console as a console in the event that a twinaxial console is not available, see Backup console for i5/OS.

Service tools server and Operations Console (LAN)

If you use Operations Console (LAN), you must create a service host name (interface). After this is created, the server is also ready to use the service tools server to support, for example, iSeries Navigator functions. However, you can have a network adapter for the service tools server when the console is something other than Operations Console (LAN). To do this, you need to configure the service host name (interface) so that the service tools server uses that connection. With a configured network adapter available at IPL, the system activates the adapter that supports the console, but also activates the adapter used for the service host name, if different. In this scenario, you now have two resources in your system that might not be used by i5/OS, depending on your hardware. Conversely, if you previously had a service host name for iSeries Navigator and are now using Operations Console (LAN), you do not have to make any IP configuration changes because the same resource is used.

Note: If you do not use Operations Console (LAN) as your console, you might have to temporarily change the console type value and **console** tag to configure a LAN adapter for use as the service tools server. After the configuration is complete, you are able to revert the console type value and any tagging back to the original values.

For more information about making console type changes without an IPL, see Changing console tags without an IPL.

Performing a takeover

The console takeover and recovery function allows one local console on a network (LAN) to take control of the server from another local console on a network (LAN). This basic function is not available for any other console type. However, with this option there is also some recoverability. The HMC has the ability to share a console connection but does not actually perform the takeover. For more information, see Console takeover and recovery.

Multiple PCs connecting at the same time

If you use Operations Console (LAN) with multiple PCs configured to become the console, all of these PCs are actively connected at IPL time. There is no way to know which PC will become the console because the first one connected will be the active console. If you enabled the console option, **Allow console recovery and console can be taken over by another console**, then you are able to take over the console at the PC you want to use.

Coexistence with multiple console types

Operations Console, both directly attached to the server and on a network (LAN), HMC, and twinaxial workstations, can coexist as console-capable devices if you remember the following rules:

- Only one device can be active at a time.
- A twinaxial workstation on any twinaxial workstation controller with port 0 (address 0 or 1) or port 1 (address 0 or 1) can become a console device if twinaxial console is selected. If twinaxial console is selected as the console type, then Operations Console devices might not be started. If there is a configured service host name, for example, to support iSeries Navigator, then the system activates the supporting adapter in addition to the twinaxial adapter.
- If you use Operations Console (LAN) for the console, but you have an eligible asynchronous communications adapter available as a backup, then the LAN adapter is activated to support the console. The asynchronous communications adapter does not automatically get started since the console type value is not set for its use at this time. However, because it is eligible to support the console, assuming the **Operations Console** tag is set, then i5/OS cannot use this resource.

Maximum active emulator sessions available for each PC

The maximum number of active emulator sessions available for each PC is 26. Active emulator sessions are identified by a single letter of the English alphabet (A through Z). You can have more than 26 configured connections, but only 26 of those sessions can be active. During the course of using these connections, you can close the emulator for a connected configuration to free up an emulator identifier. The next emulation session started can then use that identifier.

Another limitation for having multiple connected emulators on the same PC is the amount of available PC resources, memory and video capability, to support a large number of connections. Since each connection and associated functions (console, control panel, or both) will use PC resources, you might need to add more memory to support more connected sessions. Each PC's hardware, operating system, and active programs vary so that there is no clear way to identify in advance how many sessions your particular usage supports.

Multiple consoles and multiple servers

Consider the following when considering multiple consoles and multiple servers:

Local console on a network (LAN)

Operations Console allows multiple LAN connections to a single server, but only one 5250 session can have control of the server at a time. An active console is a command interface to a server (5250 emulation) that is currently interacting with the server. More than one Operations Console device can have data on the screen, but only one is truly active.

A single PC can have multiple active connections to one or more servers or partitions.

Local console directly attached

The client (PC) only supports one local console that is directly attached for a single PC.

The server only supports a single incoming directly attached connection.

You can mix both types, LAN and direct, at the same time on the same PC if you follow the preceding guidelines.

Console activation in D-mode

Consider the following based on your server's configuration:

Servers without an HMC

The only scenario where the value is not set is after a load-source hard-disk-drive replacement without a good copy from old to new. If this is the case, then all eligible adapters, by location, can support a console, except LAN. If LAN is the only available connectivity and the restoration media is not a SAVSYS, then you might need to use the control panel to perform the console service functions (65+21) to change the console type value. For more information on how to use the console service functions, see Using the console service functions (65+21).

Logical partitions

When a logical partition is initially set up, you have to tag an IOA for **console** and in the case of local consoles that are directly attached, the **Operations Console** tag. The system uses this information to search for a console. Only this resource is activated and the system uses the first connected device as the console to restore the Licensed Internal Code (LIC). The data used to restore the LIC determines if you need to set the console type value following the restoration of the code. You can also get a display asking for confirmation for selecting the console type value. If needed, you can use this console to change to another console.

If the console fails to connect, you can use the HMC command window to tag another resource and then use the console service functions (65+21) to specify a different console type value, if needed. For more information on how to use the console service functions, see Using the console service functions (65+21).

Related concepts

Using the console service functions (65+21)

Changing consoles, interfaces, and terminals

Changing console tags without an IPL

Backup console for i5/OS

Console takeover and recovery

Related tasks

Disabling support for the default embedded Ethernet port or 5706/5707

Using the OPSCONSOLE macro

Backup console for i5/OS

To quickly recover from the unexpected loss of the console that manages i5/OS, you might want to consider a backup console. Many system plans include a level of redundancy to allow for hardware failures, but some do not consider the console in those plans.

Here are some suggestions for planning for a backup console to manage i5/OS:

Considerations for a backup console

- The adapter location for Operations Console or a twinaxial console is fixed, or at least limited for some nonpartitioned systems. Based on your system's hardware requirements you might have limited console choices for i5/OS. Try to accommodate at least one additional console type, if possible.
- Consider using the takeover and recovery function as part of your i5/OS backup console strategy. However, the hardware used for the Operations Console or twinaxial console must be installed prior to the recovery. For more information on the general Operations Console consideration, see General Operations Console considerations.
- *Alternate console* refers to a twinaxial console resource tagged as the alternate console when the console is also a twinaxial console. An alternate console gives you an added layer of protection because if the

system detects a failure of the primary console during an attended mode initial program load (IPL), it automatically tries the alternate console. Tagging the same resource as both the console and the alternate console can result in an inability to select a console at all. Consider specifying the alternate console by tagging an input/output adapter (IOA) on a different bus in case you develop a bus-related problem.

- Systems using a Hardware Management Console (HMC) enable you to tag a specific IOA as the console device. For more information, see General Operations Console considerations.
- On large multi-partitioned systems or high-availability systems, use Operations Console (LAN) as the system console for each system or partition. In the event of a console failure, you can switch to the HMC 5250 console without having to verify you have additional hardware in place. Most changes of a console to HMC are performed without the need for an IPL.

Related information

- "General Operations Console considerations" on page 3

Verify your system is ready for a backup console

Recovering from the loss of a console depends on many factors, some of which include the model, the hardware resources available, the previous console type, and the intended console type. Recovery might consist of repairing the currently failed console or temporarily replacing it with another console type. Most changes of a console type can be performed without the need for an IPL, but there might be circumstances in which an IPL is necessary. Before you use the console service functions (65+21), verify the following:

- For systems without an HMC, verify that the console hardware is installed and available.
- For systems with an HMC, verify that the appropriate console resources are tagged in the partition profile.

If you plan to use a local console on a network (LAN) as a backup for another console type, the network adapter must be located in a slot designated for a console or the IOA is tagged correctly. If not previously configured, you can use BOOTP to configure the server. For more information on BOOTP, see Operations Console networking and Creating or verifying a service host name (interface name).

Possible backup console configurations

It is important to consider as much redundancy as possible for your console needs. If you consider "what if this fails?" and you have another method to provide a console, and also make compromises for the hardware requirements necessary to overcome the various levels where a failure might occur, you are reducing your exposure to an unrecoverable console failure condition.

Several backup console configurations can fit your environment. The following table lists possible solutions.

Table 3. Possible backup console configurations

If...	Then...
If your server is accessed remotely...	consider an off-site console capability or another connectivity for the console. A local console on a network (LAN) can be backed up with additional local console on a network (LAN) PCs. If the network adapter were to fail, consider a local console that is directly attached as a backup console.
If your system is configured with an HMC, but you are running Operations Console...	you can quickly switch to the HMC 5250 console if Operations Console fails, without having to change hardware. **Remember:** You must configure each console separately.

Table 3. Possible backup console configurations (continued)

If...	Then...
If you are using multiple local consoles on a network (LAN) on a single PC...	• consider additional PCs using this same type of configuration. **Important:** The PC resources can become overwhelmed when supporting multiple consoles and remote control panels. • consider setting up a local console that is directly attached on a PC and place it on a roll-away cart with a console cable. If you have supporting adapters, you can quickly roll the cart with the PC near the server or logical partition in need of the console. After connecting the cable and changing the console type value, you have a console to replace the currently failed console. This same concept can be implemented for twinaxial workstations.
If you are using multiple local consoles on a network (LAN) on multiple PCs...	• consider assigning each PC a core set of console responsibilities and then overlap coverage of backup configurations with each other. For example, if you have a PC that supports 10 local consoles on a network (LAN) and another PC with the same number of primary consoles for another 10 logical partitions, instead of backing up each PC with the other's configuration, you add a third PC and distribute the 20 consoles so that two PCs back up a portion of each PC's primary console configurations. • consider having a dedicated PC to be the backup of a certain number of consoles, but not connect it until necessary.

Note: If more than one local console on a network (LAN) is planned, you no longer need to create additional service tools device IDs on the server before you start configuring the Operations Console PC. Each PC connecting to the same target server or logical partition must have a unique service tools device ID and will be given an autocreated service tools device ID upon connecting.

For more information about the ability to switch between console devices, see Switching from one console type to another when a console is currently available.

Related concepts

General Operations Console considerations

Using the console service functions (65+21)

Operations Console networking

Related tasks

Creating or verifying a service host name (interface name)

Related reference

Switching from one console type to another when a console is currently available

Console takeover and recovery

Learn about the benefits of the console takeover and recovery function included in i5/OS, which allows an Operations Console to take control from another console device.

Takeover

The process used for a LAN-connected, console-capable device to take control from the current LAN-connected console device. This takeover action cannot be used with local consoles that are directly attached or any other console type such as the twinaxial console.

Recovery

The process of regaining control of the job running on the console after a problem with the console is encountered. The recovery process might be to the same console device or a different console-capable device, and might require additional work to enable a device using a different connectivity, except a twinaxial console. The recovery function remains running as if nothing has happened. The twinaxial console uses a different type of 5250 emulation so even though you can use it to recover with, there is loss of data in the process.

Benefits of these functions include convenience and redundancy. Console-capable devices can be placed around a site, or multiple sites, allowing users to move around and gain control of the system from any of these devices. Whatever the previous console's activity was, the new console is at the identical place, even during the process of restarting the server or installing i5/OS. When the console option for takeover is enabled, the server also has enhanced recoverability from a loss of the console.

Related concepts

Working with console takeover and recovery

Operations Console hardware requirements

For correct Operations Console configurations, verify that you have satisfied the server, adapter, cable, and PC requirements.

Important: IBM System i5 and eServer i5 models start counting logical partitions with the number 1 (even if it is the only partition) instead of a 0. For the console to connect correctly, your logical partitions must also begin numbering at 1 instead of 0. This is especially true if you rely on the BOOTP process to configure the server with its network data.

Operations Console default console port when not using an HMC

Operations Console defaults to the first embedded Ethernet port as the default console port in systems not using a Hardware Management Console (HMC). This includes the 5706/5707 adapters. However, the server will not check for the 5706/5707 adapter unless support for the default embedded Ethernet port has been disabled. Support for the default embedded Ethernet port is disabled in manufacturing for systems where the embedded ports do not exist, for example, the 9406-595. To disable support for the default embedded Ethernet port or 5706/5707 adapters, see Disabling support for the default embedded Ethernet port or 5706/5707 adapters.

Adapter requirements

You must install an adapter for Operations Console in all of the following situations:

- You want to use a local console on a network (LAN) and have elected to disable support for the default embedded Ethernet port
- You have a system where the embedded ports do not exist
- You want to use a local console that is directly attached

Operations Console supports the following adapters:

- Operations Console (LAN): 2744, 2838, 2849, and 5706/5707 (IOP-less)

  Note: The 2744 and 2849 adapters require an input/output processor (IOP) and can be located only in an expansion unit.
- Operations Console (direct): 2742 (IOP-less), 2793/2794 (IOP-less), 4745, and 9771

The adapter locations pertain to servers *without* an HMC. Using an HMC to manage the server excludes using adapters by location. Instead, you should use the HMC to designate hardware resources.

Important: If you are running Licensed Internal Code (LIC) prior to V5R4M5 and you want to move the 2793/2794 asynchronous adapter from its manufacturing default location to use Operations Console (direct), you must also use the console service functions (65+21) or the OPSCONSOLE macro to select an individual asynchronous adapter for use with the console. For more information, see Using the console service functions (65+21) or Using the OPSCONSOLE macro.

Table 4. Operations Console adapter requirements

	Operations Console (LAN)	**Operations Console (direct)**	
Model	**LAN adapter locations**	**Asynchronous adapter locations**	**Notes**
520, 525, and 515	C2 or C5 disable support for the default embedded Ethernet port or 5706/5707 adapters. If you use C2 or C5, you must disable support for the default embedded Ethernet port or 5706/5707 adapters. See Note 2 on page 15 and 3 on page 15 below.	C2 or C3 C4 is also available. Refer to Note 1 on page 15 below. The system can have asynchronous adapters located in multiple slots simultaneously. Refer to Note 1 on page 15 below.	If your LAN adapter is located in C2, then the IOP must be located in C1. If your LAN adapter is located in C5, then the IOP must be located in C3 or C6. If your asynchronous adapter is located in C2, the IOP must be located in C1. If your asynchronous adapter is located in C3, the IOP must be located in C6. If an IXS is installed, it must be located in C5/C6, the LAN adapter or asynchronous adapter must be located in C2, and the IOP must be located in C1, if needed.
550	C4	C2 or C5 The system cannot have asynchronous adapters located in both slots simultaneously.	When your LAN adapter is located in C4, the IOP can be located in C3 or C5 (except when an IXS is installed). If your asynchronous adapter is located in C2, the IOP must be located in C1 (except when an IXS is installed). If an IXS is installed, it must be located in C2/C3, the asynchronous adapter must be located in C5, and the IOP can be located in C1 or C4, if needed. Console support using a LAN connection is provided by the embedded port only.
570	C4 or C6	C2	When your LAN adapter is located in C4 or C6, the IOP must be located in C3 (when using an IOP-driven IOA). When your asynchronous adapter is located in C2, the IOP must be located in C1. If an IXS is installed, it can be located in C4/C5, the LAN adaptor or asynchronous adapter can be located in C6, and the IOP can be located in C3, if needed. If there are multiple CECs, the CEC with the load source DASD is used for console support.
595			This model requires an HMC. Tagging the desired IOA directly is used to specify the console instead of by card location.

Notes:

1. This note applies to the IBM System i5 520, 525, and 515 models that are not managed by an HMC and have an IOA that does not require an IOP. For the 520, you can install PTF MF39303 (V5R3M5) or PTF MF39304 (V5R4M0) so that your system can have asynchronous adapters located in multiple slots simultaneously, including locating the 2793 asynchronous adapter in slot C4. Slot C4 allows an IOA that does not require an IOP. For the 525 and 515, these PTFs should already be installed.

   With these PTFs, you are able to select an individual asynchronous adapter for use with the console and remote service by using either a native macro or the console service functions (65+21). The console and remote service functions must all remain on a single asynchronous adapter. If you have a system that was shipped with Licensed Internal Code (LIC) prior to V5R4M5, you cannot select slot C4 for use with the console when using the 2793, but you can select slot C4 for use with remote service.

   Example: If you have an asynchronous adapter located in both C2 and C3 for use by Operations Console (direct), you can choose to use either slot for console and remote service, without having to remove the asynchronous adapter from the other slot.
2. If you are using i5/OS Version 5 Release 4 Modification 5 or later, both network (LAN) and asynchronous communications adapters can be individually selected using the OPSCONSOLE macro or console service functions (65+21).
3. If you plan to use a 5706/5707 adapter in a card slot, you must disable support for the embedded Ethernet port by using the OPSCONSOLE macro or console service functions (65+21).

For more information about adapters, see Configuration tables for IBM System i5 and eServer i5 system units and expansion units.

These systems do not support a remote control panel directly attached to the server. However, you can use the virtual control panel or the remote control panel connected over LAN for most control panel functions. For more information, see Remote and virtual control panels.

Operations Console (direct) cable requirements

To connect your local console that is directly attached, you must use the correct cable, 97H7557 or 39J5835. The 39J5835 cable complies with the European Union Directive 2002/95/EC on the Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment. For more information, see Installing an Operations Console cable.

Related information: “Step 1. Cabling the Operations Console to your server” on page 33

Operations Console (direct) PC communications port requirement

To use the configuration wizard to configure Operations Console (direct) successfully, you must verify that you have an available communications port. You will need a connector for a serial port communications interface. Operations Console supports serial COM ports 1-9. One COM port is required for system console support.

Notes:

- Operations Console does not use any embedded serial ports located on the server.
- These systems do not support a remote control panel directly attached to the server. For other connectivity options, see Remote and virtual control panels.

To check that you have an available communications port, view the documentation for your PC or check with the PC manufacturer. Also, when you configure Operations Console, the wizard searches for a port for the console.

The use of a Universal Serial Bus (USB) to serial port adapter is supported with Operations Console. The adapter is placed at the PC end of the console serial cable and connects to the USB port on the PC. When

installing the USB adapter, follow the manufacturer's instructions. The operating system then assigns a serial port to that adapter, COM 4, for example. This adapter is used exclusively for the console. Operations Console supports serial COM ports 1-9.

Important: The adapter must plug directly into a USB connector on the PC. Neither the use of a USB hub to share connections nor the use of USB extension cables is supported. However, these devices might function correctly in some situations.

If a failure occurs with your adapter, you can try another adapter. You can also contact the manufacturer of the adapter or your PC, or contact your hardware service provider.

Related information: "Remote and virtual control panels" on page 17

PC processor and memory requirements

Use the following table to ensure that your PC is ready for Operations Console. If you are using iSeries Navigator, see Requirements for installing iSeries Navigator. For updated PC requirements, see the iSeries Access for Windows Web site.

Table 5. Processor and memory requirements

Operating System (1,2)	Operations Console PC
Microsoft Windows Vista (Local console on a network (LAN) configuration only)	• Pentium® 800 MHz • 512 MB memory minimum
Microsoft Windows XP Professional	• Pentium 500 MHz (P6 or equivalent compatible microprocessor) • 256 MB memory minimum
Microsoft Windows 2000	• Pentium 500 MHz recommended • 128 MB memory minimum (256 MB recommended)

Related concepts

Using the console service functions (65+21)

Configuration tables for IBM System i5 and eServer i5 system units and expansion units

Remote and virtual control panels

Related tasks

Disabling support for the default embedded Ethernet port or 5706/5707

Using the OPSCONSOLE macro

Installing an Operations Console cable

Related information

Requirements for installing System i Navigator

System i Access

Operations Console software requirements

Review the supported operating systems and other software requirements to correctly run your Operations Console.

Before you continue, verify that you have satisfied the Operations Console hardware requirements according to your intended configuration. Operations Console is supported on Microsoft® Windows Vista, Windows 2000 Professional, and Windows XP Professional.

PC5250 or IBM Personal Communications V5.8 (V5.7 CSD 1 minimum) must be installed for the console only. It is not required for remote control panel only configurations.

Note: If you run any software that enables SOCKS on your PC (the PC accesses the Internet through a firewall, such as Microsoft Proxy Client, Hummingbird SOCKS Client, NEC SOCKS 5, or others), you cannot route the subnet for 192.168.0.0 to the firewall. Operations Console uses addresses in the range of 192.168.0.0 to 192.168.0.255. Incorrect routing causes Operations Console to fail. Check your SOCKS configuration and verify that the entry is:

```
Direct    192.168.0.0    255.255.255.0
```

Use the Operations Console properties window to change the IP base address from 192.168.0.2. For example, you can use 192.168.1.2.

Data encryption for a local console on a network (LAN)

Operations Console network connections use a version of Secure Sockets Layer (SSL), which supports device and user authentication without using certificates. By default, Operations Console uses the strongest encryption possible for authentication and data.

Related concepts

Operations Console properties window

Related reference

Operations Console hardware requirements

Remote and virtual control panels

Learn about your control panel options, see comparisons of the control panels, find setup instructions, and solve problems through troubleshooting.

To make a connection to the control panel, you must configure a remote control panel (RCP) or a virtual control panel (VCP). All user IDs that want access need the appropriate authority, as well as device IDs.

Both RCP and VCP are graphical interfaces to the control panel. The RCP allows you to perform most of the control panel functions from a local or a remote location. The VCP allows you to perform most of the control panel functions from a local location only. By default, user-created user IDs will have these permissions.

The user must be granted access to a partition's RCP and functions to use the RCP or VCP. If a local console on a network is being used, then the service tools device ID must also be granted access to that partition's RCP to use this feature.

Users and service tools device IDs default values automatically grant access to the RCP for the logical partition. The user that authenticates a connection must also have authority to the respective partition's keylock to change the mode.

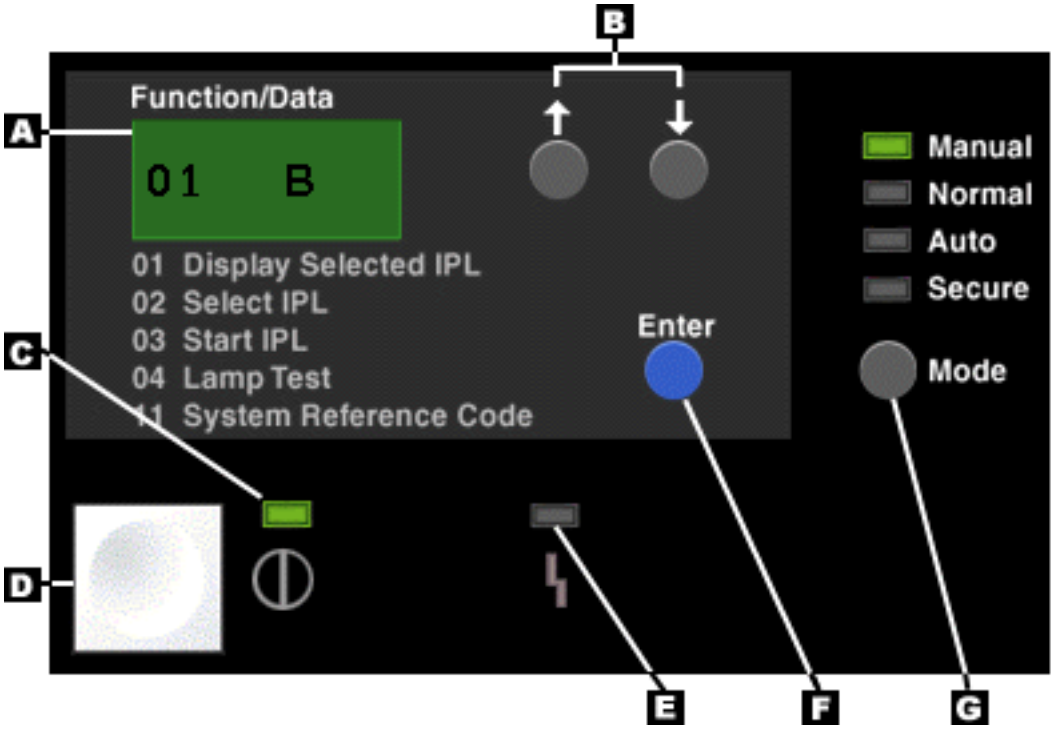


Figure 1. Remote and virtual control panel

A Function/Data display

B Increment and Decrement buttons

C Power on indicator

D Power button

E System Attention light

F Enter button

G Mode button

Remote control panel

Use the IBM i5/OS *remote control panel* to use control panel functions through a PC.

The graphical user interface of the remote control panel looks similar to the physical control panel. The remote control panel (RCP) has the following characteristics:

- The RCP installs through the Operations Console.
- You can use the interface for the RCP to restart and power off the server. It cannot power up the server. You can use the RCP to perform most of the same functions as the physical control panel.
- A directly connected RCP is not supported. RCP connectivity is supported through a local console on a network (LAN-connected RCP) or using the virtual control panel (VCP).

For information about deciding whether the RCP or the VCP will best meet your needs, see Differences between the virtual control panel and remote control panel.

Considerations for the remote control panel

The following information can help you determine the best IBM i5/OS RCP configuration for your environment:

- The local console on a network (LAN) no longer selects the RCP by default. If you want to use the RCP, use **Properties** to select the function.
- You must use a Hardware Management Console (HMC) to manage logical partitions. This means that you cannot use the RCP to activate a logical partition, and you cannot directly connect an RCP cable to the server. To work with logical partitions remotely, you can use the Web-based System Manager Remote Client or the Advanced System Management Interface (ASMI).
- Any configuration where the device ID is not authorized after the first connection will be unavailable or missing.
  - An unavailable configuration was selected but not authorized.
  - A missing configuration was not selected and was not authorized.

  After the configuration is authorized, it is displayed in **Properties** the next time you connect.
- You must be granted access to a logical partition's RCP and functions to use the RCP. If a local console on a network (LAN) is being used, then the service tools device ID must also be granted access to that logical partition's RCP to use this feature. Users and service tools device IDs default values no longer automatically grant access to the RCP for the system or logical partition. You will need to manually grant a user, service tools device ID, or both, access to a system or partition. For details on changing the attribute option, see "Creating service tools device IDs on the server" on page 41. The user that authenticates a connection must also have authority to the respective logical partition's keylock to change the mode.

Related concepts

Installing and securing the remote client

Managing your server using the Advanced System Management Interface (ASMI)

Related reference

Differences between the virtual control panel and remote control panel

Virtual control panel

The IBM i5/OS *virtual control panel* is an alternative to the remote control panel (RCP) on servers that do not support a directly connected RCP and do not have a network adapter. Like the RCP, the virtual control panel (VCP) is a way to use control panel functions through a PC.

The graphical interface for the VCP is identical to the RCP. Also, the VCP can perform most of the same functions as the RCP.

For information about deciding whether the RCP or the VCP best meets your needs, see Differences between the virtual control panel and remote control panel.

Considerations for the virtual control panel

The following table lists requirements and restrictions for the VCP.

Table 6. Virtual control panel requirements and restrictions

Requirements	Restrictions
• The VCP must have a direct connection to the server from the Operations Console using the serial console cable. • A unique service tools device profile must exist for each VCP connection. • If you want to use the mode function provided by the VCP, the service tools user profile used to authenticate the connection must have the **Partition remote panel key** privilege. To verify that your service tools user ID has this privilege, see Setting user ID permissions for the VCP. • A VCP requires the console to be directly connected over a serial cable, and the console must be connected to use the control panel functions. However, the VCP cannot power on the server. The VCP also requires a service tools device ID on the server. • You must be granted access to a logical partition's RCP and functions to use the RCP or VCP. Because the VCP setup uses the Operations Console on a network configuration path and characteristics, the service tools device ID must also be granted access to that logical partition's RCP to use this feature. Users and service tools device IDs default values automatically grant access to the RCP for the logical partition. The user that authenticates a connection must also have authority to the respective logical partition's keylock to change the mode.	• The VCP is available only while the Operations Console is connected. • You cannot use an existing network name or duplicate a name that is already configured on the PC. You might need to verify if a name is used by looking in the `hosts` file on the PC. The `hosts` file can be viewed by any standard text editor. • More than one LAN-connected RCP can be active at the same time. In addition, LAN-connected RCPs can coexist with a VCP.

Connectivity and usage considerations

Ensure that you understand the connectivity and usage requirements and restrictions before you install the Operations Console VCP. For information about installing the VCP, see Setting up the virtual control panel.

Table 7. Connectivity requirements and restrictions

Requirements	Restrictions
• The VCP requires the serial cable and connection of a local console (directly attached). • The VCP requires a unique service tools device ID for connection authentication. If no local console on a network (LAN) configuration exists, then you can use the QCONSOLE service tools device ID.	• You cannot use a name that already exists on the network or duplicate a name that is already configured on the PC. • The hosts file on the PC might need manual cleanup. Each time you create a network configuration on the PC, data is saved in a file named `hosts`. This file can be used each time the PC attempts to connect to the network, and each entry is unique to any others by the connection name. Be aware that if you delete a VCP configuration, then the corresponding `hosts` entry is not deleted. You must use a text editor to manually delete the appropriate line from this text-based file.

Table 8. Usage requirements and restrictions

Requirements	Restrictions
• To control power, you must use the Hardware Management Console (HMC) or the Advanced System Management Interface (ASMI).	• The VCP is available only while the console is connected. • All VCPs and RCPs are active at the same time. Use care when working with control panel functions when multiple PCs have access to the functions.

Related concepts

Managing the Hardware Management Console (HMC)

Managing the Advanced System Management Interface (ASMI)

Related tasks

Setting user ID permissions for the VCP

Setting up the virtual control panel

Related reference

Differences between the virtual control panel and remote control panel

Differences between the virtual control panel and remote control panel

The major functional difference between the LAN connected remote control panel (RCP) and the virtual control panel (VCP) is that the VCP connects using the console's serial cable. Both are functionally the same.

If you need to power on the system at a later time, you can use the IPL scheduling function in Operational Assistant by pressing the Attention key. You can also use the GO POWER command, and select option 2 (Change power on and off schedule). You can also use the Hardware Management Console (HMC), if installed, or the Advanced System Management interface (ASMI) to control power on a partition.

The following POWER5™ processor-based server models work with the virtual control panel (VCP) and the LAN-connected remote control panel (RCP):

505

520

550

570

595

Operations Console migration

If you are upgrading to V5R4 and you want to change to or from Operations Console, upgrade the system before migrating Operations Console.

Upgrading the system prevents any conflict between the existing console and the new console. For instructions on upgrading i5/OS, see Upgrading or replacing i5/OS and related software.

Related concepts

Upgrading or replacing i5/OS and related software

Related tasks

Installing System i Access for Windows

Prerequisite information for Operations Console users upgrading to, or installing, V5R4

You must comply with the following items before upgrading or installing your software (i5/OS, Licensed Internal Code) to V5R4:

1. For all upgrades and installations, you need to establish a connection between the server and the Operations Console PC using the service tools user ID of 11111111 (eight 1's). This keeps the expired user IDs from preventing a successful re-authentication of the client connection to the server. When you receive the i5/OS release media, the user IDs (except 11111111) are expired. To establish a successful re-authentication of the client connection to the server, enter the service tools user ID of 11111111 (eight 1's). This is especially important for automatic installations.
2. Update iSeries Access for Windows to i5/OS Version 5 Release 4 before you upgrade the i5/OS operating system. For more information, see Installing iSeries Access for Windows.

Important: When you restart your server and a console was not previously specified, you receive two additional windows to confirm the setting of the console type. At the first window, press F10 to accept the current console type. The second window tells you that a console type value did not previously exist (a zero is present for the old value), and it displays the new console type value. Press Enter to exit the window and to set the console type automatically. The next window displayed is Install the System. This condition can happen on your first manual initial program load (IPL) of V5R4, for example, during the A-mode IPL, which follows the restoration of the Licensed Internal Code during the upgrade or installation when a console value of zero is found.

Operations Console networking

Learn about the minimum network configuration requirements for setting up a local console on a network (LAN).

If you are not using the default embedded Ethernet port as the default console port, you need to install the LAN adapter for Operations Console according to your server model. To do this, see Operations Console hardware requirements. If your server is new and you ordered a local console on a network (LAN), the adapter should already be configured with the server. The LAN adapter should be dedicated for service tools.

You might want to treat the console over a LAN connection with the same physical security considerations and controls as a local console that is directly attached or a twinaxial console. For example, consider configuring a local console on a network (LAN) in a network that is separate from the main network (or the company intranet) and strictly control access to the machine acting as the console.

You also might want to restrict LAN topologies for LAN-attached local Operations Consoles to a single, physical router environment. This might be as simple as connecting the PC and server using an inexpensive hub or router. Temporarily, you could also use an Ethernet crossover cable (when using a 2849) or any Ethernet cable if you are using the Host Ethernet Adapter 5767/5768, or 5706/5707 network adapter. When you have only a single PC or small number of devices connected to the server using a router, switch, or hub, and these devices do not connect to another network or the Internet, you can then use any numeric numbers for addresses. For example, use 1.1.1.*x* or 10.220.215.*x* (where *x* can be 2 through 255, but avoid *x.x.x.*1, which might cause problems in some networks).

In the event that the local console on a network (LAN) is used in a larger network topology, or the devices go to the Internet, use DHCP packet filtering and consult a network administrator for addresses.

Bootstrap Protocol

Although the system and PC can still perform a standard BOOTP operation as described here, i5/OS Version 6 Release 1 enables the automatic discovery of a connection between the system and a PC. This function, called VSDISCOVER, is a mechanism used solely for Operations Console. Both the system and PC listen for a special broadcast frame from the network and when received, there is a negotiation using ports 67 and 68, and the system and PC can use the data exchanged to configure itself, if needed. In addition, the PC creates a configured connection that you can use to start a console session. This VSDISCOVER function is the default mechanism for configuring a connection. The BOOTP process is still used when VSDISCOVER is not necessary, such as when you already have a configured connection and the network data needs to be reset.

A local Operations Console on a network uses the Bootstrap Protocol (BOOTP) to configure the server service IP communications stack. The IP stack configuration, plus server serial number and partition ID, is requested in the Operations Console configuration wizard. The server broadcasts a BOOTP request. The Operations Console PC replies with the information submitted during the configuration wizard. The server then stores and uses the configuration information for the service IP communications stack.

The Operations Console PC must be placed on a network that is accessible by the server. This can be the same physical network or a network that permits broadcast packets to flow. This is an initial setup requirement; typical Operations Console operation does not require this. This setup should occur on the same physical network.

The BOOTP request carries the server serial number and partition ID. The server serial number and partition ID are used to assign the IP configuration information. If you are having problems configuring the service IP communications stack, check that the Operations Console PC is on the same physical network and the server serial number and partition ID are correct in the configuration.

Important: IBM System i models start counting logical partitions with the number 1 (even if it is the only partition) instead of a 0. For the console to connect correctly, your logical partitions must also begin numbering at 1 instead of 0. This is especially true if you rely on the BOOTP process to configure the server with its network data.

A local console on a network (LAN) uses ports 2323, 3001, and 3002. To use Operations Console in a different physical network, the router and firewall must allow IP traffic on these ports. BOOTP uses UDP ports 67 and 68 per RFC 951. For more information, see http://www.faqs.org/rfcs/rfc951.html.

The success of BOOTP is dependent on the network hardware used to connect the server and the PC. In some cases, you might need a different console device to configure the connection in DST. To use BOOTP, the network hardware used must be capable of autonegotiation of speed and duplex if using the 2838 Ethernet adapter for the Operations Console connection.

Additional considerations for a system connected to an HMC

Networking security considerations are different when your system is managed by a Hardware Management Console (HMC) because your network and network security are configured differently. When you set up your HMC, determine whether you want to configure a private or open network. If it is the first HMC in your network, configure that HMC as a DHCP server. For more information, see Types of HMC network connections and Preparing for HMC configuration.

Related concepts

Types of HMC network connections

Preparing for HMC configuration

Related reference

Operations Console hardware requirements

Related information

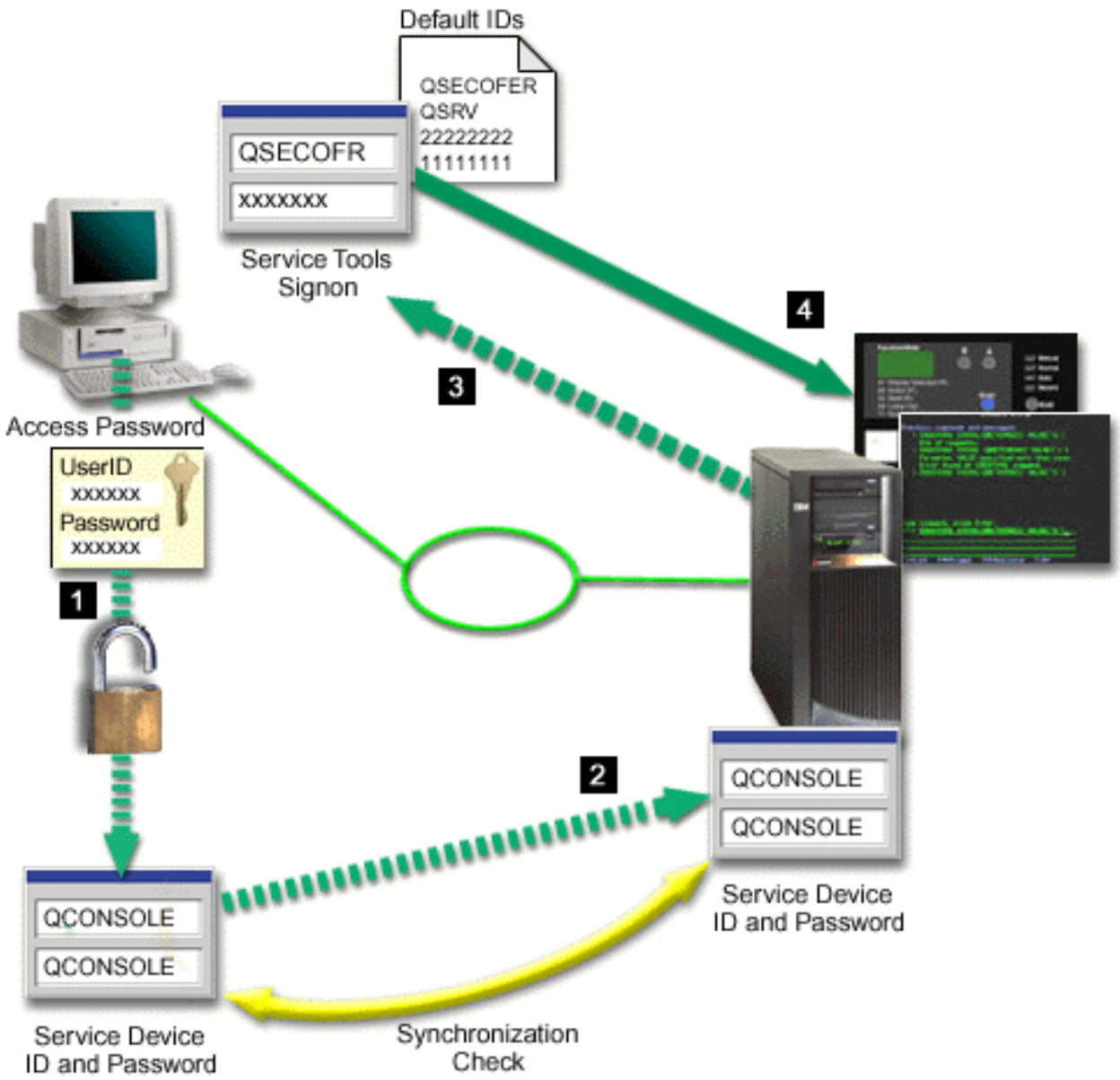
http://www.faqs.org/rfcs/rfc951.html

Configuration security

Learn about the components of Operations Console security and what considerations to make when administering control access to console functions.

A local console that is directly attached has implicit device authentication, data privacy, and data integrity due to its point-to-point connection. User authentication security is required to sign on to the console display.

Enhanced authentication and data encryption provides network security for console procedures. Operations Console network connections use a version of Secure Sockets Layer (SSL), which supports device and user authentication but without using certificates. By default, Operations Console uses the strongest encryption possible for authentication and data.



Starting with i5/OS Version 6, Release 1, Operations Console has simplified setup and authentication. By default, the system will manage service tools device IDs and the access password, so you only need to authenticate using a valid dedicated service tools (DST) user ID and password.

The following figure gives you an overview of your Operations Console LAN security. The access password (1), if correct, induces Operations Console to send (2) the service tools device ID (QCONSOLE) and its encrypted password to the server. The server checks the two values (3), and if they match, the server calculates a new service tools device ID password and informs the client of the change. The connection process then validates the service tools user ID and password before sending the system console display to the PC (4).

The Operations Console security consists of service tools device authentication, device authentication, user authentication, data privacy, data integrity, and data encryption:

Data encryption
Enhanced authentication and data encryption provide network security for console procedures. A local console on a network (LAN) uses a version of SSL that supports device and user authentication but without using certificates.

Data integrity
This security provides confidence that the console data has not changed en route to the recipient. A local console that is directly attached has the same data integrity as a twinaxial connection. If the physical connection is secure, the console data remains protected.

Data privacy
This security provides confidence that the console data can only be read by the intended recipient. A local console that is directly attached uses a physical connection similar to a twinaxial console or secure network connection for LAN connectivity to protect console data. Operations Console using a direct connection has the same data privacy as a twinaxial connection. If the physical connection is secure as discussed under service device authentication, the console data remains protected. To protect the data, ensure only authorized people have access to the console.

Device authentication
The device authentication is based on a service tools device ID. By default, the system defaults to administering service tools device IDs. The initial value for the number of automatically created service tools device IDs is set to 10. With the default QCONSOLE, 11 PCs can be connected at the same time, each with a unique service tools device ID. If you set this value to 0, you must administer the service tools device IDs manually. Service tools device IDs are administered manually in DST and system service tools (SST).

These IDs consist of a service tools device ID and a service tools device ID password. The default service tools device ID is QCONSOLE with a default password of QCONSOLE. A local console on a network (LAN) encrypts and changes the password during each successful connection. You must use the default device ID QCONSOLE to install a new server if you are using a local console on a network (LAN).

Important: The device authentication requires a unique service tools device ID for each PC that is configured with a local console on a network (LAN). When using a local console on a network (LAN), the configuration wizard determines if the system is capable of automatically creating a service tools device ID. If so, it skips this window during the configuration process. If you need to manually assign a user-created service tools device ID to a new configuration without turning off the autocreate function, disconnect the PC from the network while you create the configuration so that Operations Console cannot validate the function. You are then prompted for the user-created service tools device ID. The initial service tools device ID password default is the name of the service tools device ID in uppercase.

Note: The access password protects the service tools device ID information (service tools device ID and password) on the PC. By default, Operations Console now manages the access password for you. During the configuration process, no window is displayed in which to assign an access password. However, if you want to manually administer this password, you can change it by using the **Properties and the Access Password** tab.
When establishing a network connection, the Operations Console no longer prompts you for the access password to access the encrypted service tools device ID and password unless you have manually set it after the configuration was created. However, you will be prompted for a valid service tools user ID and password. For details, see “Changing the autocreate service tools device ID” on page 73.

Service tools device authentication
This security assures one physical device is the console. A local console that is directly attached is a physical connection similar to a twinaxial console. The serial cable you use for Operations Console using a direct connection can be physically secured similar to a twinaxial connection to control access to the physical console device.

User authentication

This security provides assurance as to who is using the service device. All problems related to user authentication are the same regardless of console type. For more information, see Working with the service tools device ID.

Security administration

Operations Console administration allows system administrators to control access to console functions, including the remote control panel and virtual control panel. When using a local console on a network (LAN), device and user authentication are controlled through the service tools device IDs and service tools user IDs.

Consider the following when administering a local console on a network (LAN):

- For the remote control panel, mode selections require security authorization for the user that authenticates the connection, such as that provided by QSECOFR. Also, when connecting the remote control panel using a network, the service tools device ID must have authority to the control panel data on the system or the logical partition that the remote control panel connects to.
- If you set the value of Autocreate service tools device IDs to 0, the following information pertains to your configurations. Otherwise, the system manages this automatically.
  - When a mismatch occurs in the service tools device ID password between the server and the Operations Console PC, resynchronize the password on both the PC and the server. However, the PC should be automatically synchronized after the service tools device ID password is reset at the server on the next connection. For more information on resynchronizing the passwords, see Resynchronizing the PC's and the server's service tools device ID passwords. If your PC is exchanged, a mismatch occurs and you need to re-create your connection configuration.
  - Because QCONSOLE is a default service tools device ID, you can elect not to use this device ID.

    Important: To prevent unauthorized access, you can temporarily configure a connection using this ID and successfully connect. Now create a service tools device ID you would like to use. When you are ready, disconnect and delete the configuration, but do not reset the device ID on the server. This action prevents an unauthorized person from using the known default service tools device ID. If you need to use this device ID later, it can be reset at that time by using the control panel or menus.
  - If you implement a network security tool that probes ports for intrusion protection, Operations Console uses ports 449, 2300, 2301, 2323, 3001, and 3002 for normal operations. Port 2301 is used for the console on a logical partition running in the Linux environment and is also vulnerable to probes. If your tool were to probe any of these ports, it might cause you to lose the console, which would require you to restart the server to recover the console. Exclude these ports from intrusion protection tests.

Security protection tips

When using a local console on a network (LAN), review the following items:

1. If you set the value of Autocreate service tools device IDs to 0, the following information pertains to your configurations. Otherwise, the system manages this automatically.
   a. For each PC that is used as a console, create an additional backup service tools device ID and control panel attributes for use in an emergency.
   b. Choose a nontrivial access password.
2. Protect the Operations Console PC in the same manner you would protect a twinaxial console or a local console that is directly attached.
3. Change your password for the following DST user IDs: QSECOFR, 22222222, and QSRV.

Note: Do not change the password for user 11111111. This is the only user that is provided without an expired password. If you experience a problem with authentication using another user ID, you can attempt to authenticate with 11111111/11111111.

4. Add backup service tools user IDs with enough authority to enable or disable both user and service tools device IDs.

Related concepts

Resynchronizing the PC's and the server's service tools device ID passwords

Related information

Working with the service tools device ID

Operations Console with iSeries Navigator

Both Operations Console and iSeries Navigator, which is the graphical user interface for managing and administering your server from your Windows desktop, can run on a single PC. Depending on how you have Operations Console connected to your server, there are two possible network configuration options available.

Operations Console allows you to use a local or remote PC to access and control a console, a control panel, or both. Operations Console enables connections or console activities across a local area network (LAN), and enables directly cabled connections. A single PC can have multiple connections to multiple servers and can be the console for multiple servers. An example is having a logically partitioned server using the same PC as the console for all logical partitions. Because each logical partition is considered a separate server, you need a separate connection to the logical partition for which you want to use the console. Operations Console allows multiple connections to a single server, but only one PC can have control of a server at a time. Based on the Operation Console connectivity, you can have either of the following methods of configuration.

- The PC using Operation Console as a local console that is directly attached requires a network connection for iSeries Navigator. To complete the iSeries Navigator connection, the server needs to have a network adapter and configured i5/OS line description (LIND).

  When Operations Console is connected over a serial cable attached to an asynchronous adapter on the server, iSeries Navigator is connected through a LAN adapter on the server. The PC communicates to Operations Console through its communication port while communicating with iSeries Navigator through the LAN connectivity.

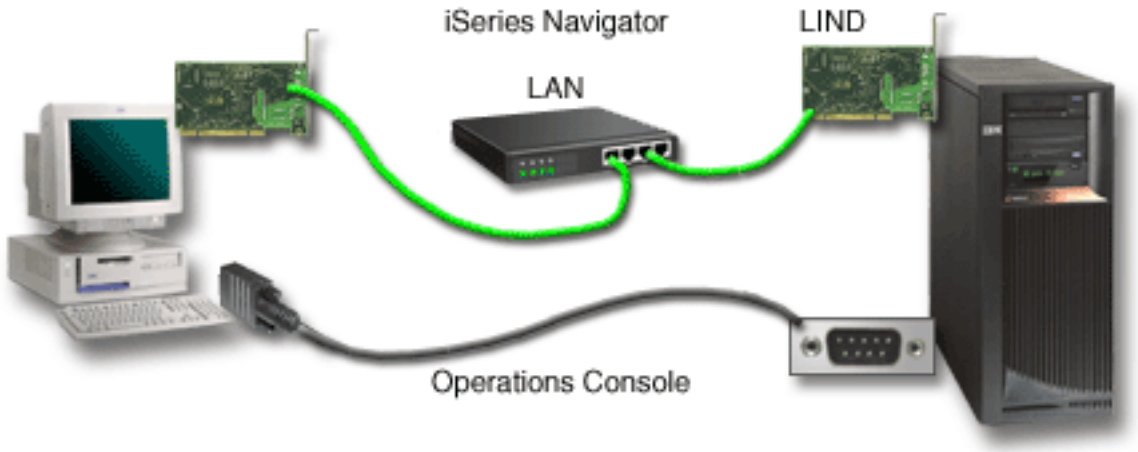


Figure 2. iSeries Navigator and Operations Console configuration over separate connections

- The PC used as a local console on a network (LAN) might require an additional network connection.iSeries Navigator requires a network connection to the network adapter and configured i5/OS LIND. Operations Console uses the service network adapter as defined by the service host name (interface name). If the network adapter and configured i5/OS LIND and the service network adapter, as defined by the service host name (interface name), are on the same network, then an additional PC LAN adapter is not needed.

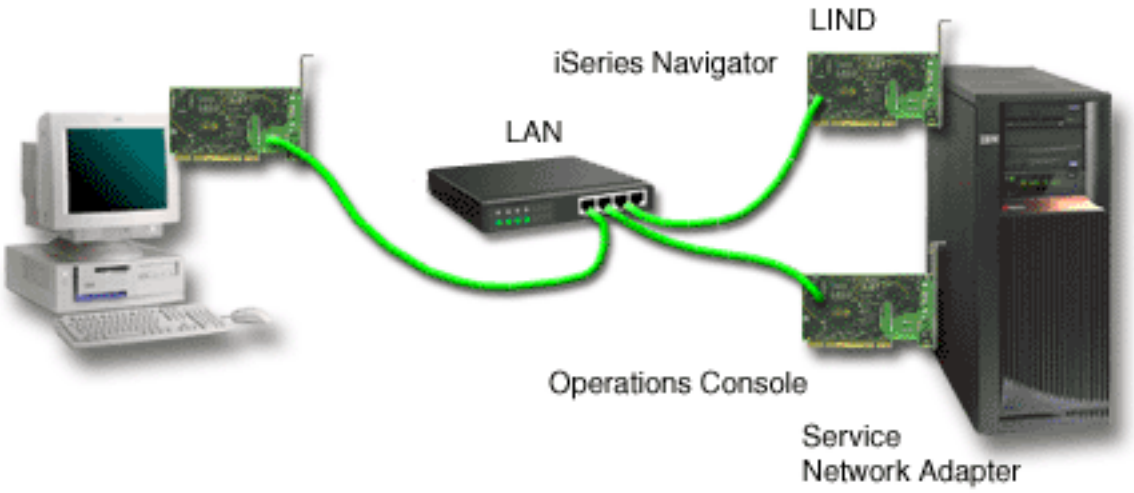


Figure 3. iSeries Navigator and Operations Console configuration on the same network

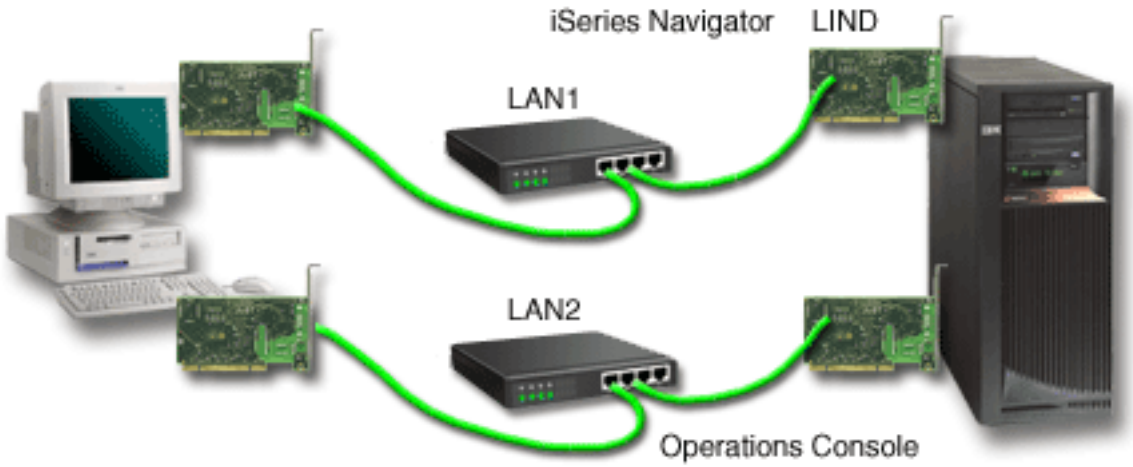


Figure 4. iSeries Navigator and Operations Console configuration on separate networks

Related information

System i Navigator

Connect your expansion units

Follow these instructions to verify readiness to add the expansion units and add the expansion units to the system.

1. You can install the expansion units with the system unit power on or off. In some cases, system unit power must be off. For more information about when system unit power must be off, refer to Expansion units.
   a. If you are installing a new system unit and expansion units, and were directed here from the Cabling your server procedure, go to step 5 on page 32.
   b. If you must power off the system to add the expansion units, or you are choosing to add the expansion units with the system power off and the system unit is not currently powered off, power it off now. For details, refer to Stop the system or logical partition. After you have powered off your system unit, continue with step 5 on page 32 to complete this procedure.
2. Verify the existing RIO/HSL configuration.

   Important: When simultaneously adding multiple expansion units to an existing RIO/HSL loop, it is required that the units be adjacent to each other so the existing loop is broken at only one spot.

   Tip: If multiple expansion units are to be added with the system power on, it is recommended to work with one RIO/HSL loop at a time. For example, if the plan is to add three expansion units to loop X and two to loop Y, follow the complete procedure to simultaneously add the three units to loop X. When the first procedure has been completed, then follow the procedure to simultaneously add the two units to loop Y. It is not necessary to complete the procedure for each expansion unit separately.

   If problems with the RIO/HSL loops are discovered in this step, they must be corrected before continuing with the expansion unit add procedure. Follow the appropriate step below to determine if there are problems with the RIO/HSL loops.

   If your system *is not* managed by an HMC, refer to Verify the RIO/HSL loops without using an HMC.

   If your system *is* managed by an HMC, refer to Verify the RIO/HSL loops using an HMC . You can use the **Save** button to overwrite the existing Last Valid RIO/HSL Topology. This action allows you to compare the topology before and after the addition of the expansion units.
3. To verify the System Power Control Network (SPCN), refer to Verify the System Power Control Network (SPCN). If problems with the SPCN are discovered in this step, they must be corrected before continuing with the expansion unit add procedure.

   Important: When simultaneously adding multiple expansion units to an existing SPCN loop, the units must be adjacent to each other so the existing loop is broken at only one spot.
4. Set the SPCN Firmware Update Policy.

   The SPCN Firmware Update Policy controls when and how SPCN firmware on expansion units will be updated. The default setting shipped with your system is for the SPCN Firmware Update Policy Enabled. This setting allows for firmware updates to be completed over the RIO/HSL interface whenever an update is required and does not allow updates over the slower serial SPCN interface.
   a. Access the ASMI using an authority level of Administrator or Authorized service provider. See Managing the Advanced System Management Interface (ASMI) for more information.
   b. In the ASMI navigation area, expand **System Configuration** and select **Configure I/O Enclosures**.
   c. Verify there are no SPCN firmware updates in progress by checking the **Power Control Network Firmware Update Status** column. This will show the words **In Progress** and a percent complete if an SPCN firmware update is in progress.

If there is an SPCN firmware update in progress, determine if the update is a Serial or HSL update by checking the Power Control Network Firmware Update Status column for one of these words indicating the type of update.

If the SPCN firmware update is an HSL update, wait for the update to complete before continuing.

Tip: To determine when the update is complete, select **Configure I/O Enclosures** every 15 to 30 seconds until the words `Not Required` are displayed in the **Power Control Network Firmware Update Status** column. Do not use the **Back** or **Refresh** buttons on the browser to monitor the status.

If the SPCN firmware update is a Serial update, either wait for the update to complete or stop the update. If you choose to stop the update, the update will need to be restarted from the beginning after you have completed the procedure. To stop the update, perform the following steps:

1) Complete step 4d.
2) Press the **Stop SPCN Firmware Update** button on the Configure I/O Enclosures panel.
3) Select **Configure I/O Enclosures** every 15 to 30 seconds until the word `Pending` is displayed in the **Power Control Network Firmware Update Status** column. Do not use the **Back** or **Refresh** buttons on the browser to monitor the status.

d. If your SPCN Firmware Update Policy is **Expanded**, record the current setting so it can be restored later and then change the setting to **Enabled**. If the SPCN Firmware Update Policy is **Enabled** or **Disabled**, continue without changing the setting.

5. Remove or open the back of the system unit.
6. Find the connector locations. If you need help finding the connectors on your expansion units or system unit, see Connector locations.
7. To connect the expansion unit with RIO/HSL cables, refer to Connect the expansion unit with RIO/HSL cables.
8. To connect the expansion unit with SPCN cables, refer toConnect the expansion unit with SPCN cables.
9. If you are installing a new server with the expansion units, return to Cabling your server. If not, continue with the next step.
10. Connect the power cables for the expansion units that you are installing to the power source. Then connect them to the power supplies on the expansion units. If you installed the expansion units with the system unit power off, continue with step 12. If not, continue with the next step.

    Note: Plug the power cable into the power source prior to connecting it into the power supply of the expansion unit.
11. The expansion units will power on automatically. After the expansion units that you have installed are powered on and you have waited 10 minutes for the hardware initialization to complete, continue with step 13.

    Tip: For each expansion unit, wait for the green power indicator to light on the control panel of the expansion unit that just powered on. This may take between one and 10 minutes. During this time, the yellow attention indicator may be lit on the control panel of the expansion unit that just powered on. After the green power indicators are lit on the control panels of all of the expansion units that were just powered on, wait 10 additional minutes for hardware initialization to complete before proceeding to step 13.
12. To start the system or logical partition, refer to Start the system or logical partition.
13. To verify the SPCN, refer to Verify the System Power Control Network (SPCN). When following these instructions, consider that the following errors logs are expected depending upon various factors in the system configuration and procedure.
    - 1000 9135 informational or permanent log entry due to an open SPCN loop.

- 1000 9137 permanent log entry due to disruption to the RIO/HSL or InfiniBand loop.
- 1000 9139 informational log entry for SPCN closed.
- 1000 910A, 1000 91DE if SPCN firmware updates were required.
- 1000 913B permanent log entry if an SPCN firmware update is required but not automatically started. If this error log entry is found, continue with the procedure and the error will be handled in step 15.

14. Verify the RIO/HSL Loops.

    If your system *is not* managed by an HMC, refer to Verify the RIO/HSL loops without using an HMC.

    If your system *is* managed by an HMC, refer to Verify the RIO/HSL loops using an HMC . If you saved the original RIO/HSL topology before adding the expansion units, use this saved topology to compare the original and modified configurations.

    When following these instructions, consider that the following errors log entries are expected depending upon various factors in the system configuration and procedure.
    - B700 6907 informational log entries for each new expansion unit that was added that has information in its non-volatile storage from a system which the expansion unit was previously attached to.
    - B700 6985 informational log entries before and after the B700 6907 informational log entries.
    - B700 6984 informational log entries to indicate a broken HSL loop.

15. Start necessary SPCN firmware updates.

    If a 1000 913B error log entry was found in step 13 on page 32, this is an indication that SPCN firmware updates are needed but not allowed due to the current SPCN Firmware Update Policy. Follow the PWR1907 procedure to update the SPCN firmware. Wait for the SPCN firmware updates to complete before continuing to the next step. This could take several hours depending on the number of expansion units on the SPCN loop and the current level of the SPCN firmware in the expansion unit.

16. If you changed the SPCN Firmware Update Policy in step 4 on page 31, change the policy back to the original setting.
    a. Access the ASMI using an authority level of Administrator or Authorized service provider. See Managing the Advanced System Management Interface (ASMI) for more information.
    b. In the ASMI navigation area, expand **System Configuration** and select **Configure I/O Enclosures**.
    c. Change the **SPCN Firmware Update Policy** setting to the setting recorded in step 4 on page 31. The default and recommended setting is **Enabled**.

17. Verify the new configuration. For details, refer to Verify that the new configuration is functioning.
18. If the system is partitioned, you can now assign the new hardware to a partition. For more information about AIX or i5/OS partitions, refer to Dynamically managing physical I/O devices and slots. For more information about Linux partitions, refer to Dynamically managing physical I/O devices and slots on Linux.

Related concepts

Planning for your Operations Console configuration

Step 1. Cabling the Operations Console to your server

Learn how to install an Operations Console cable.

Before you cable your server with Operations Console, determine the type of connection you will be making. You can attach directly to the server using the Operations Console cable or connect on a network (LAN) using an Ethernet cable.

Note: If you are changing the console device, the server value QAUTOCFG must be set to ON. Use one of the following options to verify or set this system value on the server:

- Use the WRKSYSVAL QAUTOCFG i5/OS command.
- During a manual IPL in the IPL Options window, for **Set major system options**, select **Y**. Then for **Enable automatic configuration**, select **Y**.

DANGER

When working on or around the system, observe the following precautions:

Electrical voltage and current from power, telephone, and communication cables are hazardous. To avoid a shock hazard:

- **Connect power to this unit only with the IBM provided power cord. Do not use the IBM provided power cord for any other product.**
- **Do not open or service any power supply assembly.**
- **Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.**
- **The product might be equipped with multiple power cords. To remove all hazardous voltages, disconnect all power cords.**
- **Connect all power cords to a properly wired and grounded electrical outlet. Ensure that the outlet supplies proper voltage and phase rotation according to the system rating plate.**
- **Connect any equipment that will be attached to this product to properly wired outlets.**
- **When possible, use one hand only to connect or disconnect signal cables.**
- **Never turn on any equipment when there is evidence of fire, water, or structural damage.**
- **Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.**
- **Connect and disconnect cables as described in the following procedures when installing, moving, or opening covers on this product or attached devices.**

  To Disconnect:
  1. **Turn off everything (unless instructed otherwise).**
  2. **Remove the power cords from the outlets.**
  3. **Remove the signal cables from the connectors.**
  4. **Remove all cables from the devices**

  To Connect:
  1. **Turn off everything (unless instructed otherwise).**
  2. **Attach all cables to the devices.**
  3. **Attach the signal cables to the connectors.**
  4. **Attach the power cords to the outlets.**
  5. **Turn on the devices.**

  (D005)

Important: The server must be powered off. Do not power on the server until you are instructed to do so.

The following steps assume you have already set up the PCs that are connecting to the system. You can also use these steps if you are removing one or more cables from your PC, server, or both.

To connect the Operations Console cable (directly attached):

1. Shut down and unplug the PC that will serve as the system console.
2. Locate the Operations Console cable (97H7557 or 39J5835), and connect the Operations Console cable to the corresponding connector on the adapter that you tagged for console when you created the logical partition.

Note: If you are using the 2742 adapter, the Operations Console cable must be attached to the lower connector.

3. Install the cable. If you want to use the console function (5250 emulation or command interface to server), install the Operations Console cable.
4. Connect the other end of the Operations Console cable to the first or only system port, which is located on the back of the PC that is being used as the console.

To connect the Ethernet cable on a network (LAN):

1. Shut down and unplug the PC that will serve as the system console.
2. Connect the network cable from the PC that will serve as the system console to your local network.
3. Connect another network cable from the same local network to the adapter to be used for the console. It is either located in a specific location or has been tagged using the HMC.

Notes:

- The 2849 adapter requires an input/output processor (IOP) that must be located in an expansion unit.
- If you are using the 5706/5707 or 5767/5768 adapter, you must connect the network cable to port 1 (top connector).

Related concepts

Cabling your server

Step 2. Installing iSeries Access for Windows

Before you use Operations Console, you must install iSeries Access for Windows.

Attention: Plug in and turn on your console at this time if you have not already done so.

During the installation of iSeries Access for Windows, you are going to install a 5250 emulator, unless you already have PC5250 or IBM Personal Communications V5.8 (V5.7 CSD 1 minimum), and Operations Console support. For updated PC requirements, see the iSeries Access for Windows Web site.

To check whether you have iSeries Access for Windows already installed, complete the following steps:

1. Click **Start** and select **Settings**.
2. Click **Control Panel**.
3. Double-click **Add/Remove Programs**. If you are using Microsoft Windows Vista, double-click **Programs and Features**.
4. Locate **IBM iSeries Access for Windows**.
5. To close Add/Remove Programs, click **Cancel**.
6. Close the control panel.

If you do not have iSeries Access for Windows installed, use the *System i Setup and Operations* CD-ROM to install it:

1. Insert the *System i Setup and Operations* CD-ROM in the CD-ROM drive.
2. Select the **iSeries Access for Windows** option to start the installation.
3. Wait until the IBM iSeries Access for Windows window is displayed.
4. Click **Next** and follow the prompts.

   For further installation assistance with iSeries Access for Windows, see iSeries Access for Windows.
5. If you are installing iSeries Access for Windows for the first time, you must verify that you have at least a minimum configuration for running Operations Console. If you are only adding the Operations Console component, add only the components necessary to meet this minimum configuration.

6. To ensure the minimum configuration, select **Custom** or **Full** installation and select at least the following components:

   Note: The Operations Console component is not available using the **Typical** or **PC5250 User** options.

   - **Required Programs**
   - **5250 Display and Printer Emulator** (if IBM Personal Communications V5.8 (V5.7 CSD 1 minimum) is not installed)

     You do not need a license to use 5250 Display Emulation just for Operations Console, even though the window indicates that one is required.

     Important: If your Operations Console configuration is going to support only the remote control panel, you do not need to install an emulator.
   - **Operations Console**
7. Click **Next** and follow the prompts. You will be asked to reboot your system at this time. Before applying the latest service pack, you must reboot the system.
8. Apply the latest service pack for iSeries Access for Windows.

Related reference

Applying System i Access service packs

Related information

Installing System i Access

System i Access

Step 3. Applying iSeries Access for Windows service packs

You must have the latest service pack program temporary fix (PTF) for iSeries Access for Windows and the latest level of iSeries Access for Windows on your PC.

Service packs are available for your PC at the following Web sites:

- iSeries Access for Windows Web site
- IBM FTP site: Navigate to the directory path: as400/products/clientaccess/win32/v5r4m0/servicepack.

Related information

System i Access Web site

IBM FTP site

Step 4. Completing your configuration setup tasks

You can configure your Operations Console to be a local console directly attached or a local console on a network (LAN).

To complete the setup tasks specifically for your configuration, choose one of the following options.

"Step 4. Option A. Local console directly attached"

"Step 4. Option B. Local console on a network (LAN)" on page 40

Step 4. Option A. Local console directly attached

To set up a local console directly attached, complete the following sections in order.

- Substep 1. "Installing the connection modem" on page 37

- Substep 2. “Prepare your connection” on page 38
- Substep 3. “Configuring a local console directly attached to the system” on page 38
- Substep 4. “Start your connection” on page 39

Installing the connection modem

If you are configuring a local console that is directly attached, you must install the Operations Console connection modem.

Note: The Operations Console connection modem is not a physical modem. It is a logical device driver that is included with Operations Console and allows a local console to connect to the server. When it is present, it displays as `Operations Console Connection` in the Remote Access Setup window.

Installing the connection modem for Windows 2000:

You must install the Operations Console connection modem that is supplied with Operations Console for a local console to communicate with the server. Only use these instructions if you are configuring a local console that is directly attached.

To install the connection modem, complete the following steps:

1. Click **Start** → **Settings** → **Control Panel**.
2. Double-click **Phone and Modem Options**.
3. Click the **Modems** tab.
4. Click **Add** to display the **Install New Modem** panel.
5. Select **Don’t detect my modem; I will select it from a list**, and then click **Next**.
6. Click **Have Disk** If you know the full path to the Operations Console Connection driver (cwbopaoc.inf), enter it here. Then, go to step 8. If you do not know the path, continue with step 7.

   Note: The default installation path is: C:\Program Files\Ibm\Client Access\Aoc\Inf\cwbopaoc.inf.f)
7. Click **Browse**.

   Navigate to *drive:*\path\Client Access\Aoc\Inf\ cwbopaoc.inf where *drive:* is the drive where iSeries Access for Windows is installed.

   Click **Open**.
8. Click **OK**. **Operations Console Connection** should be listed.
9. Click **Next**.
10. Select the communications port where you are going to install the Operations Console cable (for example, COM1).
11. Click **Next**.
12. If the Digital Signature Not Found window is displayed, click **Yes**.
13. Click **Finish** to return to the Modems tab of the Phone and Modem Options folder.
14. Click **OK**.

Installing the connection modem for Windows XP:

You must install the Operations Console connection modem that is supplied with Operations Console for a local console to communicate with the server. Use these instructions only if you are configuring a local console that is directly attached.

To install the connection modem, complete the following steps:

1. Click **Start** → **Control Panel**.
2. Double-click **Phone and Modem Options**.
3. Click the **Modems** tab.

4. Click **Add** to display the **Install New Modem** panel.
5. Select **Don't detect my modem; I will select it from a list**, and then click **Next**.
6. Click **Have Disk** If you know the full path to the Operations Console Connection driver (cwbopaoc.inf), enter it here. Then, go to step 8. If you do not know the path, continue with step 7.

   Note: The default installation path is: C:\Program Files\Ibm\Client Access\Aoc\Inf\cwbopaoc.inf
7. Click **Browse**

   Navigate to *drive:*\path\Client Access\Aoc\Inf\ cwbopaoc.inf where *drive:* is the drive where iSeries Access for Windows is installed.
8. Click **Open**, and then click **OK**.
9. Click **Next**.
10. Select the communications port where the Operations Console cable is attached, and then click **Next**.
11. If prompted, select **Continue Anyway** to continue the installation.
12. Click **Finish**, and then click **OK**.

Prepare your connection

Complete the steps to prepare the system for a connection.

1. Plug in your system or uninterruptible power supply and attached expansion units.
2. Open the control panel door on the front of the system. The control panel should be lit and display `01 B N V=F`. The system is not yet powered on.

   If `01 B N V=F` is not displayed, you might need to change the mode. To use the control panel to change the mode, perform the following steps:

   a. Select function `02` by pressing the Increment (^) or Decrement (V) button on the control panel.

      Tip: The Increment (^) and Decrement (V) buttons change the field values, and the Enter button advances you from field to field.

   b. Press Enter to start function `02`. The current IPL type is displayed with a pointer. The current logical key mode and IPL speed are also displayed.

   c. Using the Increment (^), Decrement (V), and Enter buttons, scroll through the IPL types, logical key modes, and IPL speeds until `02 B N V` is displayed.

   d. Press Enter to exit function `02`.

   e. Using the Increment (^) or Decrement (V) button, select function `01`, and then press Enter.

   If you need further information, see Remote and virtual control panels.

   Note: Expect a delay between the time when power is applied to the system and when an initial program load (IPL) can be performed. When power is initially applied to the system, the service processor performs a self-check and the control panel remains blank for up to 2 minutes. Wait until the `C1xxxxxx` progress codes are completed and `01` is displayed on the control panel before you perform an IPL or change any control panel functions.
3. Press the white Power On button. There is a short delay before the system powers on, approximately 5 to 20 minutes. When the system powers on, the control panel displays `01 B N V=F`. If the control panel displays `A9002000`, the console might not be connected yet.
4. Power on your system. The system will power on and connect. If you experience problems, refer to "Troubleshooting Operations Console connections" on page 75.

Configuring a local console directly attached to the system

Complete the configuration of your Operations Console (Direct) on the PC by stepping through the Operations Console configuration wizard.

Important: You must have administrator rights to create or alter a configuration. Also, the instructions assume the server is powered off. **Do not power on the server until instructed to do so.**

To configure a new local console that is directly attached to the system, follow these steps:

1. Click **Start** → **Programs** → **iSeries Access for Windows** → **Operations Console**. If Operations Console is not displayed, complete an iSeries Access for Windows selective setup. Click **Start** → **Programs** → **IBM iSeries Access for Windows** → **Selective Setup**.

   Notes:

   - The configuration wizard starts automatically. If it does not start automatically, click **Connection** → **New Connection**.
   - If Operations Console had a previous configuration, that configuration will open now.
2. Click **Next** on the Welcome window.
3. If the Configure Operations Console Connection window is displayed, click **Next**.
4. On the Select Configuration window, select **Local console directly attached to the system** and click **Next**.
5. On the Specify Connection Name window, enter a name that you want to use to refer to this configured connection. Click **Next**.
6. On the Detect Console Port window, ensure the **Detect console communication port** option is selected. Click **Next**.
7. If the Port Not Found window is displayed, the communications port could not be determined and some possible reasons are listed in the window. Click **Back** to try again or click **Next** to manually assign the port.
8. On the Select Console Port window, the next available communications port is displayed. You can either use the port provided or select another port where you have the console cable attached. Operations Console uses COM ports 1 thru 9.
9. Click **Next** after you select a port.
10. If you selected **Local console directly attached to the system** for your console type, click **Finish** on the Complete window.

You are now ready to start your connection.

Note: Operations Console no longer automatically configures to use the remote control panel. If you want to make changes, go to **Properties** → **Configuration tab** to deselect the function you do not want started for that connection.

Related tasks

Starting your connection

Start your connection

Complete the final step of setting up your Operations Console by starting your connection and powering on your system.

1. Highlight the connection name.
2. Start your connection by selecting one of the following tasks:
   - Right-click the connection name and select **Connect**.
   - Click the **Connection** icon in the toolbar.
   - Click the **Connection** menu and select **Connect**.

View the online help associated with using Operations Console by selecting **Help** from the Operations Console window Help menu.

Related concepts
Remote and virtual control panels

Step 4. Option B. Local console on a network (LAN)

Complete the following tasks in order to set up a local console on a network (LAN).

- Substep 1. "Creating or verifying a service host name (interface name)"
- Substep 2. "Creating service tools device IDs on the server" on page 41
- Substep 3. "Prepare your connection" on page 38
- Substep 4. "Configuring a local console on a network (LAN)" on page 43
- Substep 5. "Start your connection" on page 39

Creating or verifying a service host name (interface name)

The service host name (interface name) is the name of the network interface as it currently exists on your network, or it is the name you choose to refer to this connection as if this is the first console configuration for the server. You need a service host name any time a console or remote control panel is being connected using a network connection.

For example, if a network administrator has already configured the name *system* for use with iSeries Navigator, then *system* is entered in the Operations Console configuration wizard as the service host name. If the server is new and your network does not require advance configuration, then you can enter any name. The name you provide is used to refer to the interface after the console connection is successfully completed.

If you are setting up a new system using Operations Console (LAN), the LAN adapter is installed and the correct console type is specified during the manufacturing process. When working through the Operations Console configuration wizard, you must supply the connection name, as well as the network parameters. During the initial connection, this data finishes the server configuration for the network. This method uses BOOTP to configure the server. For more information about BOOTP, see Bootstrap Protocol.

If you already have a console or another workstation, use the following steps to either verify or create the configuration for the service connection. You can do this during a migration or an upgrade before disconnecting your old console. You can find the service host name by going into dedicated service tools (DST) or system service tools (SST) on the server or logical partition that you are configuring and use the Configure Service Tools Adapter window. Enter the same name on the PC as the existing service host name defined in DST or SST.

You must unlock the SST option before you can use it. For additional information on SST, see Unlocking service tools device IDs in SST.

Note: You might have to temporarily change the console to complete this task. You can also use any option pertaining to the service tools LAN adapter to verify the service host name or data.

To create or verify the service host name, complete the following steps:

1. Access service tools using DST or SST.
   - If you are using DST, select **Work with DST environment**, and then **System devices**.
   - If you are using SST, select **Work with service tools user IDs and devices**.
2. Select **Select Console**.
3. Select **Operations Console (LAN)** and press Enter. This displays `Verify Operations Console Adapters`.
4. Press F11 to configure.
5. The **service host name** (interface name) field contains the name. If you are creating a new service connection, follow these steps:

a. Enter the network data in the appropriate fields.
b. Store your configuration by pressing F7.
c. Activate the LAN adapter by pressing F14.
d. Press F3 to exit.
e. If you changed the console from the currently used console to a local console on a network (LAN) configuration, re-select the original console if that choice remains the console.

For additional information, see Working with the service tools device ID.

Related concepts

Bootstrap Protocol

Related information

Access service tools using SST

Access service tools using DST

Working with the service tools device ID

Creating service tools device IDs on the server

Learn how to set up service tools device IDs on the server if you are using a local console on a network (LAN) configuration.

Note: You only need to create service tools device IDS on the server when Autocreate service tools device ID has been turned off with a value of zero. For details, see "Changing the autocreate service tools device ID" on page 73.

If you are installing a new server using Operations Console on a network (LAN) configuration, then you must use the default service tools device ID, QCONSOLE, during the configuration wizard.

If you already have a console or another workstation, you must use the following instructions to set up service tools device IDs on the server for additional local console on a network (LAN) configurations. This is accomplished by using either the dedicated service tools (DST) or the system service tools (SST). However, you must unlock the SST option before the option is usable. For additional information on SST, see Unlocking service tools device IDs in SST.

1. Access service tools using DST or SST.
   - If you are using DST, select **Work with DST environment**.
   - If you are using SST, select **Work with service tools user IDs and devices**.
2. Select **Service tools user IDs**.
3. Use option 1 to create a new service tools device ID, and enter the new service tools device ID name in the first blank name field. Press Enter.
4. (Optional) Type a description for the newly created service tools device ID and press Enter. You have finished creating a service tools device ID.

   Note: The device ID and the service tools user ID must have proper authorization granted before the remote control panel and all of its functions are available for the associated logical partition. By default, the service tools device ID is granted access to the console and remote control panel for the partition on which it is located. If you do not want the remote control panel to be used with this service tools device ID, you must manually revoke the attribute using option 7.
5. To create additional service tools device IDs, repeat the steps starting at step 4.
6. Press F3 when you finish creating your service tools device IDs.

Notes:

1. If you must reset a service tools device ID, the password becomes the name of your service tools device ID in uppercase.

2. If you have more than one PC connected to your console, create several service tools device IDs for possible use during an emergency.
3. When creating a new service tools device ID for a server and for Operations Console that are not installed with the same version of i5/OS and iSeries Access for Windows, respectively, the password becomes the name of the service tools device ID in uppercase letters, just as if the device ID were being reset. For example, if the client is running i5/OS Version 5 Release 4 and the server is running i5/OS Version 5 Release 3, and you are creating a new service tools device ID for a new PC connection, the PC asks for a password for the device ID. Assume that you name the device system1. When you create this name on the PC, you are prompted for a password. You must use SYSTEM1 because the system is unable to assign a different password for this name. The same is true if the client is running i5/OS Version 5 Release 3 and the server is running i5/OS Version 5 Release 4. The i5/OS V5R4 has no way to assign a password because the password is automatically made the same as the system name in uppercase letters.
4. Sometimes the service tools device ID password must be reset. One example is when the password must be resynchronized between the PC and the server. When a mismatch occurs in the service tools device ID password between the server and the Operations Console PC, you must resynchronize the password by performing recovery steps on the server. The PC no longer requires a manual reset of the service tools device ID password. For more information, see Resynchronizing the PC's and the server's service tools device ID passwords. For additional information on service tools concepts, see Working with the service tools device ID.
5. Do not leave QCONSOLE in a reset state on the server. This is considered a security exposure.

Related concepts

Resynchronizing the PC's and the server's service tools device ID passwords

Related tasks

Unlocking service tools device IDs in SST

Related information

Access service tools using SST

Access service tools using DST

Working with the service tools device ID

Prepare your connection

Complete the steps to prepare the system for a connection.

1. Plug in your system or uninterruptible power supply and attached expansion units.
2. Open the control panel door on the front of the system. The control panel should be lit and display `01 B N V=F`. The system is not yet powered on.

   If `01 B N V=F` is not displayed, you might need to change the mode. To use the control panel to change the mode, perform the following steps:

   a. Select function `02` by pressing the Increment (^) or Decrement (V) button on the control panel.

      Tip: The Increment (^) and Decrement (V) buttons change the field values, and the Enter button advances you from field to field.

   b. Press Enter to start function `02`. The current IPL type is displayed with a pointer. The current logical key mode and IPL speed are also displayed.
   c. Using the Increment (^), Decrement (V), and Enter buttons, scroll through the IPL types, logical key modes, and IPL speeds until `02 B N V` is displayed.
   d. Press Enter to exit function `02`.
   e. Using the Increment (^) or Decrement (V) button, select function `01`, and then press Enter.

   If you need further information, see Remote and virtual control panels.

Note: Expect a delay between the time when power is applied to the system and when an initial program load (IPL) can be performed. When power is initially applied to the system, the service processor performs a self-check and the control panel remains blank for up to 2 minutes. Wait until the C1xxxxxx progress codes are completed and 01 is displayed on the control panel before you perform an IPL or change any control panel functions.

3. Press the white Power On button. There is a short delay before the system powers on, approximately 5 to 20 minutes. When the system powers on, the control panel displays 01 B N V=F. If the control panel displays A9002000, the console might not be connected yet.
4. Power on your system. The system will power on and connect. If you experience problems, refer to "Troubleshooting Operations Console connections" on page 75.

Configuring a local console on a network (LAN)

Complete the configuration of your Operations Console (LAN) on the PC by using the Operations Console configuration wizard.

The system is expected to have been powered on and is IPLing or already IPLed.

Important: You must have administrator rights to create or alter a configuration.

To configure a new local console on a network (LAN), follow these steps:

1. Click **Start → Programs → iSeries Access for Windows → Operations Console**. If Operations Console is not displayed, complete an iSeries Access for Windows selective setup. Click **Start → Programs → IBM iSeries Access for Windows → Selective Setup**.

   Notes:

   - When Operations Console starts it will check your network for any systems not already configured and display them.
   - If you had one or more previously configured connections they will also appear.
2. Select from the following options:
   - If the system you want to connect to is in the list of configured connections, go to "Start your connection" on page 39.
   - If the system you want to connect to is not in the list of configured connections, manually create one in step 3.
   - If there were no configured connections prior to starting and no systems were detected, the configuration wizard automatically starts. Continue with step 4.
3. Select **Connection → New Connection**.
4. Click **Next** on the Welcome window.
5. If the Configure Operations Console Connection window is displayed, click **Next**.
6. On the Select Configuration window, ensure **Local console on a network (LAN)** is selected and click **Next**. Consider how the service host name is being created. Consider how the service host name is being created. During the next step, you need to know if you already created a service host name (service interface), or if you will be creating one during the step. For more information about the service host name (interface name), see Creating or verifying a service host name (interface name).
7. In the Specify Service Host Name window, specify the service host name and click **Next** to allow Operations Console to search for the system on the network. Operations Console attempts to contact the system using the service host name you just entered. One of the following will occur:
   - If an address is returned, Operations Console will display the network address of the system and the IP address is disabled. Click **Next**.
   - If an address is returned and the PC previously resolved the name and address, Operations Console will display the network address of the system and automatically goes to the next window.

- If an address was not returned, enter the IP address that you want to assign to the service host name you entered. Click **Next**.

The data shown in the Specify Interface Information window depends on several factors as explained above.

8. Ensure that you verify all returned data before proceeding. Consider the following:
   - All fields might not appear at this time and some fields might be disabled. This is the result of the previous step in which you attempted to contact the system.
   - If the PC does not receive information from the network, you must enter any required data manually. This might happen if the system has never been configured or if the system is not connected to the network yet.
   - System i models start counting logical partitions with number 1 (even if it is the only partition) instead of a 0. For the console to connect correctly, your logical partitions must also begin numbering at 1 instead of 0. This is especially true if you rely on the BOOTP process to configure the server with its network data.
9. If all the data is correct, click **Next**.
10. Select from the following options:

    Note: The next window you see depends on whether Operations Console was able to connect to the system and what information was provided.
    - If the Specify Service Tools Device ID window is displayed, the target system was either not able to be contacted, or the system is not running i5/OS Version 6 Release 1. Perform the following steps:
      a. Enter a device ID. You can either use the default QCONSOLE service tools device ID that is provided or enter a service tools device ID that you created specifically for this configured connection.
      b. Click **Next**.
      c. Click **Finish** in the Complete window to save the configuration and to exit the setup wizard.
    - If the Complete window is displayed, click **Finish** to save the configuration and to exit the setup wizard.

    You are now ready to start your connection.
11. Go to "Start your connection" on page 39.

Related tasks

Starting your connection

Start your connection

Complete the final step of setting up your Operations Console by starting your connection and powering on your system.

1. Highlight the connection name.
2. Start your connection by selecting one of the following tasks:
   - Right-click the connection name and select **Connect**.
   - Click the **Connection** icon in the toolbar.
   - Click the **Connection** menu and select **Connect**.

View the online help associated with using Operations Console by selecting **Help** from the Operations Console window Help menu.

Related concepts

Remote and virtual control panels

Working with Operations Console

Learn how to maintain and operate Operations Console after you have successfully set it up.

After you have completed Planning for your Operations Console configuration and Setting up Operations Console, you have options available to help you manage your local console connections.

Related concepts

Planning for your Operations Console configuration

Setting up Operations Console

Working with your console configuration

Learn how to manage your local consoles through maintenance tasks.

Changing keyboard definitions

Learn how to edit and change your keyboard definitions.

Complete the following steps to change your keyboard definitions:

1. In the emulator window, use the drop-down menu to do the following steps:
   a. Click **Edit**.
   b. Click **preferences**.
   c. Click **keyboard**.
2. Click **User-Defined**.
3. Click **Browse...** and then navigate to where iSeries Access for Windows is installed. Under the **Client Access** folder, navigate to the **Emulator** folder, followed by the **Private** folder.
4. Select your choice.
5. Click **OK**, and then click **OK** again.

Note: If you are using IBM Personal Communications, the default path is: **Documents and Settings** → **User Name** → **Application Data** → **IBM** → **Personal Communications**.

Changing a console configuration

Learn how to change an existing local console configuration to meet your specific needs while using Operations Console.

To change or create a local console, you must be a member of the administrators group. If you are changing a system name, you must delete the current configuration and re-create it with the new name. For information on how to delete a current configuration, see Deleting a console configuration.

Related concepts

Server control

Related tasks

Deleting a console configuration

Changing a local console directly attached

To change the configuration of an existing local console that is directly attached, complete the following steps:

1. If your local console is connected to a server, disconnect as follows; otherwise, go to step 2:
   a. Select the configuration name.
   b. From the Connection menu, click **Disconnect**. The connection status displays `Disconnecting`.
   c. Wait until the status displays `Disconnected` at the local console.
2. Select the configuration name.
3. From the Connection menu, click **Properties**.
4. Select the **Configuration** tab.
5. Make your changes and click **OK**.

Changing a local console on a network (LAN)

Complete the following steps to change your local console on a network (LAN) configuration:

1. Select the configuration name.
2. Click **Disconnect**. Wait until the status displays `Disconnected`.
3. Select the configuration name.
4. From the Connection menu, click **Properties**.
5. Select the **Configuration** tab.
6. Make your changes and click **OK**.

Note: If network data is changing, you must delete and re-create the connection configuration. Also, you should close and restart Operations Console before attempting to connect a new configuration. This action removes all cached values associated with any old configurations. Be certain any changes at the client (PC) reflect those values assigned at the server.

Deleting a console configuration

Learn how to delete an existing local console configuration to meet your specific needs while using Operations Console.

To delete an existing console configuration, you must be a member of the administrators group.

Note: You can also use the Delete key on the keyboard. To do this, highlight the configuration you want to delete and press the Delete key.

Related concepts

Server control

Deleting a local console

To delete an existing local console, complete the following steps:

1. If your local console is connected to a server, disconnect as follows; otherwise, go to step 2 on page 47:
   a. If the local console does not have control, do the following to request control; otherwise, go to step 1b:

      Note: For more details on server control, see Server control.

      1) Select the configuration name from the Operations Console window.
      2) From the Connection menu, click **Request Control**.
      3) If the Service Device Sign-on window is displayed, click **Cancel**.
   b. Select the configuration name from the Operations Console window.
   c. From the Connection menu, click **Disconnect**. The connection status displays `Disconnecting`.
   d. Wait until the connection status displays `Disconnected` at the local console.

2. Select the configuration name from the Operations Console window.
3. From the Connection menu, click **Delete**.
4. Click **Yes** to confirm the deletion.

Deleting the network object

If you create a local console directly attached configured connection the operating system creates a network object. You might need to delete the network object each time you delete a configuration entry in Operations Console. Verify that the network object does not exist by completing the following steps:

1. If you are using Window 2000, click **Start** → **Settings** → **Control Panel** → **Network Connections**, or if you are using Windows XP, click **Start** → **Control Panel** → **Network Connections**.
2. If you deleted a local console configuration, look for an icon that has the name of the system that the local console used to connect.
3. If the icon exists, you must delete the network object as follows:
   a. Right-click the icon.
   b. Select **Delete**.

Changing the mode of the emulator for a 3179 or 3477

You might need to change the mode of the emulator from its current setting to something wider or narrower depending on what you are viewing.

By default, the emulator is set to 24 X 80 (3179), so viewing a spool file or vlog requires you to use the keyboard to shift right and left in the window. In this case, it might be more convenient to use the 27 X 132 (3477) mode.

Important: During the transition from one mode to the other, the console is disconnected and reconnected.

To change the mode of the emulator, complete the following steps:

1. In the emulator window, click **Communications**.
2. Select **Configure**, and then click **Session Parameters**.
3. Select the desired screen size and click **OK**.
4. Click **OK**. If you are not using IBM Personal Communications, you will receive a message indicating that the connection is ended.
5. Click **OK**. The emulator session closes.

If the option **Allow console recovery and console can be taken over by another console** is not enabled, the console returns to the signon window and is in the correct mode. You can exit these instructions.

If the option **Allow console recovery and console can be taken over by another console** is enabled, the console returns to the signon window, but the Console Information Status window and the option to perform a takeover are most likely set to NO. This is due to a change in the emulator's attributes and the new console type does not match that of the current console when it connected. At this point, you must do one of the following:

- Use SST from another workstation to perform the native macro OPSCONSOLE RESTART. For more information, see Using the OPSCONSOLE macro.
- Use the console service functions (65+21) to do a **65**, **21**, **21**, which performs the restart. For more information, see Using the console service functions (65+21).

  Note: The console closes again, but should reconnect in two or three minutes.

Related concepts

Using the console service functions (65+21)

Related tasks

Using the OPSCONSOLE macro

Disabling support for the default embedded Ethernet port or 5706/5707 adapters

Learn how to disable console support for either the embedded Ethernet port or add-on 5706/5707 adapters, or both. These options do not disable the port or adapters, but makes them ineligible as console-supporting resources. Also, this support is only available on servers that are not managed by a Hardware Management Console (HMC).

Disabling console support for either the embedded Ethernet port or add-on 5706/5707 adapters, or both, allows you to use one or both of these resources for another purpose other than Operations Console. Initially, the embedded Ethernet port is the default location for Operations Console (LAN) configurations and is dedicated for that purpose. If a 5706/5707 adapter is also present in a location where the console can use it, you can disable this support to prevent Operations Console from selecting the adapter for console use. These instructions are typically used only when the system is not managed by the HMC and the console resource is determined by location.

To disable either the embedded Ethernet port or add-on 5706/5707 adapters, complete the following steps:

1. Access service tools using DST or SST.
   - If you are using DST, select **Work with DST environment**, and then **System devices**.
   - If you are using SST, select **Work with service tools user IDs and devices**.
2. Select **Select Console**.
3. Type a 2 in either the **Allow supported internal LAN adapter to be the console** or **Allow supported Gigabit LAN adapter to be the console** field, depending on what you want to disable.
4. Press Enter.

If you do not have a working console device, but you have another workstation that can access system service tools (SST), then you can use the preceding DST/SST procedure or use the OPSCONSOLE macro to disable your intended resource. If you do not have any working devices, then you must use the console service functions (65+21).

Related concepts

Using the console service functions (65+21)

Related tasks

Using the OPSCONSOLE macro

Related information

Access service tools using SST

Access service tools using DST

Using the console service functions (65+21)

Use the console service functions (65+21) only when you encounter an unexpected console failure and there are no other workstations available for recovery or resolution. Inappropriate use can result in the inability to use the intended console.

Any hardware allocations or configurations must be accomplished before using the console service functions (65+21). For example, if you installed an input/output adapter (IOA) for use with the console device, you must tag this IOA to change the type of console or connectivity.

Important: To use the console service functions (65+21), the server must be far enough through the initial program load (IPL) for the code to run correctly. If a console device is available, you can use that device for changes or recovery. If a console device is not available, you can perform the console service functions (65+21) only after a failing system reference code (SRC) is displayed. The code is typically A6005008 for a manual IPL.

The console service functions (65+21) apply to systems with or without a Hardware Management Console (HMC), as well as a control panel. If your system is managed by an HMC, you can enter these functions using the HMC, Operations Console remote control panel, or the virtual control panel. If your system is not managed by an HMC, you can enter these functions at the physical control panel, Operations Console remote control panel, or the virtual control panel.

The following functions are available using the console service functions (65+21):

- Changing the console value in i5/OS (01 - 04)

  You can use the console service functions (65+21) to change the console value from its current value to another. For example, assume that you ordered your system with Operations Console (LAN), but you are having trouble getting it to work. If you have received the console cable for a directly attached console, you might want to change the value from a 03 (LAN) to a 02 (Direct).
- Clearing the resource and configuration for the Operations Console (LAN) adapter (C3)

  With this option, you can disassociate the current LAN adapter used for Operations Console. You might use this option to overcome a mistake in the configuration. For example, assume that you made a typing error and entered another device's IP address. At connection time, the client configured the system's LAN adapter for use by the console, but the console fails to connect because the other device is active. This option clears the system's network data for the console and allows you to delete the client's configuration so that you can start over and make the BOOTP work again.

  Depending on your intent to clear the LAN adapter configuration, you might also want to stop and restart the LAN adapter. The example here benefits from following the clear function with a deactivate and activate (A3) function to save time from having to do an IPL.
- Deactivating and activating the Operations Console LAN adapter (A3)

  With this option, you can reset the LAN adapter used by Operations Console when some network problem causes the system to get into a bad state and the console cannot become active. This forces the LAN adapter to deactivate, and then restart. This might solve the problem, providing the original problem that caused the connection failure has been solved.

  This option might be used in place of an IPL for some circumstances, such as after the LAN adapter configuration has been cleared.
- Dumping Operations Console-related flight recorders to vlogs (DD)

  Note: This option will not work during an IPL in D-mode.

  You can capture valuable resolution information regarding an Operations Console connection failure for support personnel. This option is less invasive than performing a main storage dump, which forces the server to restart. The console service functions (65+21) gather the flight recorder logs for Operations Console and then the server creates a set of vlogs for major code 4A00 and minor code 0500. You can send these vlogs to your authorized service provider for analysis. When possible, continue the IPL of the server to i5/OS to guarantee that all vlogs are created even if the IPL fails. The intent is that the Licensed Internal Code (LIC) function has started the vlog tasks before performing the dump of flight recorders.
- Enabling or disabling the embedded Ethernet port and 5706/5707 adapters (E1, E2, D1, D2)

  Note: These options are only used when the system is not managed by an HMC.

  You can enable or disable support for the embedded Ethernet port and for the 5706/5707 adapters. The values displayed depends on the model and code level, for example, E6C30005 or E1E20005. The E6 in the first example corresponds to the E1E2 in the second example on earlier releases. Starting in V5R4M5 the E6 in the first example would be replaced by 06 or E2 where 06 indicates both the

embedded Ethernet port and the 5706/5707 adapters are supported. The E2 would indicate that the user designated C2 to be used for a local console on a network (LAN) configured connection. For a complete list of all values see Troubleshooting > SRCs > A6005008.

- Selecting an individual LAN adapter location (B*n*)

  Your system can have LAN adapters for use with a console located in multiple slots simultaneously, including locating the network adapter in slot C2 or C5. A 5706/5707 adapter can be used without an IOP if your hardware supports this function. If you use another network adapter, such as the 2849, then you must install an IOP.

  The B*n* set of options are only available when the embedded Ethernet support is turned off and the 5706/5707 adapter support is turned on. The numbers appearing with the B*n* set are model dependent and may appear in the normal search order, not necessarily numerically.

- Selecting an individual asynchronous adapter location (F*n*)

  Your system can have asynchronous adapters located in multiple slots simultaneously, including locating the 2793 asynchronous adapter in slot C4. Slot C4 allows an IOA that does not require an IOP. This is possible only for systems that are not managed by an HMC and have an input/output adapter (IOA) that does not require an input/output processor (IOP). To allow for this greater flexibility on the 520, you must install PTF MF39303 (V5R3M5) or PTF MF39304 (V5R4M0). These PTFs should already be installed on the 525 and 515. Starting with i5/OS V5R4M5, all POWER5 systems have the ability to designate a specific asynchronous communication adapter for console or remote service. The numbers in the F*n* are determined by the model and may be seen in the search order the system would look, not necessarily numerically.

  With these PTFs, you will be able to select an individual asynchronous adapter for use with the console and remote service by using either a native macro or the console service functions (65+21). The console and remote service functions must all remain on a single asynchronous adapter. If you have a system that was shipped with Licensed Internal Code (LIC) prior to V5R4M5, you cannot select slot C4 for use with the console when using the 2793, but you can select slot C4 for use with remote service.

  Also, if you are running LIC prior to V5R4M5 and you have moved the 2793/2794 asynchronous adapter from its manufacturing default location to use Operations Console (Direct), you must use the 65+21 functions to increment *nn* of SRC A6*nn* 500*x* until the *nn* value is *F2* or *F3*. This action will enable the asynchronous adapter in slot C2 or C3.

How console service functions work

Learn about how the console service functions work.

Note: If your system is not in manual mode, and the extended functions are not activated, or both, follow these steps:

1. If your system uses a keystick, insert it in the key slot.
2. Place the system into manual mode by using the system's control panel.
3. Using **Up** and **Down**, select function **25**. Press Enter.
4. Use **Up** to select function **26**. Press Enter.

A function 65 is performed from one of the input methods. You have approximately 60 seconds to enter a function 21 for the system to pair the two functions together. If not, the function 21 is a force of dedicated service tools (DST) to the console. Depending on the state of the current IPL, you might not see a change at the console, assuming the console is still present after the 65. If the 65 and 21 are entered in less than 60 seconds, a system reference code (SRC) of A6*nn*500A is displayed on the control panel. The value of *nn* depends on the console value currently being used, 01 thru 04. Repeating the 65 and 21 puts the system into an edit mode where you can make a change or cause an action to be performed.

Note: If you are using a physical control panel with a double row of data, you might need to perform a function 11 after each function 65+21 to force the system to show the resulting SRC code. If you are using the remote control panel, the virtual control panel, or another input type, it might not be necessary to do function 11 after the function 65+21 operation.

After the second 65+21 pair is entered, the control panel responds with an SRC of A6*nn*500B to indicate you are in edit mode. Each repeated 65+21 within edit mode increments *nn* of the SRC until you reach the value representing the action you intend to perform. At this time, you enter a single 21, which causes the selected function to be performed. The SRC then becomes A6*nn*500C to indicate the function was successfully submitted.

If at any time you exceed 60 seconds between the 65 and 21 or between succeeding 21s, SRC A6*nn*500D might be displayed, indicating a timeout condition and the system is no longer in edit mode. If you planned to make a change, you must restart the operations. This SRC will reset in approximately three minutes. You can quit the edit mode by using function 66. The function 66 does not have to complete successfully.

Use the following codes to track your progress:

A6*nn* 500*x*

Where *nn* is:

00 = No console defined

01 = Twinaxial console

02 = Operations Console (Direct)

03 = Operations Console (LAN)

04 = Hardware Management Console (HMC) or Thin Console

C3 = Clear LAN configuration

A3 = Deactivate followed by an activate of the LAN Operations Console adapter

DD = Dump all console related flight recorder into a set of vlogs

D1 = Disable Ethernet embedded port

D2 = Disable add-on 5706/5707 LAN adapter

E1 = Enable Ethernet embedded port

E2 = Enable add-on 5706/5707 LAN adapter

B2 = Enable LAN adapter in slot C2

B5 = Enable LAN adapter in slot C5

Bn = Enable LAN adapter in slot Cn (where n is a valid console location based on the model). (This option will only display when support for the embedded port is disabled and support for the 5706/5707 is enabled.)

F2 = Enable asynchronous adapter in slot C2

F3 = Enable asynchronous adapter in slot C3

F4 = Enable asynchronous adapter in slot C4

Fn = Enable asynchronous adapter in slot Cn (where n is a valid console loocation based on the model)

Notes:

- Selecting *02* will automatically activate the asynchronous communications adapter used for Operations Console (Direct).
- Selecting *03* might also require a function A3 to activate the LAN adapter in rare cases. Also, if a LAN connected console is connected, the emulator might go to a `Disconnected` state. If so, you can start it again by clicking **Communication** and selecting **Connect**.

Where *x* is:

A6*nn* 500A = Your current console value is displayed.

A6*nn* 500B = You did a second 65+21 pair so you are in edit mode.

A6*nn* 500C = You executed a second 21 to cause an action, such as setting the console to another value.

A6*nn* 500D = Too much time has passed after entering edit mode to cause an action. You must enter edit mode again if you intend to make a change. A 21 at this time will force the console to DST, not cause an action.

If you do not want to make a change after entering edit mode, you can wait 3 minutes and the completion code indicates a change is no longer pending. You can also enter a function 66 to cancel any pending changes and exit.

An example of a console change is when you have a twinaxial console (01) and you want to use LAN (03). This example shows the additional function 11 that would be entered if you are using a double-row control panel to force the resulting SRC code.

65 - 21 - 11 = A601500A You are in display mode and the console value is 01.

65 - 21 - 11 = A602500B You entered edit mode and incremented the counter.

65 - 21 - 11 = A603500B You incremented the counter again.

21 - 11 = A603500C You invoked the action (set the console value to 03).

If the LAN adapter already had a valid configuration, for example, you previously configured the LAN adapter for use with the service tools server, you can now create a local console on a network (LAN) configuration on the client, if one does not already exist. You can then turn off the twinaxial device and connect the Operations Console (LAN) configuration.

Note: To reset the console without changing the console value, you can enter a 65 - 21 - 21. The system will respond with A6*nn*500A after the first 21 and A6*nn*500C after the second 21. This causes the connection to the console to be dropped during the reset process. Do not use this function when you already have a working console. This function does not correct all errors associated with a console failure, but rather resets the hardware associated with the configured console connection.

Related tasks

Putting the physical control panel in manual operating mode

Using the OPSCONSOLE macro

Learn how to use the OPSCONSOLE macro, which is the system-side debugging and analysis tool for managing or collecting data for console-related procedures.

Native macros are advanced debug and analysis tools resident on the server. These tools are intended to be used only with the direction of support personnel because inappropriate use of these tools can cause unpredictable problems with your system. If you are not comfortable in the service tools area, call your service provider for assistance before using these tools. These instructions assume you do not have a console device, but do have another workstation capable of using the system service tools (SST).

Important: Incorrect use of native macros can result in a change requiring a complete system reload. Use these native macros only at the request of a support representative.

To use the Operations Console native macro support, follow these steps:

1. Access service tools using SST.
2. Select **Start a service tool**.
3. Select **Display/Alter/Dump**.
4. Select **Display/Alter storage**.

5. Select **Licensed Internal Code (LIC) data**.
6. Select **Advanced analysis**. (Page down to see this option.)
7. Page down until you find the **OPSCONSOLE** option.
8. Type a 1 next to the option and press Enter. The **Specify Advanced Analysis Options** window is displayed and the command displays as `OPSCONSOLE`.
9. Enter the appropriate option and any required parameters in the **Options** field. Use the following options based on the function you are running:
   - Change the console type = **cnsltype *x*** (where *x* is 1, 2, 3, or 4)
   - Clear the resource and configuration for the Operations Console LAN adapter = **cnfglan -clear**
   - Dump Operations Console-related flight recorders to vlogs = **dump -vlog**
   - Deactivate the communications adapter for a local console that is directly attached = **deactdirect**
   - Activate the communications adapter for a local console that is directly attached= **actdirect**
   - Deactivate the LAN adapter for a local console on a network (LAN) = **deactlan**
   - Activate the LAN adapter for a local console on a network (LAN) = **actlan**
   - Restart the console device (any console) = **restart**

     Note: Use the **restart** option when you need to deactivate the current console and allow the server to determine and start or restart a console. You can use the **restart** option to correct a problem with the original console or when switching from one console type to another.

The following codes are only used when the server is *not* managed by an HMC:

- Enable the embedded Ethernet port = **enbintlan** You might want to run this command if you have an IBM System i5 and eServer i5 model manufactured before V5R4 and you want to use the embedded port for the console.
- Disable the embedded Ethernet port = **disintlan** You might want to run this command if you have an IBM System i5 and eServer i5 model manufactured at V5R4 as the default LAN console resource and you want to use the resource for another purpose.
- Enable a 5706/5707 or 5767/5768 adapter = **enbextlan** You might want to run this command if you have an IBM System i5 and eServer i5 model manufactured prior to V5R4 to take advantage of the faster network capability from one of these adapters instead of your current network adapter.
- Disable a 5706/5707 or 5767/5768 adapter = **disextlan** You might want to run this command if you have an IBM System i5 and eServer i5 model and want to prevent the use of this LAN adapter for use as a console.
- Enable both the embedded port and the 5706/5707 or 5767/5768 adapter = **enbboth** You might want to run this command if you have an IBM System i5 and eServer i5 model manufactured prior to V5R4 to make your current server use these resources as the default settings for new models being built.
- Disable both the embedded port and the 5706/5707 or 5767/5768 adapter = **disboth** You might want to run this command if you have an IBM System i5 and eServer i5 model and do not want the adapters used for the console.
- Display both the embedded port and the 5706/5707 or 5767/5768 adapter configuration flags = **dspcfg** You might want to run this command if you have an IBM System i5 and eServer i5 model and a service and support representative asked you for this information. This macro returns the state of the embedded port and Gigabit LAN adapter support.
- Select an individual asynchronous adapter for console and remote service = **enbslot *x*** (*x* is 1 thru 6 depending on model). See note 1 for models 515, 520, and 525 running V5R3M5 or V5R4M0.

Notes:

1. This option applies to the IBM System i5 520, 525, and 515 models that are not managed by an HMC and have an IOA that does not require an IOP. For the 520, you can install PTF MF39303 (V5R3M5) or PTF MF39304 (V5R4M0). For the 525 and 515, these PTFs should already be installed.

2. If you are running LIC prior to V5R4M5 and you have moved the 2793/2794 asynchronous adapter from its manufacturing default location to use Operations Console (Direct), you must first activate the communications adapter for a local console that is directly attached (**actdirect**).
3. If you no longer want to select an individual asynchronous adapter, you can clear your current selection by using **clrslot**.

The following options are available with V5R4M5 :

- Select a specific LAN adapter location = **enblslot** ***x*** (*x* is 1 thru 6 depending on model)
- Clear the LAN adapter location = **clrlslot**

Related information

Access service tools using SST

Access service tools using DST

Operations Console properties window

Verify and change information about the server and connection configurations using the Properties window.

The Properties window contains information about the server associated with the connected configuration. You can make changes to an existing configuration.

The **General** tab contains information about the server that your selected connection represents. You will also see the assigned service tools device ID for the configured connection here. The **Log Directory** field displays the path to the Operations Console data logs and is the only field you are allowed to edit. If the selected connection is not connected, the data provided originates from the last successful connection. If you select **Properties** for a connected configuration, you are presented with a window that indicates some changes might not take effect until the next time you reconnect the configured connection.

If the partition number displays ****, a configuration error is associated with the configured connection. The error might be an incorrect partition ID or an incorrect service host name IP address.

The **Configuration** tab contains options that change which functions are used and how the configuration connects with one or more objects.

In the **Configuration** window, the system administrator can use the **Answer BOOTP** option to determine which configuration of the PCs will supply the IP data to the server. New servers or logical partitions that attempt to connect to a local console on a network (LAN) might be using BOOTP. If more than one PC or configuration is allowed to supply the data, the first PC to respond to the broadcast packet supplies this data. Controlling which PC supplies this data might allow the administrator additional flexibility.

An example is when it is desirable to refer to a system within Operations Console with a name other than the name already assigned to the service tools host name (service interface). You have a PC in the computer room that was used to initially set up your server or partition so it uses the real service interface name. You want all the other PCs to display the name as something else. You can create the configured connection on the other PCs to use a fictitious serial number for the server so that BOOTP is always ignored from the configurations of these PCs. However, if you clear this option, you prevent this PC from accidentally configuring the server with the wrong name and still use the real server's serial number. For more information regarding BOOTP, see Bootstrap Protocol.

Also, by enabling the **Allow BOOTP** option, you can edit the subnet mask and service gateway address.

For both local console directly attached configurations, the default IP used for the console is 192.168.0.2. If this PC uses the address range for another purpose, this field provides the user with a convenient method to change the address used by Operations Console. For example, you can use 192.168.1.2.

Note: An initial local console on a network (LAN) configuration configures only the console by default as does a local console that has directly attached configuration. You can turn on or off one of the functions if you do not want to use it.

The **Device ID** tab is no longer available. The PC automatically manages the service tools device ID password even if the system is capable of creating service tools device IDs automatically.

The **Access Password** tab allows you to change the access password. By default, Operations Console will manage this password. However, if you decide to change the password you will then manage this password for the life of the configured connection. The access password is used, in part, to authenticate the device making the connection.

While on the Properties window, you can use the **?** help for more information. You can move the **?** to the field you want more information on, and then click again. A context sensitive help window is displayed containing information regarding that field.

Related concepts

Bootstrap Protocol

Operations Console user interface

Operations Console allows the user more flexibility when interacting with Operations Console and with the graphical interface it provides. By using these features, you can customize the Operations Console window so that you can view and interact with the information most important to you.

Each time Operations Console starts, it searches for new systems that are available to be connected. If no systems are detected and there are no previously configured connections, the setup wizard also starts.

The Options menu item provides the ability to modify the following functions:

Show Warnings
: This option can be used to prevent many of the common dialog windows from displaying. For example, the confirming a delete function dialog window is not displayed if this is not selected.

Prerequisite Warning
: The dialog that is presented during the configuration wizard concerning the requirements can be turned off using this option.

Use Single Sign-on
: This option provides the ability to share common signon data when connecting multiple configurations at the same time. This allows the use of a single signon dialog window instead of one for each connection.

Double-Click
: This option has two items associated with it. The first is for expanding or collapsing the tree structure, the + (plus sign) control. Instead of a single click to expand or collapse, you can change the function to use a double-click. The second item requires the user to use another method for starting a connection instead of double-clicking on the configuration name.

Each configured connection has a + (plus sign) to the left of the icon. The + (plus sign) is a standard Windows expand and collapse function. Each configured connection expands out into separate functions associated with that particular connection. If you right-click on a remote control panel while the configured connection is in expanded mode, a system reference code (SRC) history option becomes available. The SRC history option allows you to retrieve all or part of the recorded SRCs issued by the server. This function can be very useful when you are resolving problems in a variety of situations.

You can drag and drop your configured connections to display them the way you want. This allows you to group configurations together so a common function can be performed on multiple connections at the same time. The standard Windows tagging methods for selecting more than one connection applies. Connections most likely to share functions can be grouped at the top of the list, for example.

Selected data columns can be placed in the order you want them. Using the drag and drop method, you can arrange any column, except iSeries Connection, in the position most useful to you. You can also select which columns to display. From the View menu, select the **Choose Columns** menu. Then, select the columns you want to display and click on the column title to include it or not include it.

Connecting your local console to a server

Learn about the different methods for connecting a local console to a server.

You can connect your local console to a server by these methods:

Connecting a local console on a network (LAN) to a server

Connecting a local console on a network (LAN) to a server allows you to have an active console and a functional remote control panel (if configured).

If you have problems when performing some of these steps, see Network connection errors.

Perform the following steps to connect a local console on a network (LAN) to a server:

1. Click **Start** → **Programs** → **IBM iSeries Access for Windows** → **Operations Console** to start the connection.

   By default, Operations Console does not automatically try to connect a local console on a network (LAN) to a server. If you selected **Start connection when Operations Console starts** in Properties, the local console connects to the server automatically. The connection status displays `Connecting` before changing to `Connecting Console`.
2. If you did not select **Start connection when Operations Console starts** in Properties, you need to connect to the server as follows:
   a. Select the configuration name.
   b. From the Connection menu, click **Connect**.
3. In the LAN Service Device Sign-on window, sign on using your assigned access password, service tools user ID, and password.

   Operations Console needs a valid access password, service tools user ID, and service tools user's password to authorize the connection between the local console and server. For more information, see Working with the service tools device ID. For a visual of this concept, see Configuration security.

   After you sign on successfully, the connection status displays `Connected`.
4. Confirm that the console and remote control panel, if configured, is displayed.

If you encounter other status messages, see Troubleshooting status messages for their descriptions and possible solutions.

To use your PC to access another server, you must connect to another server. For instructions, see Connecting a local console to another server.

Related concepts

Network connection errors

Troubleshooting status messages

Related tasks

Connecting a local console to another server

Related reference

Configuration security

Related information

Working with the service tools device ID

Connecting a local console directly attached

Learn how to connect a local console that is directly attached to a server, to access and control the server.

Perform the following steps to connect a local console that is directly attached:

1. Click **Start** → **Programs** → **IBM iSeries Access for Windows** → **Operations Console** to start the connection.

   By default, Operations Console does not automatically try to connect a local console that is directly attached to a server.
2. If you did not select **Start connection when Operations Console starts** in Properties, connect to the server as follows:
   a. Select the configuration name.
   b. From the Connection menu, click **Connect**.

If you encounter other status messages, see Troubleshooting status messages for their descriptions and possible solutions.

Related concepts

Troubleshooting status messages

Connecting a local console to another server

When using Operations Console, you can have multiple configurations and connect to several servers at the same time, depending on the connectivity type.

Connecting to another server as a local console on a network (LAN), a local console that is directly attached, allows you to work with another server in your network or at a remote location. Only one local console directly attached device is allowed to be configured and connected at one time. You can, however, have multiple local console on a network (LAN) devices configured and connected at one time.

It is assumed that the additional connection has already been created.

Perform the following steps to connect to another server:

1. On the Operations Console Connection window, select the configuration name that you want to connect.
2. From the Connection menu, click **Connect**.

Switching from one console type to another when a console is currently available

If you know in advance that you will need a different console type, you can use the current console to make the changes necessary for use with a different console.

If the hardware resources for the targeted console type have already been specified and configured for use as a console, making the change might be as simple as specifying the new console type value and activating the associated hardware resource. However, if hardware used for the targeted console type requires allocation or configuration, you need to use the appropriate information in Changing consoles, interfaces, and terminals.

An example is the planned loss of the network used by your LAN-connected console. You are doing some infrastructure changes requiring more than a day and you also have the console cable already installed between the server's asynchronous communications adapter and the PC. The server is not managed by an HMC. Using the LAN-connected console you can change the console type to Operations Console (Direct). You can then use the OPSCONSOLE RESTART native macro to force the system to the other configuration. After the asynchronous communications adapter is active, you can disconnect the LAN-connected console and create a configuration for the local console that is directly attached, if a configuration does not already exist, and start a connection.

For systems managed by an HMC, you can dynamically tag a different resource and then force the system to start using the new console. For more information about changing from one console type to another, see Changing consoles, interfaces, and terminals.

To return to the previous console type, you need to use the current console and the same basic method as previously described to make your change.

Notes:

- To force the system to use the new console type, you can choose to have the change take effect immediately or wait until the next time you IPL the server. For an immediate change, you can use the console service functions of 65+21+21 or the native macro OPSCONSOLE RESTART.
- For more information on the console service functions (65+21), see Using the console service functions (65+21). For more information on the Operations Console native macro, see Using the OPSCONSOLE macro.

Related concepts

Changing consoles, interfaces, and terminals

Using the console service functions (65+21)

Related tasks

Using the OPSCONSOLE macro

Switching the console type to recover access to the system

If you develop a problem with the current console, depending on the type of problem, you might be able to recover access to the system by changing the console type.

Note: The following information assumes that hardware to support a new console type is available in the correct location or can be tagged without the need to add or move hardware. Systems with an HMC require that you change at least one tag prior to using a new console type. The tag change, unless performed using a method that does not require an initial program load (IPL), requires you to shut down and activate the system to reflect a change in the partition profile. This same restriction also applies when you are ready to return to the original console type.

Before you start, observe the following:

- Several console service functions (65+21) might be needed to recover or resolve an Operations Console problem. These functions might work depending on the problem, connectivity used for the current console, the target console type, and the current state of the system.
- If you are unsure of any function or recovery action, contact your authorized service provider for assistance.

Use one of the following methods to change the console type:

- If you are using a PC connected to a LAN for the console and have another PC set up to be the console, you might be able to use the other PC for the console until the problem with the first console is fixed.
- Use SST from another workstation.
- Use the console service functions (65+21) to change or reset the console.
- Use the appropriate native macro from another workstation. Any hardware allocations or configurations must be accomplished before connecting with another connectivity. For example, you can use the alternative method for tagging a different console to save an IPL instead of deactivating and activating the partition to enable the change with just the partition profile. Some tasks might require one or more IPLs to get the system into a state where you can use the new console.

For more information about changing to a different console type, see Changing consoles, interfaces, and terminals.

Related concepts

Using the console service functions (65+21)

Changing consoles, interfaces, and terminals

Related tasks

Using the OPSCONSOLE macro

Related information

Access service tools using SST

Working with your local console on a network (LAN)

Learn how to manage and maintain your local console on a network (LAN) configuration.

Establishing multiple connections

By enabling the takeover and recovery function, you can establish multiple connections with local consoles on a network (LAN).

The following behavior exists when the takeover and recovery function is enabled.

When a workstation is already a local console on a network (LAN) and another local console on a network (LAN) connects, the connection is successful and the system displays the DST Sign-on window. After signing on, the user is presented with the Console Information Status window. This window informs the user which device is currently the console. If the user that is signed on has the privilege to take over the console and the device meets all of the requirements of the existing console, then the **Take over the console** field status displays `YES`. Otherwise, the **Take over the console** field status displays `NO` and a brief description of the problem is displayed at the bottom of the screen. Many connections of this type can be connected, but only one connection can be the active console. Also, leaving the newly connected Operations Console PC in this state does not allow Operations Console activities to be automatically transferred to this PC.

If the state of the **Take over the console** field is `YES`, then you can take over the console by pressing F10 and confirm the takeover.

If the state of the **Take over the console** field is `NO`, then you can disconnect the connection using the Operations Console window.

To disconnect the connection, choose one of the following procedures:

- Disconnect the connection using the Operations Console window.
  1. Select the connection name you want to disconnect.

2. Click **Connection** → **Disconnect**.

- Disconnect the Operations Console emulator session.
  1. In the emulator window, click **Connection**.
  2. Select **Disconnect**.

If no device is acting as the console the next time a connection is made, either through Operations Console or the Operations Console emulator, this PC becomes the console.

The following behavior exists when the takeover and recovery function is not enabled.

When a workstation is already a local console on a network (LAN) and another local console on a network (LAN) connects, the connection is successful and the system displays the Console Information Status window. In this window, the **Take over the console** field displays `NO` along with a message indicating the function is not enabled.

Working with console takeover and recovery

The console takeover and recovery function supports Operations Console workstations and the 5250 emulator on the Hardware Management Console (HMC). Before enabling this function, consider the function's requirements and restrictions.

The *takeover* function is the process used for a LAN-connected, console-capable device to take control from the current LAN-connected console device. Because there can be only one local console that is directly attached and the HMC 5250 emulation console can be shared, the takeover function cannot be used with the local console that is directly attached. However, any 5250 emulation-based device can be used to recover a loss of the console by changing the console type. The twinaxial console uses a different form of 5250 emulation and does not qualify as a console type to switch to or from without loss of data. This might require a reallocation of hardware to support the new console.

Tip: Takeover is also supported in a D-mode initial program load (IPL). Two devices can be connected, with data, at the same time during a D-mode IPL, but only one device can be the console at one time.

The *recovery* function is accomplished by suspending the data stream to the console that either loses its connection or is in the process of being taken over. It then saves the data to be delivered when the next device becomes the console. This process takes place even if the newly established console is the same as the former console.

Console recovery uses part of the takeover function. Recovery can be from the same device or another 5250-based device. For example, if you are using a local console on a network (LAN) and have multiple PCs set up to be the console, and the existing console fails, you can use the takeover function from the same PC (after correcting the reason for the failure) or from another PC. Regardless of what the former console was doing, the new console is in the same job, at the same step, as the original console. The job continues even though the original console is not operational.

The current console type is still the only console allowed when takeover is enabled. However, each console-capable workstation is presented with either a DST Sign-on window or the Console Information Status window. If the console is set to Operations Console (LAN), for example, a local console that is directly attached is presented the Console Information Status window without displaying the DST Sign-on window. The **Take over the console** field displays `NO` to indicate it cannot take over the existing console. However, it can be used for a recovery action. When the console type is not set to be the HMC (`4`), the HMC 5250 emulator posts a `Connection refused - partition not configured for HMC console` message.

Every console-capable device that can support 5250 emulation is presented with a window of data regardless of its specific connectivity and regardless of whether it is the console at the time it connects successfully to the server, which means that more than one device has data on the screen after the

console is established. A console-capable device no longer displays a blank screen and a Disconnected state when another device is the active console. Instead, the device displays an error message (HMC) or the Console Information Status window. The key feature of this function is that it allows the job running at the console to be "transferred" to another device without loss of data.

Console takeover and recovery function requirements

Consider the following requirements before enabling the console takeover and recovery function.

- You must enable console takeover if you want to take over a console or if you want to be protected from the loss of the console using the recovery action.
- The DST user ID used to sign on at an eligible device must also have the privilege to take over the console.
- If you do not want takeover capability, but you do want recovery from loss of the console, you must still enable the takeover option. The recovery of the console without data loss is directly tied to the takeover option.

Console takeover and recovery function restrictions

Consider the following restrictions before enabling the console takeover and recovery function.

- Console takeover cannot be used with local consoles that are directly attached to the server.
- Only devices with the same attributes can perform a takeover. For example, if device LAN1 is running in 24 X 80 mode and LAN2 is running in 27 X 132 mode, and LAN1 is the console, LAN2 displays NO in the **Take over the console** field. There are additional device attributes, such as language, that might also prevent a console takeover.
- The console takeover and recovery function does not support twinaxial consoles. This console's configuration uses a different type of 5250 emulation in its connection to the server.

Default setting

The default setting for the console takeover and recovery function is **disabled**. If this function is disabled, all console-capable devices display the Console Information Status window whenever they are not the active console. When the console is set to a 4 (HMC), a local console directly attached device does not automatically connect. An Operations Console LAN-connected device only starts if the network adapter has a valid configuration, such as that provided after configuring the service tools server for iSeries Navigator.

Enabling console takeover

Learn how to grant a user the privilege to take over a console, and then how to enable the console takeover and recovery function.

Before you can perform a console takeover, you must have the privilege to take over the console. Use the following procedure to grant the privilege, and then continue with the next procedure to enable console takeover.

To grant a user the privilege to take over a console using dedicated service tools (DST) or system service tools (SST), perform the following steps:

1. Access service tools using DST or SST.
   - If you are using DST, select **Work with DST environment**.
   - If you are using SST, select **Work with service tools user IDs and devices**.
2. Select **Service tools user IDs**.
3. Type a 7 in front of the desired user ID and press Enter.
4. Scroll down until you find the **Take over console** option and type a 2 on that line to grant the user this privilege.

5. Press Enter.

To repeat this procedure for additional user IDs, repeat steps 4 and 5.

Notes:

1. The privilege to take over a console is used the next time the user ID signs on.
2. When a user signs on at a device capable of taking over the console, the status of the **Take over the console** field is updated. To reflect a change such as a user being granted the takeover console privilege, the user must exit the Console Information Status window using **F3** or **F12** and then sign on again.

To enable the console takeover and recovery function using DST or SST, perform the following steps:

1. Access service tools using DST or SST.
   - If you are using DST, select **Work with DST environment**, and then **System devices**.
   - If you are using SST, select **Work with service tools user IDs and devices**.
2. Select **Select Console**.
3. Type a 1 in the **Allow console recovery and console can be taken over by another console** option and press Enter.

The console takeover option takes effect immediately.

Related information

Access service tools using SST

Access service tools using DST

Considerations for using recovery and a backup console

You might want to consider a backup console plan that involves the need for a change in the console type.

The recoverability of the console using a different console connectivity provides you with additional options. Use the following information if you have a backup console plan that involves the need for a change in the console type.

Changing the console in i5/OS can take effect immediately depending on how you change the console.

- For *systems managed by an HMC*, a change to the console tag is required to use a new console type. If possible, plan for this change in advance. Changing the partition profile usually takes effect only after you power off and then activate the partition. Attempting to change the console type value in DST or SST results in an error message that indicates that the resource is not available. You can, however, force the tag change by using a command line interface to the HMC.
- For *systems not managed by an HMC*, the adapter location takes the place of the tagging. If the adapter of your other console type is located correctly, you can change the console type value. The change takes effect when the system is restarted. Alternatively, you can use the console service functions (65+21) to force the system to check for another console.

If you change the console by using the console service functions (65+21), then the change takes effect immediately.

Supporting hardware for each console type that you want to use for recovery must be available (not in use) at the time of recovery. For example, if you want a local console that is directly attached to be able to recover a local console on a network (LAN) device, both adapters must be located in their respective locations or be correctly tagged. For the console change to be completed, you must change the console type value, either by using an available menu or by using the console service functions (65+21).

To accomplish a recovery by using a different console type, you must satisfy the hardware requirements for the new console before attempting the takeover. This means that either the supporting hardware must already be available (not in use), including any logical partition tagging, or you must move supporting hardware, physically or logically, before attempting the recovery. Then, you must use one of the methods to change the console type value to the desired setting. You can use an existing workstation and SST, if available, the native macro, or the console service functions (65+21).

If you change the console tag during a D-mode initial program load (IPL), typically by using the console service functions (65+21), you are able to connect another device without performing another IPL as long as the new required resources are available. For example, if the input/output adapter to be switched to is not located on the same bus, then the bus on the target resource might not be able to perform an IPL at this time.

Related concepts

Changing consoles, interfaces, and terminals

Using the console service functions (65+21)

Related tasks

Using the OPSCONSOLE macro

Scenarios for taking over or recovering a console connection

Learn about the various methods of the console takeover and recovery function by reading through some scenarios.

Scenario: LAN-connected devices with takeover enabled:

Learn about what happens during the process of starting the server when console takeover is enabled and more than one LAN-connected device is available.

Setting: The LAN devices are called LAN1, LAN2, and LAN3. The mode is unattended (normal mode). The server is going through an initial program load (IPL). At the point in the IPL when the console device is being determined, the first device to connect, of the type specified by the console setting (LAN, in our example), becomes the console and is presented with the usual console windows.

In this example, LAN1 is the first device connected. During the process of starting the server, this device displays the status changes like any other console and eventually the i5/OS Sign-on window. LAN2 and LAN3 display a special DST Sign-on window with a new line of data stating, `ATTENTION: This device can become the console.` The rest of the window is the same as the DST Sign-on window. At LAN2, a user with the privilege to take over the console signs on. This user is now presented with the same Console Information Status window and the **Take over the console** field displays `YES`, indicating that takeover is possible. At LAN3, a user without the console takeover privilege signs on. The **Take over the console** field displays `NO` because here the user does not have the correct authority for takeover.

At this point, only one device has met all the conditions for a console takeover. At the bottom of the screen is `F10=Take over console connection`. Pressing F10 presents the user with the Take over Console Connection From Another User window. This is a confirmation window that gives the user a last chance to cancel the takeover. Selecting 1 and then pressing Enter at this point causes the takeover to occur. Almost immediately, LAN1 receives the special DST Sign-on window and LAN2, the device that initiated the takeover, receives the exact same window LAN1 received when the transfer took place. The job, if something was running, is not aware a takeover is taking place. In fact, the original console can be installing Licensed Internal Code or i5/OS, or even running a complete system save in the restricted state, and the server is unaware of it. You can even disconnect the console connection, reconnect, get the current job's screen data, and the job is unaffected. If a large amount of screen data is sent by the job and cannot be delivered, the data is stored until later. When a console reconnects, by an authorized user who has the privilege to take over a console from an eligible device, the user might see fast screen refreshes until all of the stored data is delivered. Actually, doing a disconnect and a reconnect is considered a recovery (not a takeover).

The data present at LAN3 does not change after the takeover. However, if the user at LAN3 presses Enter, a manual refresh of all the fields except the **Take over the console** field occurs. The user must exit this window and sign on again to see the change to that field.

Scenario: Normal server startup and dual-connectivity configurations with console takeover enabled:

Learn about what happens during the process of starting the server when console takeover is enabled and more than one Operations Console connectivity is being used. That is, a local console directly attached device, of which there can only be one, is connected and three Operations Console LAN devices are connected.

Setting: The console type is set to Operations Console (LAN). The directly attached PC is called CABLED, and the LAN PCs are called LAN1, LAN2, and LAN3. The mode is unattended (normal mode) and the server is going through an initial program load (IPL). At the point in the IPL when the console device is being determined, the first device to connect, of the type specified by the console setting (LAN, in our example), becomes the console and is presented with the usual window a console receives for the type and circumstances in which the server was started. Each additional device that connects is presented with one of two windows.

In this example, LAN1 is the first device connected. During the process of starting the server, this device displays the status changes like any other console and eventually the i5/OS Sign-on window. LAN2 and LAN3 display a special DST Sign-on window with a new line of data stating, `ATTENTION: This device can become the console.` The rest of the window is the same as the DST Sign-on window. The device called CABLED does not initially connect because it does not meet the console type of Operations Console (LAN). However, if the asynchronous communications adapter is activated with a function **66**, it is taken directly to the Console Information Status window where the user can see data related to the current console. The **Take over the console** field displays `NO` since it is not of the correct type, which is Operations Console (LAN). At LAN2, a user with the privilege to take over the console signs on. This user is now presented with the same Console Information Status window and the **Take over the console** field displays `YES`, indicating that takeover is possible. At LAN3, a user without console takeover privilege signs on. The **Take over the console** field displays `NO` because here the user does not have the correct authority for takeover.

At this point, only one device has met all the conditions for a console takeover. At the bottom of the screen is `F10=Take over console connection`. Pressing F10 presents the user with the Take over Console Connection From Another User window. This is a confirmation window that gives the user a last chance to cancel the takeover. Selecting 1 and then pressing Enter at this point causes the takeover to occur. Almost immediately, LAN1 receives the special DST Sign-on window and LAN2, the device that initiated the takeover, receives the exact same window LAN1 received when the transfer took place. The job, if something was running, is not aware this action is taking place. In fact, the original console can be installing Licensed Internal Code or i5/OS, or even running a complete system save in the restricted state, and the server is unaware of it. You can even disconnect the console connection, reconnect, get the current job's screen data, and the job is unaffected. If a large amount of screen data is sent by the job and cannot be delivered, the data is stored until later. When a console reconnects, by an authorized user from an eligible device, the user might see fast screen refreshes until all of the stored data is delivered. Actually, doing a disconnect and a reconnect is considered a recovery (not a takeover).

Scenario: Recovery of a console requiring a new console setting:

Learn about the instances where you must change the console connectivity to recover from a console error. An example of this might be the loss of your network during normal operations.

The console type value can be changed using one of several methods, which include:

- DST or SST menus (delayed)
- Native macros (delayed) (The OPSCONSOLE RESET native macro makes the change immediate.)

- Console service functions (65+21) (immediate)

For immediate change when another workstation is available, use the OPSCONSOLE native macro. You can use the macro to change the console type value and then perform the function OPSCONSOLE RESET to force the system to use the new console type. For more information on using the Operations Console native macro, see Using the OPSCONSOLE macro.

For immediate change when another workstation is not available, use the console service functions (65+21). If you are attempting to install, for example, and the console fails, then the only method available to you is the console service functions (65+21). For more information, see Using the console service functions (65+21).

The other methods previously mentioned might require manual steps to activate the appropriate resources for the new console type. These changes also require that the associated resources are available in a state where they can be used. Changes made using these methods take effect the next time you activate the server, in which case a newly tagged input/output adapter (IOA) allows the local console directly attached to connect.

In this scenario, we are attempting to change the console's connectivity and use another device immediately. You are using a local console on a network (LAN) and the network fails. The console is in use by your logical partition and you have an asynchronous communications adapter available to be tagged for the console. You decide to change the tag to the asynchronous communications IOA to allow a local console that is directly attached to work. You use the alternate procedure (dynamic tagging) to make the tag changes for both the **console** and **Operations Console** tags. You also invoke a **65, 21, 21** from the HMC command line to force the system to find and use the new console type.

After the change is successfully performed, the user must sign on again. Because this scenario is from a local console on a network (LAN) to a local console that is directly attached, the new console does not receive the special DST Sign-on window or the Console Information Status window since it is the only valid console after the console type value change. When the network problem is fixed, the LAN-connected device goes directly to the Console Information Status window and is not able to take control of the console without changing the console type value back to Operations Console (LAN). Takeover is not available when a device is directly connected because only one connection of this type is allowed by the server.

Related concepts

Using the console service functions (65+21)

Related tasks

Using the OPSCONSOLE macro

Related information

Access service tools using SST

Access service tools using DST

Scenario: Recovering the console during a D-mode IPL:

Learn how to recover from a network failure during a D-mode initial program load (IPL) when the configured console is a local console on a network (LAN).

In this scenario, you are installing Licensed Internal Code as part of a system recovery action and the configured console is a local console on a network (LAN). However, the device does not become active and you receive an A6005008 system reference code (SRC). The system is large and it takes a long time to get to this point and you do not want to start over. The system is not managed by a Hardware Management Console (HMC) and the correct asynchronous communications adapter is available without further configuration changes. You can use the console service functions (65+21) to change the console type value. This automatically starts the asynchronous communications adapter associated with the local

console that is directly attached. If you want to use the same PC you are using for the local console on a network (LAN), you disconnect the local console on a network (LAN) and create (or use a previously created configuration) a local console directly attached connection. When the console service functions (65+21) have successfully completed, you connect the local console that is directly attached. This device becomes the console automatically and you are at the expected step. If the network failure precedes the old console in receiving the language window, the new console presents that window. If the failure happens after you started an action, the new console is either running that action or the action might be complete, in which case you see the results of that action.

When your system is managed by an HMC and you have the asynchronous communications adapter installed, you can complete a console change with the logical partition and managed system powered on. For more information, see "Scenario: Recovery of a console requiring a new console setting" on page 64.

Related concepts

Using the console service functions (65+21)

Related tasks

Completing a console change with the logical partition and managed system powered on

Working with the service tools device ID

Learn how to create, reset, and change the service tools device ID passwords.

Note: You only need to perform functions on service tools device IDs when the autocreate service tools device ID function has been turned off with a value of zero, or you are using a user-created service tools device ID.

Considerations for resetting the service tools device ID passwords

Before resetting the service tools device ID password, consider the following:

Important: You must unlock the SST option before you can use it. For more information on unlocking the option, see Unlocking service tools device IDs in SST.

- Manually resetting the service tools device ID password on the client (PC) is not required. After resetting the service tools device ID password on the server, the client automatically resets this password the next time the client successfully connects.
- The service tools device ID password on the PC must be the same as the service tools device ID password on the server. If you reset one, you must reset the other. The client (PC) does this for you automatically, however.
- The Operations Console encrypts the service tools device ID password when you click **Next** in the Access Password window.
- If you are creating a new local console on a network (LAN) that you have not connected yet, and you click **Cancel** after the Access Password window, you can re-create the configuration with the same service tools device ID.
- If you have previously successfully connected using a local console on a network (LAN) at least one time, you must reset the service tools device ID password on the PC and the server. For details, see Resynchronizing the PC's and the server's service tools device ID passwords.
- Operations Console changes and re-encrypts the service tools device ID password during each successful connection.
- If you delete the local console on a network (LAN) configuration after connecting, you must reset the service tools device ID password on the server before you reuse the service tools device ID for a new local console on a network (LAN) configuration. For instructions about resetting the device profile password, see Resynchronizing the PC's and the server's service tools device ID passwords.
- If the configuration you just deleted was using QCONSOLE as the service tools device ID, do not reset the password until the next time you create a configuration. This is a security restriction to prevent unauthorized entry.

If you need to reset the service tools device ID password, see Resetting the service tools device ID password on the PC and server.

Related concepts

Resynchronizing the PC's and the server's service tools device ID passwords

Resetting the service tools device ID password on the PC and server

Related tasks

Unlocking service tools device IDs in SST

Resetting the service tools device ID password on the PC and server

You do not need to reset the service tools device ID password unless the passwords on the PC and server have gotten out of synchronization and you have received an error message.

Note: You only need to perform functions on service tools device IDs when Autocreate service tools device ID has been turned off with a value of zero, or you are using a user-created service tools device ID.

If this is the case, see Resynchronizing the PC's and the server's service tools device ID passwords to make them both the same again. Because this password is actually changed at each successful connection, manually changing the password, except for synchronization, is not necessary.

Related concepts

Resynchronizing the PC's and the server's service tools device ID passwords

Unlocking service tools device IDs in SST

Learn how to unlock the service tools device IDs using system service tools (SST).

By default, this option is locked to prevent unauthorized changes to existing service tools device IDs, the creation of new IDs, or the deletion of IDs. This procedure can only be performed in dedicated service tools (DST). To unlock this SST option, complete the following steps:

Note: If you receive the message, `The user can not perform the option selected`, this indicates that the option is not unlocked.

1. Access service tools using DST. This procedure can only be performed in DST.
2. Depending on your Licensed Internal Code (LIC), complete the steps in one of the following options.
   - For servers with V5R4 or later LIC installed, complete the following steps:
     a. Select **Work with DST environment** → **Service tools security data**.
     b. Type a 7 next to the **Work with lock for device IDs from SST** option, and then press Enter. The status displays as `Enabled`.
   - For servers with V5R2 or V5R3 LIC installed, complete the following steps:
     a. Select **Start a service tool** → **Display/Alter/Dump** → **Display/Alter storage** → **Licensed Internal Code (LIC) data** → **Advanced analysis**.
     b. Page down until you find the **FLIGHTLOG** option. Type a 1 next to the option, and then press Enter. The Specify Advanced Analysis Options window is displayed. The command displays as `FLIGHTLOG`.
     c. Enter the **SEC UNLOCKDEVID** option. To lock the Service Tools Device IDs menu, enter the **SEC LOCKDEVID** option.

Related information

Access service tools using DST

Deallocating or moving the Operations Console LAN adapter

You might need to deallocate the LAN adapter from use by Operations Console. A migration is one example of why you might need to do this.

Plan to deallocate the LAN adapter if you are not using a local console on a network (LAN) configuration even as a backup, or use the service tools server. After the LAN adapter is deallocated, you can move it or use it for another purpose. You must also be using a workstation other than a local console on a network (LAN) because the following steps might cause the console to disconnect.

Deallocating the LAN adapter currently associated with a local console on a network (LAN) is accomplished by using either the dedicated service tools (DST) or the system service tools (SST). However, you must unlock the SST option before you can use it. For additional information on SST, see Unlocking service tools device IDs in SST.

1. Access service tools using DST or SST.
   - If you are using DST, select **Work with DST environment**, and then **System devices**.
   - If you are using SST, select **Work with service tools user IDs and devices**, and then **Configure service tools LAN adapter**.
2. Press F6 to perform a clear, and then F7 to store the new values.

Important:

- You must change the console type, and possibly the console tag if you are using an HMC.
- You must change the console tag to something other than Operations Console (LAN), or the adapter is reallocated the next time you start the system.

Related tasks

Unlocking service tools device IDs in SST

Related information

Access service tools using SST

Access service tools using DST

Changing network values

Learn how to change the network adapter's network data, the adapter used for a local console on a network (LAN), or the service tools server, such as a new IP address.

Note: You only need to perform functions on service tools device IDs when Autocreate service tools device ID has been turned off with a value of zero or you are using a user-created service tools device ID.

To make network changes, complete the following steps:

1. Access service tools using dedicated service tools (DST) or system service tools (SST).
   - If you are using DST, select **Work with DST environment** → **System devices**.
   - If you are using SST, select **Work with service tools user IDs and devices**.

     Note: You must unlock the SST option before you can use it. For additional information on SST, see Unlocking service tools device IDs in SST.
2. Select **Select Console**.
3. Select **Operations Console (LAN)**. The LAN adapter currently in use is displayed.
4. Press F11.
5. Use one of the following methods to make your change:
   - If you are making a simple change, such as the IP address, enter the new values.
   - If you are changing the adapter card, press F6 to clear the value.
6. Press F7 to store the new values.
7. Press F3 until the DST main menu is displayed.

Important: If the change does not affect the network IP address or the service host name (interface name), you can exit these instructions now. The change is reflected on the next IPL or the next time the console is restarted. To force an immediate change, you can use OPSCONSOLE RESTART. This causes the current console to disconnect.

If you made a change that caused the network IP address or service host name (interface name) to be different for the currently configured connections, this change must be reflected on all PCs that connect to this service host name (interface name). Since you cannot modify the network IP address or service host name (interface name) of an existing connection's configuration on the client, you must delete the current connection and recreate a new connection using the new network IP address. Continue with step 8.

8. Reset the service tools device ID password on the server if the system does not have auto-create service tools device ID enabled.
   a. Access service tools using DST or SST.
      - If you are using DST, select **Work with DST environment**.
      - If you are using SST, select **Work with service tools user IDs and devices**.
   b. Select **Service tools user IDs**.
   c. Type a 2 in front of the service tools device ID to be reset, and press Enter.
   d. Press Enter again to confirm the reset.

      Important: If more than one PC connects to this service host name (interface name) using a network connection you must delete the configurations and therefore, reset the service tools device IDs of those PCs as well. To reset another service tools device ID, repeat these steps.

      Note: When you reset the password in DST, the device ID password becomes the device ID name in uppercase letters.
   e. Press F3 until the DST main menu is displayed.
9. Choose *one* of the following methods to complete the network changes.

   There are two methods for completing the necessary work to allow a new IP address or service host name (interface name). The first is restarting the server. This is the recommended method because you have more control when you do the remaining work on the PC. The system continues to use the old values until you restart the server. The second method is the manual intervention. This method forces the system to use your change immediately.

   - **Restart the server**

     This method requires that the client reconfiguration be complete prior to establishing the next connection using a local console on a network (LAN). If you are currently using the local console on a network (LAN), you can start the server (in attended mode) and reconfigure the client during the process of starting the server. You can, for example, use a different PC as the console instead of the one you currently have connected. You can complete the configuration on that PC using the steps here. After the server is started, you can disconnect the current console PC's connection and start a connection on the other PC with the newly created configuration. In this manner, you can reconfigure the existing client at your leisure, before the next connection to the server.
     a. Choose from the following options:
        – If you have an HMC, use the HMC to power on the managed system.
        – If you do not have an HMC, start the server in attended mode. See Start or stop the system or logical partition.
     b. Continue with Completing the PC changes.
   - **Perform a manual intervention**

     This method forces the system to use your change immediately.
     a. Access service tools using DST or SST.
        – If you are using DST, select **Work with DST environment**, and then **System devices**.

– If you are using SST, select **Work with service tools user IDs and devices**.

Note: This causes all LAN-connected console PCs to display `Connecting console` as a status. Also, if more than one LAN-connected console PC is connected, the selection of the next console device is unpredictable.

b. Continue with Completing the PC changes.

Important: To force an immediate change, you can use OPSCONSOLE RESTART.

Related concepts

Resetting the service tools device ID password on the PC and server

Related tasks

Unlocking service tools device IDs in SST

Using the OPSCONSOLE macro

Start or stop the system or logical partition

Completing the PC changes

Related information

Access service tools using SST

Access service tools using DST

Completing the PC changes

Learn how to complete the changes to the PC by deleting the old configuration and creating a new one.

To complete the PC changes, follow the steps below:

1. To delete the old configuration, perform these steps:
   a. Select the configuration name (under iSeries Connection). This is the name that Operations Console uses to refer to a specific server.
   b. From the Connection menu, click **Disconnect**. The connection status displays `Disconnecting`.
   c. Wait for the status to display `Disconnected`.
   d. Select the configuration name (under iSeries Connection).
   e. From the Connection menu, click **Delete**. Optionally, you can press the Delete key.
   f. Click **Yes** to confirm the deletion if prompted.
2. Close and reopen Operations Console to purge the PC of network data associated with the configuration you are changing.

   Note: It is also suggested that you remove or alter the old entry in the **hosts** file on the PC. You can do a search for **hosts** and then use a text editor to edit the file.
3. Create a new configuration using the following steps:
   a. From the Connection menu, select **New configuration**.
   b. Continue the configuration and enter the new IP data or service host name at the appropriate time.
   c. Complete the rest of the new configuration.

The PC is now ready to make a connection. If you have already started the system, you are now ready to reconnect using the new network data.

Activating the asynchronous communications adapter on the server

Learn how to manually activate the asynchronous communications adapter for use with Operations Console with or without an HMC.

The following procedures explain how to activate an asynchronous communications adapter on the server manually. You can activate the asynchronous communications adapter manually whether you have a local Hardware Management Console (HMC) or not. (A local HMC is one that is connected to the server directly through a private network.) Refer to the appropriate procedure for your system.

Related concepts

D1008065 after attempting to activate the asynchronous communications adapter

Related tasks

Failure to display D1008065 and D1008066 automatically after calling the function

Activating the asynchronous communications adapter on a server with an HMC

To activate an asynchronous communications adapter on a server with an HMC, follow these steps:

1. Select from the following options:
   - If you are using an HMC with Version 6 or earlier, continue with step 2.
   - If you are using an HMC with Version 7 or later, continue with step 3.
2. Perform the following steps:
   a. In the navigation area, expand the managed server's entry with which you want to work.
   b. Expand **Service Applications**, then click on **Service Focal Point**.
   c. In the contents area, click **Service Utilities**.
   d. From the Service Utilities window, select the managed system with which you want to work.
   e. From the Selected menu on the Service Utilities window, select **Operator Panel Service Functions**.
   f. From the Operator Panel Service Functions window, select the logical partition with which you want to work (it might be the only partition on your system).
   g. From the Partition Functions menu on the Operator Panel Service Functions window, select **Enable Remote Service (66) — i5/OS**.
3. Perform the following steps:
   a. In the navigation area, click **Systems Management** → **Servers**.
   b. In the contents area, select the managed system you want to work with.
   c. Click **Tasks** → **Serviceability** → **Control Panel Functions** → **(66) Enable Remote Service**.

The system attempts to initialize the asynchronous communications adapter. If it is successful, the Function/Data window displays system reference code (SRC) D1008066. If the modem initialization is unsuccessful, the Function/Data window displays D1008065 after attempting to activate the asynchronous communications adapter.

Activating the asynchronous communications adapter on a server without an HMC

To activate an asynchronous communications adapter on a server without an HMC, follow these steps:

1. Use the system's control panel to place the server into manual mode
2. Use the Up and Down buttons to select function **25**, and then press Enter.
3. Use the Up button to select function **26**, and then press Enter.
4. Use the Down button to select function **66**, and then press Enter.

The system attempts to initialize the asynchronous communications adapter. If it is successful, the Function/Data window displays the system reference code (SRC) D1008066. If the modem initialization is unsuccessful, the Function/Data window displays D1008065 after attempting to activate the asynchronous communications adapter. If the system fails to produce an SRC automatically, you might

need to manually attempt to retrieve the results. For more information, see Failure to display D1008065 and D1008066 automatically after calling the function.

Deactivating the asynchronous communications adapter on the server

Learn how to manually deactivate an asynchronous communications adapter in use with Operations Console with or without an HMC.

The following procedures explain how to deactivate an asynchronous communications adapter on the server manually. You can deactivate the asynchronous communications adapter manually whether or not you have a local HMC. A local HMC is one that is connected to the server directly through a private network. Refer to the appropriate procedure for your system.

Related concepts

D1008065 after attempting to activate the asynchronous communications adapter

Related tasks

Failure to display D1008065 and D1008066 automatically after calling the function

Deactivating the asynchronous communications adapter on a server with an HMC

Deactivate an asynchronous communications adapter on a server with an HMC.

1. Choose from the following options:
   - If you are using an HMC with Version 6 or earlier, continue with step 2.
   - If you are using an HMC with Version 7 or later, continue with step 3.
2. Perform the following steps:
   a. In the navigation area, expand the managed server's entry with which you want to work.
   b. Expand **Service Applications**, then click on **Service Focal Point**.
   c. In the contents area, click **Service Utilities**.
   d. From the Service Utilities window, select the managed system with which you want to work.
   e. From the Selected menu on the Service Utilities window, select **Operator Panel Service Functions**.
   f. From the Operator Panel Service Functions window, select the logical partition with which you want to work (it might be the only partition on your system).
   g. From the Partition Functions menu on the Operator Panel Service Functions window, select **Disable Remote Service (65) — i5/OS**.
3. Perform the following steps:
   a. In the navigation area, click **Systems Management**.
   b. In the navigation area, click **Servers**.
   c. In the contents area, select the managed system you want to work with.
   d. Click **Tasks** → **Serviceability** → **Control Panel Functions** → **(65) Disable Remote Service**.

The system attempts to deactivate the asynchronous communications adapter. If it is successful, the Function/Data window displays system reference code (SRC) D1008065. If the modem initialization is unsuccessful and SRC D1008065 is not displayed, see Failure to display D1008065 and D1008066 automatically after calling the function.

Deactivating the asynchronous communications adapter on a server without an HMC

Deactivate an asynchronous communications adapter on a server without an HMC.

1. Use the system's control panel to place the server into manual mode
2. Use the Up and Down buttons to select function **25**, and then press Enter.
3. Use the Up button to select function **26**, and then press Enter.
4. Use the Down button to select function **65**, and then press Enter.

The system attempts to deactivate the asynchronous communications adapter. If it is successful, the Function/Data window displays system reference code (SRC) D1008065. If the modem initialization is unsuccessful and SRC D1008065 is not displayed, see Failure to display D1008065 and D1008066 automatically after calling the function.

Changing the autocreate service tools device ID

By default, the system manages service tools device IDs automatically. However, if necessary, you can either turn off this function or increase the value for the number of automatically created service tools device IDs.

You can only access the option using dedicated service tools (DST).

To change the autocreate service tools device ID, follow these steps:

1. Access dedicated service tools (DST).
2. Select **Work with DST environment**.
3. Select **Service tools security data**.
4. Perform one of the following:
   - To change the value of the option **Autocreate service tools device IDs**, enter a value 1 - 49.
   - To turn off the autocreate service tools device IDs function, enter a value of 0.
5. Move the cursor to the input line at the bottom, select the option for **Autocreate service tools device IDs**, and press Enter.

Troubleshooting Operations Console connections

Find possible solutions to connection, authentication, emulator, and other problems when using Operations Console.

Problems can occur during an Operations Console session, whether they are encountered during your initial setup or while managing your configuration. If you have a console problem that you cannot overcome using the troubleshooting section and you need to change the console type, see Changing consoles, interfaces, and terminals.

The Operations Console client (PC) keeps a set of log files to be used only by IBM. These log files can help assist with user problems. If you report a problem to your service provider, you might be asked to send specific log files from the PC.

Settings dialog window

Operations Console has a built-in, hot-key-activated, Settings dialog window that has special options used to help troubleshoot problems. The Settings window is activated by pressing and holding the Alt, Shift, and s keys (Alt+Shift+s). The options to split the log files can be very helpful to your service provider, especially if you have many connection configurations. Splitting the logs so each configuration has its own log makes it easier to find problems. When only one connection has a problem, activity in other connections are not seen in the log.

Important: Do not make any other changes or turn on any other functions without advice from the service provider. Improper use of the options on this window can cause unpredictable behavior on any or all configured connections.

There is also a hot-key-activated function to capture the screen data when the connection is not responding correctly. To capture the screen data, select the configuration and press and hold the Ctrl and c keys (Ctrl+c). This action dumps the contents of the last 10 screen buffers (three screens of data) and the timestamp they were received into the connection log. This log can be used by service and support to see what the last updates to the emulator were. Activating this process a again, without changes to the window, does not output any more data to the connection log.

When Operations Console is started the discovery process is started. If you have active connections to other systems and just completed the setup of a new system that should be able to be discovered, you can activate a new discovery by pressing and holding the Alt and shift keys, then press the w key (Alt+Shift+w). Your new system is displayed, and you can start a connection to it.

Related concepts

Changing consoles, interfaces, and terminals

Troubleshooting status messages

If you encounter connection problems when connecting a console, Operations Console provides status messages, indicating whether or not you have a connection problem, to assist you in troubleshooting the connections. It is displayed under `Status` in the Connection details area of the Operations Console window.

Before you start troubleshooting the connection, verify you have the latest service packs for iSeries Access for Windows. For instructions, see Applying iSeries Access for Windows service packs.

Related concepts

Troubleshooting connection problems

Local console does not detect console cable

Related tasks

Remote control panel fails to start

Related reference

Applying System i Access service packs

Status messages when configuration is running correctly

These status messages indicate you *do not* have connection problems.

Connecting console or Connecting remote control panel
: Displayed while the console is making the initial connection to a server. If it is displayed for more than a couple of minutes, see Connecting console in the list of status messages that indicate connection problems.

Pending authorization
: Displayed during an initial connection to a server when the Service Device Sign-on window is displayed. This status remains until a first user signs on successfully. A local console on a network (LAN) always posts the LAN Service Device Sign-on window the first time a connection is made. Subsequent connections to the same server do not re-prompt the user.

Connected
: Displayed at the local console after an initial connection to the server is completed (the user signed on successfully to Operations Console).

Disconnecting
: Displayed at the local console when the local console user disconnects from a server and the PC is disconnecting the connection.

Disconnected
: Displayed at the local console after the local console user disconnects from a server and the PC is no longer communicating with the server.

Status messages when you have connection problems

These status messages indicate you *do* have connection problems.

Remote control panel unavailable
: Displayed during an initial connection to a server. It is displayed when there is a problem with the remote control panel connection, and you choose not to retry the connection. To find a possible solution, see Remote control panel fails to start.

Connecting remote control panel
: Displayed when the connection fails during the initial connection or stops working after the initial connection. To find a possible solution, see Troubleshooting connection problems. This status message disappears when you solve the problem.

Connecting console
: Displayed while the console is making the initial connection to a server. If it is displayed for more than a couple of minutes, the connection failed. It also displays when the connection stops working after the initial connection. To find a possible solution, see Troubleshooting connection problems.

Connecting console or Connecting remote control panel
: Displayed when the console and remote control panel connections fail or stop working. To find a possible solution, see Troubleshooting connection problems. This status message disappears when you solve the problem.

Console unavailable
Displayed when there is a problem during an initial connection to a server and you choose not to retry the connection. It usually displays when the Operations Console connection modem is not available, but the Operations Console cable is attached. The Operations Console connection modem is not a physical modem, but a logical device driver that is included with Operations Console and allows a local console to connect to a server. To find a possible solution, see Troubleshooting connection problems.

Console unavailable or Remote control panel unavailable
Displayed when there is a problem during an initial connection to a server, and you choose not to retry the connection for the console or remote control panel. It indicates that there is a problem with the console connection, possibly because the Operations Console connection modem is not available or the console cable is disconnected. The Operations Console connection modem is not a physical modem, but a logical device driver that is included with Operations Console and allows a local console to connect to a server. It also indicates that there is a problem with the remote control panel connection. To find a possible solution, see Local console does not detect console cable and Remote control panel fails to start. In each case, the user selected `No` to a previous message allowing the user to retry the failing function.

Troubleshooting connection problems

Find possible solutions to connection problems that might be encountered during your Operations Console connection.

Local console

When connecting your local console, you might encounter problems. Failure to connect is defined as problems resulting in the status not going to `Connected` and the emulator not starting.

Console fails to start

Under certain circumstances, a local console that is directly attached fails to connect. This might be the result of the server's asynchronous communications adapter being deactivated for some reason, such as an exception that takes place.

This deactivation most likely results when you start your server and have an associated system reference code (SRC) on the control panel or Hardware Management Console)HMC), if installed, along with the attention light.

To reset the asynchronous communications adapter with or without an HMC, see "Deactivating the asynchronous communications adapter on the server" on page 72.

If the deactivation is successful, the Function/Data window (or the HMC) displays `D1008065`.

To activate the asynchronous communications adapter on the server with or without an HMC, see Activating the asynchronous communications adapter on the server.

The system attempts to initialize the adapter. If it is successful, the Function/Data window (or the HMC) displays `D1008066`. If it cannot initialize the asynchronous communication adapter, it displays D1008065 after attempting to activate the asynchronous communications adapter. If the expected SRC is not displayed after several minutes on servers without an HMC, see Failure to display D1008065 and D1008066 automatically after calling the function.

Related concepts

D1008065 after attempting to activate the asynchronous communications adapter

Related tasks

Deactivating the asynchronous communications adapter on the server

Activating the asynchronous communications adapter on the server

Failure to display D1008065 and D1008066 automatically after calling the function

Network connection errors

Learn about some possible solutions to try if you are experiencing problems that occur when a local console on a network (LAN) fails to connect to a server.

Try these possible solutions:

- Verify the network is working.
- Verify that you provide the correct password to allow the server to access your service device information during the configuration wizard. Also, verify that you are providing the correct service tools user ID and password.
- If you are using Ethernet for your network, you can use a crossover cable to directly connect the PC to the adapter temporarily. This isolates the PC and server from any potential problems on your network that might interfere with correct operations.

  Note: A crossover cable is a standard network cable that has the transmit and receive signal wires reversed. This essentially allows each end to act as if a hub, switch, or router is between them.

Error message: Connection to system is not secure

Learn about why this error message is received when there is an unsecure connection.

These messages are appropriately displayed during a D-mode (installation) initial program load (IPL). Authentication is not performed and the remote control panel (LAN) is not supported for this type of IPL.

Status remains `Connecting`

Learn about some possible solutions to try if you are experiencing problems that prevent the local console from connecting to the server due to incorrect hardware or software configurations.

Try these possible solutions:

- Verify that the PC resources are free of address or interrupt request (IRQ) conflicts. Operations Console uses addresses in the range of `192.168.0.0` to `192.168.0.255`. If you run any software that makes your PC SOCKS-enabled, check your SOCKS configuration and make sure that the entry is:

  ```
  Direct     192.168.0.0     255.255.255.0
  ```

  Note: Use the Operations Console properties window to change the IP base address from 192.168.0.2. For example, you can use 192.168.1.2.

  A SOCKS-enabled PC accesses the Internet through a firewall, such as Microsoft Proxy Client, Hummingbird SOCKS Client, or others.
- For a local console on a network (LAN) configuration and you are using Ethernet for your network, you can use a crossover cable. This isolates the PC and server from any potential problems on your network that might interfere with correct operations.

  Note: A crossover cable is a standard network cable that has the transmit and receive signal wires reversed. This essentially allows each end to act as if a hub, switch, or router is between them.

Related concepts

Operations Console properties window

Console connection and port detection fails

Learn about some possible reasons why your local console that is directly attached fails to connect and why your port detection fails.

Possible reasons for connection failure include:

- Occasionally RealPlayer or RealJukebox interferes with port detection and usage.
- Some PDA drivers or software might prevent connections or port detection.

Performance degradation

Learn about some possible reasons for performance degradation on a local console directly attached connection involving the communications port.

The most likely reason for performance degradation is that the communication port is not running a buffered UART (Universal Asynchronous Receive/Transmit serial port chip). This can be verified in the **Advanced** settings for the serial port. You must verify the buffered UART is selected, and that the **Receive Buffer** setting is not set to the right-most setting.

If this attempt does not help and you suspect that there is a possibility that the PC might truly not have the buffered UART, slow the connection down between the PC and server. Depending on the operating system, you might have to change the registry, the DUN object, or the telephone book entry, or all three.

The problem with the unbuffered UART is that the high-speed connection inputs data to the UART faster than it can handle, which causes missed packets of data resulting in a 30-second retry. This can occur randomly, but becomes persistent. The slower speed reduces the exposure to an overrun of data and therefore, no more 30-second retries.

Unable to connect with infrared devices installed

Learn about a possible solution to try if the PC is having connection problems when using infrared devices and a local console with a directly attached connection.

If the PC that is having connection problems has infrared devices (many notebooks use this), you might need to disable infrared in some cases. Most of these devices work from COM1, but fail to display as using the associated hardware resources. Some experimentation might need to be performed to isolate the problem during configuration of Operations Console.

Unexpected disconnections

Local PCs that have power-management capabilities can cause disconnected connections.

If the local PC has power-management capabilities, disable this function. Most PCs, and especially notebooks, reset the communications ports when invoking power management after the specified time. This can potentially disconnect the established connection.

Session unexpectedly disconnects

Learn about a possible solution to try if you have a console session that unexpectedly disconnects while working with a local console that is directly attached.

If the console session closes unexpectedly and the status is `Connecting console`, the input/output processor (IOP) that controls the console might experience a reset/reload. When the IOP, particularly the MFIOP, goes into a reset or reload, the connection to the local console that is directly attached does not automatically reconnect. You must perform a control panel function **65**, and then a function **66** to manually reactivate the connection. For more information on deactivating and activating the asynchronous communications adapter, see Deactivating the asynchronous communications adapter on the server and Activating the asynchronous communications adapter on the server.

Related tasks

Deactivating the asynchronous communications adapter on the server

Activating the asynchronous communications adapter on the server

Using HyperTerminal to validate connectivity

Use HyperTerminal to assist in determining if the connection between the client (PC) and server is good when using a local console that is directly attached.

HyperTerminal is a Windows application used for connecting to various sources and is supplied by all Windows operating systems on the installation media, though might not be automatically installed. When the local console directly attached does not connect, you can use HyperTerminal to determine if the PC has connectivity to the server.

Note: The data is slow to display so be sure to allow 15 - 20 seconds for an action to complete before moving to the next step. Also keep in mind that some steps might not provide data to the window.

Installing HyperTerminal:

Learn how to install HyperTerminal.

To install HyperTerminal, complete the following steps:

1. Click your path depending on your Windows operating system.
   - **Start** → **Programs** → **Accessories** → **HyperTerminal**
   - **Start** → **Programs** → **Accessories** → **Communications** → **HyperTerminal**

   Note: Make sure that you use the executable file and not one of the predefined connections or the folder.
2. If the executable file is not found, use these instructions to install it:
   a. Place the installation media, if CD, into the CD-ROM drive and wait for the program to begin. Then, close the window. If the program does not automatically start, or the installation media is not a CD, continue with the next step.
   b. Click your path depending on your Windows operating system.
      - **Start** → **Control Panel**
      - **Start** → **Settings** → **Control Panel**
   c. Double-click **Add/Remove Programs**.
   d. Click **Windows Setup** tab.
   e. Click **Communications**.
   f. Click **Details**.
   g. Select the HyperTerminal check box.
   h. Click **OK**, and then **Apply**.
   i. Follow the instructions in any prompts that might display. If you are presented a window in which you might replace a newer file with an older one, click **Yes** to keep the newer file.

When you are ready, see Using HyperTerminal.

Related tasks

Using HyperTerminal

Using HyperTerminal:

Learn how to use HyperTerminal.

If you have not installed HyperTerminal, see Installing HyperTerminal. To use HyperTerminal, complete the following steps:

1. Click your path depending on your Windows operating system.
   - **Start → Programs → Accessories → HypertTerminal**
   - **Start → Programs → Accessories → Communications → HypertTerminal**
2. In the Connect To window, enter a name, select an icon, and then click **OK**. A new Connect To window is displayed.
3. Click the little arrow at the end of the line for **Connect using:**.
4. Select the communications port being used for the console. It might also be listed as **direct to COMn** (where n is 1 to 9).
5. Click **OK**. A COMn Properties window is displayed.
6. Change the speed to **9600**, and click **OK**. The HyperTerminal window opens. In the lower-left corner, the status displays `Connected` and the time is incrementing. In the data window you might see:
   - No text
   - Unintelligible text
   - +++ATH0

   Note: Failure to set the speed to 9600 results in all unintelligible text and you will not be able to view the desired results.
7. Select **Disconnect**.
8. Select **File → Properties**.
9. In the Properties window for the connection you just created, click the **Settings** tab.
10. Click **ASCII Setup**.
11. Select the following check boxes:
    - **Send line ends with line feeds**
    - **Echo typed characters locally**
    - **Append line feeds to incoming line ends**
    - **Wrap lines that exceed terminal width**
12. Click **OK**, and then click **OK** again.
13. Select **Connect**.
14. At the server's control panel, enter a function **65** (you must take the server to a known state). The server's control panel might display `D1008065` after a few minutes. Also, in the HyperTerminal window, you might receive some data.

    Note: You might need to enter a function **25** and **26** to have access to the upper functions.
15. At the server's control panel, enter a function **66**. The panel might display `D1008066`. Also, in the HyperTerminal window, you might receive some data.
16. Using uppercase letters, type `NEGOTIATE 1` in the HyperTerminal window, and press Enter. The HyperTerminal data window displays `115200`.

    Note: If nothing is returned, repeat **NEGOTIATE 1**.

    If a speed value is returned, you had data exchanged in both directions and have full connectivity. If Operations Console is not connecting, you most likely have a setup problem on the client side.

    If a speed value was not returned, you might try powering off the PC, powering it back on, and repeating the test. You might also attempt to connect the console again. In rare cases the server might need to be restarted. For the best results, complete the following steps in sequence:

    a. Power off the server.

    b. Power off the PC.

c. Power on the PC.
d. Start a connection for the console.
e. Power on the server.

If the above procedure fails to solve your connection problem, contact your service provider for further assistance.

Related tasks

Installing HyperTerminal

Resynchronizing the PC's and the server's service tools device ID passwords

Learn how to resynchronize the PC's and the server's service tools device ID passwords when they do not match.

Note: You only need to perform functions on service tools device IDs when Autocreate service tools device ID has been turned off with a value of zero or you are using a user-created service tools device ID.

When a mismatch occurs in the service tools device ID password between the server and the Operations Console PC, the following error message is displayed: `The PC service tools device ID password and the iSeries service tools device password do not match. Either the service tools device ID <name of device ID> is already in use or the passwords must be reset on this PC and the iSeries.` In this case, you need to resynchronize the password by performing recovery steps on the server.

Note: To reset the service tools device ID using the service tools device, you must access service tools using DST or SST. If another workstation capable of SST is present, you can use it. Otherwise, you might have to do one of the following:

- Use a different local console on a network (LAN), if available.
- Reconfigure the same local console on a network (LAN) using an unused emergency service tools device ID.
- Use an Operations Console local console that is directly attached to the server (if an Operations Console cable is available).
- Use a twinaxial-attached console.
- Use the control panel or remote control panel to reset QCONSOLE, if available.

For instructions on resetting the service tools device ID password on the server or logical partition, see Resetting the service tools device ID password on the server or logical partition.

Note: The PC does not require the service tools device ID password to be reset manually. It automatically detects a reset on the server and resets itself on the next connection. If you feel that this automatic process failed, see Manually resetting the service tools device ID password on the PC.

Related concepts

Resetting the service tools device ID password on the server or logical partition

Manually resetting the service tools device ID password on the PC

Related information

Access service tools using SST

Access service tools using DST

Resetting the service tools device ID password on the server or logical partition

Learn about the various ways to reset the service tools device ID password on the server or logical partition.

Note: You only need to perform functions on service tools device IDs when Autocreate service tools device ID has been turned off with a value of zero or you are using a user-created service tools device ID.

Resetting the service tools device ID password using another device:

Learn how to reset the service tools device ID password on the server if you can obtain a console session or access system service tools (SST) using another device.

Resetting the service tools device ID password using another device is accomplished by using either the dedicated service tools (DST) or the SST. However, you must unlock the SST option before you can use it. For additional information about SST, see Unlocking service tools device IDs in SST.

1. Access service tools using DST or SST.
   - If you are using DST, select **Work with DST environment**.
   - If you are using SST, select **Work with service tools user IDs and devices**.
2. Select **Service tools device IDs**.
3. Type 2 in front of the service tools device ID to be reset, and then press Enter.
4. Press Enter again to confirm the reset.

Related tasks

Unlocking service tools device IDs in SST

Related information

Access service tools using SST

Access service tools using DST

Resetting the service tools device ID password using an unused service tools device ID:

Learn how to reset the service tools device ID password on the server if you do not have another device to sign on to the system, but do have an unused service tools device ID.

1. Delete the current configuration as follows:
   a. Select the configuration name (under iSeries connection).
   b. From the Connection menu, click **Delete**.
   c. Click **Yes** to confirm the deletion if you are prompted.
2. Create a new configuration and use the unused service tools device ID during the configuration.
3. Use one of the methods listed in Resetting the service tools device ID password on the server or logical partition to reset the failing service tools device ID after connecting.

Related concepts

Resetting the service tools device ID password on the server or logical partition

Resetting the default service tools device ID:

If you cannot use another service tools device or service tools device ID to sign on and you are using the default service tools device ID (QCONSOLE), you must use the control panel, the remote control panel, or the Hardware Management Console (HMC) to reset the service tools device ID password.

Note: Disconnect the affected connection before starting this function.

Related tasks

Putting the physical control panel in manual operating mode

Resetting the service tools device ID password using the HMC:

Use this task to reset the service tools device ID password using the HMC.

1. Choose from the following options:
   - If you are using an HMC with Version 6 or earlier, continue with step 2.
   - If you are using an HMC with Version 7 or later, continue with step 3.
2. Perform the following steps:
   a. In the navigation area, expand the managed system you want to work with.
   b. Expand **Service Applications** and click **Service Focal Point**.
   c. In the contents area, click **Service Utilities**.
   d. From the Service Utilities window, select the managed system you want to work with.
   e. From the Selected menu on the Service Utilities window, select **Operator Panel Service Functions**.
   f. From the Operator Panel Service Functions window, select the logical partition you want to work with. This logical partition might be the only logical partition on your system.
   g. From the Partition Functions menu on the Operator Panel Service Functions window, select **Disable Remote Service (65) — i5/OS**
   h. Repeat step 2g seven times.
3. In the navigation area, click **Systems Management**.
4. In the navigation area, click **Servers**.
5. In the contents area, select the managed system you want to work with.
6. Click **Tasks** → **Serviceability** → **Control Panel Functions** → **(65) Disable Remote Service**.
7. Repeat step 6 seven times. To view the resulting system reference code (SRC) data, complete the following steps:
   a. Click **Tasks** → **Serviceability** → **Reference Code History**.
   b. Select the reference code D1008065 at the top of the list. This refreshes the window with the reference code details so that you can track words 7 (17) and 8 (18).
   c. Click **Close**. The window does not update automatically and you must manually open the window each time you want to check your progress.

Resetting the service tools device ID password using the control panel or remote control panel:

Use this task to reset the service tools device ID password using the control panel or remote control panel.

Note: Before starting this task, disconnect the PC using the QCONSOLE device ID.

1. Put the physical control panel in manual operating mode. Systems without a keystick display `01 B` in the Function/Data window.
2. From the control panel, use the Up or Down buttons so that the Function/Data window displays `25`. Then press Enter. The Function/Data window should display `25 00`.
3. Using the Up button, increment the function to display `26`. Press Enter. The system most likely responds with `01 B` in the Function/Data window.

   Note: If the system responds with `65 FF`, repeat steps 2 and 3.
4. Using the Down button, decrement the function to display `65`, and then press Enter. The system responds with `65 00`.

Note: You might need to perform a function **11** to display the results (D1008065). Allow at least 10 seconds for the initial function **65** to complete before performing a function **11** if the display is not responding with D1008065.

5. Using the Up button, increment the function to display 13, and then press Ente. The system responds with ...0001 and will continue to increment as you perform each function **65**.
6. Repeat steps 4 on page 84 and 5 so that you have entered seven function **65**s. You have five minutes to complete this task. When the seventh **65** is entered and if it is found that more than five minutes have elapsed, the reset is not processed and the count returns to zero. Use the following information to help determine your progress and success of the reset:

   The double-row display control panel presents data similar to:

   ```
   xxxxxxxxxxxxxxxx
   xxxxxxxxxxxxxxxx
   ```

   Each word is eight characters but four words are displayed at a time for words 12 through 19. For example, requesting word 12 (function 12) provides you:

   ```
   word__12word__13
   word__14word__15
   ```

   Requesting word 13 (function 13) provides you:

   ```
   word__16word__17
   word__18word__19
   ```

   The remote control panel presents data similar to:

   ```
   xxxxxxxx
   ```

   Each word is eight characters only and displayed individually. If you want word 17, you have to request function **17**.

   Important: To know where you are in the process, the following information is provided:

   - Word 17 of the SRC D1008065 contains each function **65** you have completed. When it reaches a count of seven, the reset of the service tools device ID password takes place. Word 18 is then set to 00000000.
   - Word 18 displays 00000001 until you have entered the seventh function **65**. When the reset is complete, this word is set to 00000000 unless more than five minutes have elapsed.

     Note: If you enter function **65** more than seven times, the count restarts.
7. Highlight the connection name and then use one of these methods to start your connection:
   - Right-click the connection name and select **Connect**.
   - Click the connection icon in the toolbar.
   - Click the connection menu and select **Connect**.

Manually resetting the service tools device ID password on the PC:

If the automatic resynchronization failed, learn how to manually reset a connection's service tools device ID password on the client PC.

If the password was reset on the server, then the next connection made by the client automatically tries a reset version of the password in the case of a failure using the current value. If successful, the newly generated password is saved for the next connection.

If you suspect that the automatic process failed and you want to manually reset the password, complete one of the following tasks:

- Delete the configuration and then create a new configuration:
  1. Disconnect:
     a. Select the configuration name (under iSeries Connection). This is the name that Operations Console uses to refer to a specific system.

b. From the Connection menu, click **Disconnect**. The connection status displays `Disconnecting` .
c. Wait for the status to display `Disconnected`.

2. Delete the configuration:
   a. Select the configuration name (under iSeries Connection) that you want to delete.
   b. From the Connection menu, click **Delete**.
   c. Click **Yes** to confirm the deletion if prompted.
3. Create the configuration with the service tools device ID you previously reset or with the new service tools device ID.

- Reset the password for the same service tools device ID:
  1. Select the connection name that you are changing for, and then click **Connection** → **Properties**.
  2. Select the **Device ID** tab.
  3. Click **Reset**, and then **OK**. The Access Password window is displayed.
  4. Enter the current access password, and then click **OK**.

Troubleshooting authentication problems

Authentication problems are those issues that prevent you from completing a connection. The problem might be that the data entered is not acceptable and the connection does not open an emulator.

Authentication errors

Learn about some possible solutions to try if your PC cannot complete a connection between the local console and the server.

While you are connecting a local console to a server, you might encounter local console connection problems. The errors consist of software configuration problems or unrecognizable service tool user IDs.

- Verify that you are entering a valid service tools user ID and password during the configuration wizard. For example, you just performed a scratch installation and the console is not coming up after the code was restored. The PC being used has a user-created service tools device ID. In this case, the only valid service tools device ID is QCONSOLE since all of the user-created service tools device IDs were removed or reset as part of the initialization of the load source hard disk drive. You must delete and then recreate a connection using QCONSOLE as the service tools device ID.
- Verify that your server and Operations Console are installed with the same version of i5/OS and iSeries Access for Windows, respectively. If you are running different versions and are creating a new service tools device ID, the password becomes the name of the service tools device ID in uppercase, just as if the device ID were to be reset. For example, if the client is running i5/OS Version 5 Release 4 code and the server is running i5/OS Version 5 Release 3 code and you are creating a new service tools device ID for a new PC to connect, the PC asks for a password for the device ID. You might name the device “system1”, for example. When you create this on the PC, you are prompted for a password. You must use “SYSTEM1” because the system cannot assign a different password for this name. The same is true if the client is running i5/OS Version 5 Release 3 and the server is running i5/OS Version 5 Release 4. The i5/OS Version 5 Release 4 code, at either end, cannot assign a password since the password is automatically made the same as the name in uppercase.

You might also receive an error message regarding a secure connection. For information about this error, see Error message: Connection to system is not secure.

Related concepts

Error message: Connection to system is not secure

Local console on a network (LAN) receives device ID password error message

Learn about a possible solution to try if a local console on a network (LAN) receives a device ID password error message.

Due to a synchronization problem involving the service tools device ID's password between the client (PC) and server, you might receive the following error message while having a local console on a network (LAN) connection:

```
The PC service tools device password and the iSeries service tools device password do not match.
Either the service tools device ID is already in use or the passwords must be RESET on this PC
and the iSeries.
```

To resynchronize these passwords, see Resynchronizing the PC's and the server's service tools device ID passwords.

Related concepts

Resynchronizing the PC's and the server's service tools device ID passwords

Troubleshooting emulator problems

Find possible solutions to emulator problems you might encounter during your Operations Console connection.

- When setting up your initial connection, you might encounter emulator problems such as the PC5250 window does not display user data. If the emulator window does not start and the connection status is not `Connected`, see Local console.
- Padlock icon in PC5250 window is displayed open.

Related concepts

PC5250 window does not display user data

Local console

Padlock icon in PC5250 window is displayed open

PC5250 window does not display user data

Learn about a possible solution to try if you are experiencing a PC5250 emulator problem.

Note: This problem only affects a local console that is directly attached to the server.

This problem can be caused by a nonbuffered UART for the serial connection in the PC. For more information, see Performance degradation.

Padlock icon in PC5250 window is displayed in an open state

Learn about why an open padlock icon is not always a true indicator that encryption is being used.

The padlock icon in the PC5250 window is displayed as locked only when PC5250 is directly using SSL. With Operations Console, PC5250 is never using SSL so the padlock icon is always in the open state. However, there are many instances where the padlock icon on the Properties page of a configuration is indicating a false status.

Troubleshooting system reference code (SRC) data

Learn about some common console-related system reference code (SRC) data received on your server.

If you receive any of the following SRCs, you might have a problem with your Operations Console connection or with another console. These lists of SRCs are not all-inclusive, but they are the ones most commonly seen when problems with a console or Operations Console are detected.

Important: References to the data in an SRC are referred to as words 11 through 19 when using the remote control panel, and words 1 through 9 when viewed at the HMC.

To access SRC data using the HMC, complete the following steps:

1. Select from the following options:
   - If you are using an HMC with Version 6 or earlier, continue with step 2.
   - If you are using a an HMC with Version 7 or later, continue with step 3.
2. Perform the following steps:
   a. In the navigation area, expand **Server and partition** → **Server Management**.
   b. To view the reference code that corresponds to function 11 on the control panel: In the contents area, select the system or logical partition and view the associated value in the Operator panel value column.
   c. To view reference codes that correspond to function 12-19 on the control panel: In the contents area, expand the system.
   d. Select the system or logical partition.
   e. Right-click the system or logical partition and select **Properties**.
   f. Select the **Reference Code** tab. Select the entry that corresponds to the time stamp you want to view.
   g. Click **Details**.
   h. Record the values that correspond to functions 12 through 19 on the control panel.
   i. When finished, click **OK** twice.
   j. To collect system information that corresponds to function 20 on the control panel: In the navigation area, open the Service Applications folder.
   k. Select **Service Focal Point**.
   l. In the contents area, select **Service Utilities**.
   m. In the Service Utilities window, select the system and select **Selected** → **Operator Panel Service Functions**.
3. In the navigation area, click **Systems Management**.
4. In the navigation area, click **Servers**.
5. In the contents area, select the managed system you want to work with.
6. Click **Tasks** → **Serviceability** → **Reference Code History**.
7. Select the reference code you want to view.

To access SRC data using the control panel, complete the following steps:

1. On the control panel, press the increment button until function 11 is shown on the Function/Data display.
2. Press the middle button.
3. Record the data.
4. Repeat steps 1-3 for functions 12 through 20, until you have recorded the machine type, model, and serial number shown for function 20.

Note:

- If 11 is shown in the Function/Data display on the control panel display, the numbers that follow are the reference codes.
- If a number other than 11 is shown in the Function/Data display, the number might not indicate a problem with the system. These reference codes might indicate functions you select from the control panel display.
- If you have a console with Type and Reference Code columns on it, record the data under the Type column as the first 4 characters of function 11 on the problem reporting form. If an A, B, C, or D is displayed as the first character in the Type column, use the data in the Reference Code column as the last 4 characters of function 11.

Refer to the following topics to find information about specific SRCs and troubleshooting options.

SRCs A6nn500x

These system reference codes (SRCs) are used to access console types and console tasks associated with the console service functions (65+21).

These SRCs are associated with the operation of the control panel method to change the console type or to accomplish a console task when the console or other workstation is not available. For more information on how to use this function, see Using the console service functions (65+21).

The following list includes the A6*nn*500*x* SRCs and what they mean:

Note: *nn* can be any alphanumeric designation.

- A6*nn*500A - You are displaying the current console value setting.
- A6*nn*500B - You did a second 65+21 operation so you are in edit mode.
- A6*nn*500C - You did a second 21 option to cause an action, such as setting the console to another value.
- A6*nn*500D - Too much time elapsed after entering edit mode to cause an action, so you must enter edit mode again if you intend to make a change. Entering a function 21 at this time forces the console to dedicated service tools (DST), which does not cause an action.

Related concepts

Using the console service functions (65+21)

SRCs A6005001, A6005004, and A6005007

These system reference codes (SRCs) are used for a console that fails during initial program load (IPL) (not Operations Console).

The following SRCs might be displayed for twinaxial consoles.

A6005001
A console resource (controller) was not found when the server was started.

A6005004
A console device was not found when the server was started. A twinaxial controller was found but cannot be used. This indicates only the presence of a controller. It does not indicate that the controller can be defective.

A6005007
A console device was not found when the server was started. The controller (6A59) was found but the connection is starting. This can be a problem with the device or emulator, or the data flow path might not be established or maintained.

These SRCs, as well as the attention light, are reset when a console is detected and becomes active. It is possible that you might have to restart the server to find a console device again if one of these SRCs exists for a long period of time. Whether you need to restart the server depends on many factors, including which model and other hardware are present. You can force the server to try to find the console again by doing a function **21** from the control panel, remote control panel, or virtual control panel. You can also use the console service functions (65+21) to gather data or attempt recovery.

Related concepts

Using the console service functions (65+21)

SRC A6005008

This system reference code (SRC) is used for a console that fails during initial program load (IPL) (Operations Console or D-mode IPL).

The system displays code A6005008 if restarting the server did not find a console and if the console type is set to anything except a 1.

- If you are attempting to use a twinaxial console, the only data relevant in this SRC is word 16. Use Table 11 on page 92 to determine the twinaxial failure. The first four characters of this word contains the last four characters of the original failure type. For example, if word 16 contains `50010001`, the twinaxial-related SRC is A6005001 and the console type is set to use a twinaxial console.
- If you are attempting to use Operations Console, select the appropriate section in the table below as follows:
  - Local console on a network (LAN) uses words 13, 14, and 15.
  - Local console that is directly attached uses words 17, 18, and 19.

Note: If you just replaced the LAN adapter associated with a local console on a network (LAN), wait at least 35 minutes for the server to find and use the new LAN adapter. The server will start to use the new adapter, the console starts, and the SRC disappears.

The following table contains the Word 13 values for the *xxyy* status indicators, which display differently depending on the system's code level and whether you have installed PTF MF39303 (V5R3M5) or PTF MF39304 (V5R4M0). The *xxyy* values only display on systems that are *not* managed by a Hardware Management Console (HMC).

Table 9. Word 13 values for the xxyy status indicators

If Word 13 value is:	*xx* means:	*yy* means:
With PTF MF39303 (V5R3M5) or PTF MF39304 (V5R4M0)	• E0 - System is upgraded from V5R3 and support for the 1 GB Ethernet adapter is not set. • E1 - Disabled. Both the internal embedded adapter and external adapters are not being searched for. • E2 - Allows the internal embedded adapter. • E4 - Allows the external adapter. • E6 - Allows both internal embedded adapter and external adapter.	C2, C3, or C4 - Location of selected asynchronous adapter used for console, ECS, and remote service. **Important:** If you have a system that was shipped with Licensed Internal Code (LIC) prior to V5R4M5, you cannot select slot C4 for use with the console when using the 2793, but you can select slot C4 for use with ECS and remote service.
Without PTF MF39303 (V5R3M5) or PTF MF39304 (V5R4M0)	• E1 - Allows the internal embedded adapter. • 00 - No support for the internal embedded adapter.	• E2 - Allows the external adapter. • 00 - No support for the external adapter.

Table 9. Word 13 values for the xxyy status indicators (continued)

If Word 13 value is:	*xx* means:	*yy* means:
Example: With PTF MF39303 (V5R3M5) or PTF MF39304 (V5R4M0)	E6C30005 (*xxyy*000*n*) = Allows both the internal embedded adapter and external adapter (typical values for new systems), and the asynchronous adapter can be used for console, ECS, and remote service. The system is on the network, but it is not communicating with the PC.	
Example: Without PTF MF39303 (V5R3M5) or PTF MF39304 (V5R4M0)	E1E20005 (*xxyy*000*n*) = Allows both the internal embedded adapter and external adapter (typical values for new systems). The system is on the network, but is not communicating with the PC.	

The following table defines the Word 13 *n* values in *xxyy*000*n* for a local console on a network (LAN).

Table 10. Troubleshooting A6005008 for a local console on a network (LAN)

If Word 13 value (*n*) is:	Failure	Word 14 means:	Word 15 means:
1	No supported hardware detected or hardware detected is not expected. For example, you replaced the LAN IOA so the serial number is different.		In some cases the serial number of the expected adapter might be displayed. If a serial number is displayed, an adapter was previously configured. If you are installing a new server or partition that you will rely on BOOTP to complete the configuration, you might have to clear this data using the console service functions (65+21).
2	LAN IOA failed to report		
3	Hardware error	Common error codes: 53001A80, 53002AC0 - Network, cable or the LAN adapter might not be operational. 00000000: This error code indicates the adapter reported, but is not initialized yet. This is not considered an error at this time. The adapter should be activated shortly. For other error codes, contact your service provider.	Adapter position or serial number of adapter
4	BOOTP status: If attempts are zero, then BOOTP is ready when called. If attempts have a value, the PC did not respond.	Attempts	Adapter position or serial number of adapter

Table 10. Troubleshooting A6005008 for a local console on a network (LAN) (continued)

If Word 13 value (*n*) is:	Failure	Word 14 means:	Word 15 means:
5	The server's LAN connection is active, but the PC failed to connect. Are the PC and server on the same network? Are they using the same protocol? Can the PC ping the server? (`ping serverhostname`)	IP address	Adapter position or serial number of adapter

The following table defines the Word 16 values. The twinaxial console-related SRC is represented by the first four characters. The console type value is represented by the last two characters in the form *xxxxyyzz*.

Table 11. Word 16 values for the xxxxyyzz status indicators

Word 16 values for *xxxxyyzz*:		
Where *xxxx* is:		The twinaxial console-related SRC is represented by the first four characters.

Table 11. Word 16 values for the xxxxyyzz status indicators (continued)

Word 16 values for *xxxxyyzz*:		
Where *yy* is:	01	Supported, reporting workstation IOA in the tagged IOA location.
	02	Reporting communications IOA in the tagged IOA location with at least one reporting port that supports the asynchronous protocol and needed physical interface.
	03	Supported, reporting LAN IOA in the tagged IOA location, or a LAN port with the tagged port dynamic reconfiguration connector (DRC).
	04	The HMC has been configured.
	0A	No console IOA tag, no console IOP tag, and no console port DRC tag found, and the HMC has not been configured. **Note:** This is normal for standalone systems since they do not involve tagging.
	0B	A physical slot number cannot be determined from the IOA tag.
	0C	No reporting IOA in the tagged IOA location.
	0D	More than one valid reporting console IOA in the tagged IOA location. This is an unexpected error that should be reported to your service provider.
	0E	A reporting IOA was found at the location specified by the console IOA tag, but it was *not* a communications IOA and was not valid for any other type of console (for example, twinaxial console).
	0F	An IOP is tagged for the console (not an IOA or host Ethernet adapter port).
	10	Reporting LAN ports were found at the location specified by the console IOA tag, but the specific LAN port type (CCIN) is not supported for LAN console.
	11	A reporting communications IOA is in the tagged IOA location, but it has no reporting ports.
	12	A reporting communications IOA is in the tagged IOA location, but it has no reporting LAN ports and no reporting ports that support Operations Console (Direct).
	13	No reporting port resource was found with the DRC tag for the console port resource.
	14	A reporting port was found with the DRC tag for the console, but it did not qualify to be used with Operations Console
Where *zz* is:	00	Not defined by user (old default value)
	01	Twinaxial console
	02	Operations Console (Direct)
	03	Operations Console (LAN)
	04	Hardware Management Console (HMC) or Thin Console

The following table defines the Word 17 values for a local console that is directly attached.

Table 12. Troubleshooting A6005008 for a local console directly attached

Direct cable			
If Word 17 value is:	**Failure**	**Word 18 means:**	**Word 19 means:**
1	Asynchronous adapter not detected		
2	No cables detected	Adapter position	Adapter type
3	Wrong cable detected	Adapter position	Cable ID
4	Port in use	Adapter position	Adapter type
FA	Not configured for direct cable		

Note: It is expected that a D-mode IPL with a new load source hard disk drive displays the console type value of `00`. An example of when this can occur is if the copy of data from a failing hard disk drive does not copy all data or you are installing a new logical partition. Also, occasionally the hard disk drive is late in reporting and the console type value is not retrieved in time. In these cases, you can use the console service functions (65+21) to set a console type value or attempt to contact the console.

Related concepts

SRCs A6005001, A6005004, and A6005007

Using the console service functions (65+21)

SRC A6005082

This system reference code (SRC) occurs during a manual initial program load (IPL) when the system obtains a console, but the console closes.

Note: The console type does not affect this SRC.

These are some possible reasons why you might receive SRC A6005082:

- You perform an IPL on the server to dedicated service tools (DST) and then close the emulator, disconnect the console, or close Operations Console after the console is found.
- A console is found, but then the server loses the console connection.

This SRC disappears if the console is reassigned and the server can locate a console.

SRC A9002000

The Operations Console creation fails in i5/OS.

These are some possible reasons you might receive system reference code (SRC) A90002000:

- The console was not found by i5/OS.
- The system value **QAUTOCFG** must be set to on. i5/OS is unable to create the new console device if it is off.
- If you just migrated the console from one type to another and the new console fails to work in i5/OS, you might need to use another workstation to manually delete the controller and device description associated with the old console device.

Note: You might be able to use the console service functions (65+21) to assist in a recovery or gathering resolution data.

Related concepts

Using the console service functions (65+21)

SRC 0000DDDD

This system reference code (SRC) explains how your PC might power off if it has power-management capabilities.

Note: This SRC can occur on older PCs.

The PC might reset the communications port when power management is restarted, which ends any connections already established. Certain types of power management on the PC and in the operating system can cause SRC 0000DDDD to display in the control panel or remote control panel. This SRC data disappears when PC activity resumes. For more information, see Reference code list for customers.

Related concepts

Reference code list for customers

Failure to display D1008065 and D1008066 automatically after calling the function

When working with servers that have a double row for the Function/Data window, after calling the function **65** or **66**, the control panel might not automatically display the resulting system reference code.

In these cases, you must do a function **11** to determine whether the function **65** or **66** completed successfully. If you were doing an activation (**66**) and the function did not complete successfully, see D1008065.

Note: This procedure only applies to servers that are not managed by an Hardware Management Console.

1. Using the control panel or the remote control panel, press the Up or Down buttons until 11 is displayed.
2. Press Enter.

For more information, see Reference code list for customers.

Related concepts

Reference code list for customers

Startup step C6004031 takes longer than expected

Sometimes the i5/OS operating system can take longer than expected to detect the hardware resource for a console.

These are some common factors that determine how long this startup step takes:

- Console type value
- Additional console-capable resources
- Number of buses to check for a console

Some servers might experience longer delays due, in part, to the way the detection works.

Startup step C6004508 takes longer than expected in D-mode IPL

Sometimes the step for console detection can take longer than usual during a D-mode initial program load (IPL).

This situation can be the result of a problem or configuration change. If you are troubleshooting a connection issue, you can force the system to end the search for the console by performing a function **21** (enable dedicated service tools (DST)) from the control panel, remote control panel, or Hardware Management Console. This speeds the process of posting a failing system reference code (SRC) without waiting the entire search time, which can be 45 minutes or longer. Allow the system to attempt to find the console for 5 - 10 minutes before circumventing the step unless you expect a failure to occur and only need to retrieve the SRC data.

Important: Use care when considering this bypass function. Bypassing the remaining time in the process of the search might prevent a correctly working console from being activated in some cases.

D1008065 after attempting to activate the asynchronous communications adapter

Sometimes the common return codes for system reference code (SRC) D1008065 are displayed when an attempt to activate the asynchronous communications adapter fails.

Word 13 values for the *nnmm yyzz* status indicators display differently depending on the system's code level and whether or not you have installed PTF MF39303 (V5R3M5) or PTF MF39304 (V5R4M0). Values *nnmm* only display on systems that are not managed by a Hardware Management Console (HMC), so the expected values are `FF`.

Table 13. Word 13 values for the nnmm yyzz status indicators

If Word 13 value is:	*xx* means:	*yy* means:	*zz* means:	*nn* means:
With PTF MF39303 (V5R3M5) or PTF MF39304 (V5R4M0)	• E0 - System is upgraded from V5R3 and support for the 1 GB Ethernet adapter is not set. • E1 - Disabled. Both the internal embedded adapter and external adapters are not being searched for. • E2 - Allows the internal embedded adapter. • E4 - Allows the external adapter. • E6 - Allows both internal embedded adapter and external adapter.	C2, C3, or C4 - Location of selected asynchronous adapter used for console, ECS, and remote service. **Important:** If you have a system that was shipped with Licensed Internal Code (LIC) prior to V5R4M5, you cannot select slot C4 for use with the console when using the 2793, but you can select slot C4 for use with ECS and remote service.	• 10 - IOP RVX port • 20 - IOP internal modem • 30 - IOPless RVX port • 40 - IOPless internal modem • FF - No supported resource was found	• 00 - Received `OK` status from modem • 01 - CTS timeout • 02 - Received `Connect` status from PC client • 03 - Stop request • 07 - Received function 66 while active • 08 - Failed to find port • 16 - Port not found

Table 13. Word 13 values for the nnmm yyzz status indicators (continued)

If Word 13 value is:	*xx* means:	*yy* means:	*zz* means:	*nn* means:
Without PTF MF39303 (V5R3M5) or PTF MF39304 (V5R4M0)	• E1 - Allows the internal embedded adapter. • 00 - No support for the internal embedded adapter.	• E2 - Allows the external adapter. • 00 - No support for the external adapter.	• 10 - IOP RVX port • 20 - IOP internal modem • 30 - IOPless RVX port • 40 - IOPless internal modem • FF - No supported resource or port was found	• 00 - Received `OK` status from modem • 01 - CTS timeout • 02 - Received `Connect` status from PC client • 03 - Stop request • 07 - Received function 66 while active • 08 - Failed to find port • 16 - Port not found
Example: With PTF MF39303 (V5R3M5) or PTF MF39304 (V5R4M0)	E6C210002 (*xxyyzznn*) = Allows for the internal embedded adapter and the asynchronous adapter. The asynchronous adapter is located in slot C2, which is running with IOP support, can be used for console, ECS, and remote service. The system is directly connected and is communicating with the PC.			

Note: Only the most common values for *nn* are documented here. If you have a value other than what is provided, contact your service provider.

Word 14 (panel function **12** and lower-left first eight digits if using the control panel and not the Hardware Management Console) contains the reason an SRC of D1008065 is returned. A successful activation usually occurs when the console type value is set to Operations Console (direct), value of `02`. All zeros indicate the server was able to activate the asynchronous communications adapter but for some reason was unable to detect the correct condition on the PC. The most common reason for this is that the serial port on the PC is in an unexpected state. Powering off the PC and then powering it back on might clear this condition. An unstable iSeries Access for Windows installation might also cause this condition. Try uninstalling and then reinstalling iSeries Access for Windows, and removing the Operations Console connection modem, and reinstalling the connection modem to correct this condition.

Table 14. Troubleshooting D1008065 using Word 14 and Word 15 values

If Word 14 value is:	Word 14 means:
00000000	Successful activation
00000001	Port not found
00000002	No cable attached
00000004	Activation failed (see word 15)
If Word 15 value is:	**Word 15 means:**
CC100301	Resource might be in use
CC10031A	Cable mismatch or country or region code not set (Use the Change Network Attributes (CHGNETA) command to set the country or region code, if needed.)

Note: Only the most common values are documented here. If you have a value other than what is provided, contact your service provider.

Troubleshooting configuration wizard problems

Learn about some solutions to problems that might be encountered while you use the Operations Console configuration wizard.

Local console does not detect console cable

Learn about some solutions to problems that occur when the local console does not detect the presence of the Operations Console cable.

If this problem exists, a status message of `Connecting` or `Unavailable` is usually present or the port detection in the setup wizard fails.

- Verify that the cable is connected correctly. For more information on cable installation, see Installing an Operations Console cable.
- For the console, verify that the asynchronous communications adapter on the server is located correctly.
- Verify that the part number for the Operations Console cable is correct.
- Verify that the system is in a state such that the console is active. For example, if the console is active after you start the server, system reference codes (SRCs) B6004031, B6004508, or B600500*x* (where *x* is a number) indicate that the system is in the correct state.
- Verify that the PC resources are free of address or interrupt request (IRQ) conflicts. Operations Console uses addresses in the range 192.168.0.0 - 192.168.0.255. If you run any software that makes your PC SOCKS-enabled, check your SOCKS configuration:
  - Direct 192.168.0.0 255.255.255.0
  - A SOCKS-enabled PC accesses the Internet through a firewall, such as Microsoft Proxy Client, Hummingbird SOCKS Client, or others.

  Note: Use the Operations Console properties window to change the IP base address from 192.168.0.2.

Related concepts

Operations Console properties window

Related tasks

Installing an Operations Console cable

Old network data interferes with reconfiguration of network connectivity

Learn about some possible solutions if your local console on a network (LAN) configuration continues to get an old IP address.

If you are configuring a local console on a network (LAN) and you continue to get an old IP address, you might need to edit the **hosts** file on the PC to remove the entry in question.

1. Remove or alter the old entry in the **hosts** file on the PC. You can search for **hosts** and then use a text editor to edit the file.
2. Close and restart Operations Console before attempting to connect a new configuration. This action removes all cached values associated with any old configurations.

Troubleshooting remote control panel and virtual control panel problems

Learn about problems that might occur when you try to access the remote control panel (RCP) or virtual control panel (VCP).

Remote control panel fails to start

If you are connecting over a network, the RCP might fail to start when either the user ID or service tools device ID being used does not have permission to use the RCP.

Virtual control panel fails to start

Learn why the virtual control panel (VCP) might fail to start.

If the VCP fails to start, do the following:

1. Verify that the cables are correctly connected. For more information, see Installing a console cable.
2. Verify that the resources of the PC are free of address or interrupt request (IRQ) conflicts. The Operations Console uses addresses in the range 192.168.0.0 - 192.168.0.255. If you run any software that makes your PC SOCKS-enabled, check your SOCKS configuration, and make sure that the entry is as follows:

   ```
   Direct 192.168.0.0 255.255.255.0
   ```

   A SOCKS-enabled PC accesses the Internet through a firewall, such as Microsoft Proxy Client, Hummingbird SOCKS Client, or others.

Related tasks

Installing an Operations Console cable

Unable to use the mode function

Learn about why you might be unable to use the mode function on a remote control panel (RCP) or virtual control panel (VCP).

If you are unable to use the mode function on a RCP or VCP, verify that the user that authenticated the connection (Service Device Sign-on) has the Partition remote panel key privilege for the logical partition to which they are connected. To verify the privilege setting, do the following:

1. Access service tools using dedicated service tools (DST) or system service tools (SST).

   Remember: You must unlock the SST option before you can use it. For instructions, see Unlocking service tools device IDs in SST.

   - If you are using DST, select **Work with DST environment → Service tools user IDs**.
   - If you are using SST, select **Work with service tools user IDs and devices → Service tools user IDs**.
2. Verify the privilege setting.
3. If you need to change the privilege setting, select **Change privileges**.

That user must be granted this privilege, by logical partition, to use the mode function. Also, if the system supports the keystick, the keystick must be inserted before the mode function is active.

Related tasks

Unlocking service tools device IDs in SST

Related information

Access service tools using SST

Access service tools using DST

Virtual control panel authentication errors

Learn about virtual control panel (VCP) authentication errors and solutions.

See the following table for Operations Console VCP authentication errors and solutions.

Table 15. VCP authentication errors and solutions

Error message	Solution
The current access password entered is not valid. Please enter the valid access password.	This message typically means that the access password that you entered in the Service Device Sign-on window is not the same as the password that you entered in the Specify Access Password window while using the configuration wizard. Ensure that the Caps Lock key is not active, and then reenter the access password using the password that you assigned. Passwords are case sensitive.
The PC service tools device password and the service tools device password do not match. Either the service tools device ID <*name*> is already in use or the passwords must be reset on this PC and the server.	This message indicates that the Service Tools Device ID password might be incorrect. If this is the case, then the Service Tools Device ID password stored on the PC no longer matches the value stored on the server. The password assigned to the Service Device ID while using the configuration wizard on the PC must match the password assigned to the service device ID on server. If you used the QCONSOLE device ID, then both the PC and server must have the password set to QCONSOLE. Each time that you authenticate successfully, this password is encrypted again to a new value and stored on both sides of the connection. In rare situations, this password does not synchronize, so you need to reset the value back to the original default values on both the PC and the server. For instructions, see Resynchronize the PC's and the server's service tools device ID passwords.

Related tasks

Resynchronize the PC's and the server's service tools device ID passwords

Troubleshooting other Operations Console problems

Learn about some solutions to problems with your Operations Console that are not covered in the other troubleshooting sections.

Changing console tags without an IPL

Learn about a solution to change console tags without having to perform an initial program load (IPL).

If you have a problem with Operations Console on a server or partition that is managed by a Hardware Management Console (HMC), you can change the tags without requiring an IPL. This procedure might be needed to change console types to work around a problem. Alternatively, this procedure might be needed to only change which resource to use for the console, if the console type is not changing, such as when an adapter fails and it cannot be replaced immediately. You must use the HMC command interface.

To change Operations Console tags without performing an IPL, see Completing a console change with the logical partition and managed system powered on.

Related tasks

Completing a console change with the logical partition and managed system powered on

Operations Console remains in QCTL

Learn about some solutions if Operations Console remains in QCTL when it should be CTLxx.

This situation is usually present after a migration, but can be found any time you are working with system resources. QCONSOLE still remains in QCTL when you might expect it to be reassigned as another workstation.

Verify that the system is not starting with debug turned on. An indication might be that no other interactive subsystem is starting, if present, and others might also be absent. Check to see that the SYSVAL QIPLTYPE property is set to `0`.

Note: If the new console fails to work in i5/OS, you might need to use another workstation to manually delete the controller and device description that are associated with the old console device.

Error message: The user cannot perform the option selected

Learn about a solution to try when the local console receives the message, `The user cannot perform the option selected`.

If you are working with a local console on a network (LAN) configuration and attempted to access the **Service tools device IDs** option on the Work With Service Tools User IDs and Devices window within system service tools (SST), it posts the message, `The user cannot perform the option selected`. This error indicates that the option is not unlocked yet. To unlock the option, see Unlocking service tools device IDs in SST.

Related tasks

Unlocking service tools device IDs in SST

System requests are not working

Learn about a solution to try when system requests are not working.

When using Operations Console, SYSREQ corresponds to Shift+ESC and is defined as the default for PC5250 emulation.

Most keyboards have a Print Screen key, also labeled as SYSREQ and are activated by using that key with the Ctrl key. However, Windows reserves this key for the **Print Screen** function.

You must remap the keyboard by using the operating system, not PC5250, to change it.

Unable to sign on because of a lost or expired password or disabled user ID

Learn how to correct a problem when you are unable to access the takeover function.

If you have the special dedicated service tools (DST) Sign-on window but are unable to sign on because of either a disabled user ID or expired password, you can attempt recovery by doing the following:

- Verify that no other devices (PCs) that typically are eligible to become the console are connected.
- Perform the console service functions (65+21) using **65**+**21**+**21**.

This action causes the console to be lost temporarily. The device then becomes the console with a sign-on window appropriate to the system state, assuming that it matches the current console type setting. For example, if you IPL the system to the command line, then you see the i5/OS Sign-on window. You can then sign on using any user ID with the authority to continue the recovery of the DST user ID that has the problem. For more information about the DST user ID and passwords, see Working with the service tools device ID.

Related concepts

Using the console service functions (65+21)

Related information

Working with the service tools device ID

Setting up remote control panel and virtual control panels

Learn how to set up the remote control panel and the virtual control panel.

Setting up the remote control panel

You can set up the remote control panel (RCP) through an Operations Console configuration.

Related concepts

Setting up Operations Console

Troubleshooting Operations Console connections

Accessing the control panel functions using the remote control panel

To use a remote control panel (RCP) to select and activate functions on the control panel, you must have the Operations Console configured to use an RCP and you must establish a connection to the RCP.

If you do not have the Operations Console configured to use an RCP, see Setting up the remote control panel.

To connect to the RCP, do the following:

1. Start a connection to the console.
2. Sign in, and wait for the emulator window to be displayed, unless your connection is configured only for an RCP.
3. If the console configuration includes the RCP, the RCP automatically starts. If the console configuration does not include the RCP, add it by clicking **Properties** → **Configuration** and selecting the appropriate settings.

Related concepts

"Setting up the remote control panel"
You can set up the remote control panel (RCP) through an Operations Console configuration.

Related tasks

Setting up the remote control panel

Setting up the virtual control panel

You can set up the virtual control panel (VCP) through an Operations Console configuration.

To receive control panel functions by using a VCP, you must set up Operations Console and configure a VCP. The configuration path to create a VCP connection uses the Operations Console on a network path but does not require a network or network adapter.

You must also have a local console directly attached to the server that is being configured. To set up a local console directly attached to the server configuration, follow the setup instructions in Setting up Operations Console. The VCP functions have some limitations and restrictions.

Before you complete the following steps, ensure that you understand and meet the VCP requirements provided in Considerations for the virtual control panel.

To install the VCP, do the following:

1. Install the latest service pack for iSeries Access for Windows. For more information, see the iSeries Access for Windows Service Packs Web site.

2. Determine the value of the current console:
   a. Access service tools using dedicated service tools (DST) or system service tools (SST).
      - If you are using DST, select **Work with DST environment → System devices**.
      - If you are using SST, select **Work with service tools user IDs and devices**.
   b. Select **Select console**. The value of the current console is displayed. A value of 0 means that the console value is not set. The console value must be one of the following values:

Console value	Console
1	Twinaxial console
2	Operations Console (direct)
3	Operations Console (LAN)
4	HMC or Thin Console The HMC and Thin Console cannot be connected to the server at the same time.

3. Complete one of the following steps only if the option Autocreate service tools device ID is 0:
   a. If the console value is **Operations Console (LAN)**, create a service tools device ID and set user ID permissions.
   b. If the console value is not **Operations Console (LAN)**, then you can use the existing service tools device ID of QCONSOLE for the VCP. You do not need to create a service tools device ID. If you are uncertain about whether the Operations Console (LAN) console option was ever used, reset the QCONSOLE service tools device ID before using the VCP. For instructions, see Creating a service tools device ID for the console VCP to access the service tools device ID and perform the reset password task for QCONSOLE.
4. Create a new configuration for the VCP:
   a. From the **Connection** menu, click **New Connection**.
   b. Click **Next**. (If the window asking about prerequisites is displayed, click **Yes**.)
   c. Leave the option **Local Area Network (LAN)** selected, and click **Next**.
   d. Enter a name to refer to the VCP connection. If the PC that you are working with is connected to a network, do not use a name that can be found on that network or defined on the PC.
   e. Click **Next**.
   f. Enter 192.168.0.2 for the TCP/IP address when notified and click **Next**.
   g. Select the correct logical partition, and click **Next**.

      Important: IBM System i models start counting logical partitions with the number 1 (even if it is the only partition) instead of a 0. For the console to connect correctly, your logical partitions must also begin numbering at 1 instead of 0. This is especially true if you rely on the BOOTP process to configure the server with its network data.
   h. In the **Service TCP/IP Address** field, type `192.168.0.2`.

      Note: In some cases, the address `192.168.0.`*n* might have been previously used for something other than the Operations Console. In those cases, you might have had to use a different base address for the Operations Console, such as `192.168.1.`*n*. If so, use the base address currently assigned to the Operations Console, but make the last value 2. For example, use `192.168.1.2`.
      1) To check the current base address, use the regedit or another registry editing program. Navigate to the following: **HKEY_LOCAL_MACHINE → Software → IBM → Client Access → CurrentVersion → AS400 Operations Console → LCS**.
      2) Expand **LCS**, and select the appropriate configuration.

3) Check the key **IP Address**. Use the IP address reported on your PC to validate the VCP address. You might also need to check the entries in the `hosts` file on your PC for a matching name or address.

i. In the **Service gateway address 1** field, enter `0.0.0.0`.

j. If requested, enter the service tools device ID you are going to use for the VCP connection, and click **Next**.

k. In the **serial number** field, enter a serial number, and click **Next**. This number does not have to be the real system serial number.

l. Enter the service tools device ID and password that you are going to use for the VCP connection authentication, and click **Next**. If you are using the default service tools device ID QCONSOLE, then enter its name and password. If you created a device ID, then enter its name and password. Beginning with iSeries Access for Windows, Version 5 Release 4 (V5R4), you are not prompted for the service tools device ID password. Instead, you are prompted for the service tools device ID name only.

m. Enter the password that you want to use to connect this console configuration. This password is only used by the PC for the VCP connection and is not known at the server. For example, if you entered `access` as the password, then use `access` later to sign on.

n. Enter the password for confirmation, and click **Next**.

o. Click **Finish**.

p. Select the configured connection you just created, and select **Properties**.

q. Click the **Configuration** tab.

r. Clear the **Use console with this connection** option, and click **OK**.

5. You can now connect the console, if needed, and the VCP configuration to access the control panel functions. To determine how to make the connection, see Connecting a local console directly attached without remote access allowed.

Related concepts

Setting up Operations Console

Considerations for the virtual control panel

Related tasks

Creating a service tools device ID for the console VCP

Setting user ID permissions for the VCP

Accessing the control panel functions using the virtual control panel

Connecting a local console directly attached without remote access allowed

Related information

System i Access Service Packs

Access service tools using SST

Access service tools using DST

Creating a service tools device ID

The Operations Console virtual control panel (VCP) requires an available, unused service tools device ID.

Note: Only perform this procedure if autocreate service tools device ID is off (value of zero).

If the console value in IBM i5/OS is not set for **Operations Console (LAN)**, you can use the existing service tools device ID of QCONSOLE for the VCP.

To create a service tools device ID for the Operations Console VCP, do the following:

1. Access service tools using DST or SST.

Remember: You must unlock the SST option before you can use it. For instructions, see Unlocking service tools device IDs in SST.

- If you are using DST, select **Work with DST environment**, and then **Service tools device IDs**.
- If you are using SST, select **Work with service tools user IDs and devices**, and then **Service tools device IDs**.

2. Enter 1 next to the empty **device ID** field.
3. Enter the name you want for the device ID, and press Enter.
4. Enter a password into both password fields.
5. Optional: Enter a description.
6. Press Enter.
7. Select **Change attributes** to set the service tools device ID attributes for the logical partition remote panel key.
8. Press F3 to return to the DST or SST main menu.

Related tasks

Unlocking service tools device IDs in SST

Related information

Access service tools using SST

Access service tools using DST

Setting user ID permissions for the VCP

If you are using a service tools user ID other than QSECOFR, QSRV, 22222222, or 11111111 for use with the Operations Console virtual control panel (VCP), you must set the service tools user privileges for the partition remote panel key to allow access to the mode function.

To verify or set the service tools user privilege, do the following:

1. Access service tools using DST or SST.

   Remember: You must unlock the SST option before you can use it. For instructions, see Unlocking service tools device IDs in SST.

   - If you are using DST, select **Work with DST environment**, and then **Service tools user IDs**.
   - If you are using SST, select **Work with service tools user IDs and devices**, and then **Service tools user IDs**.

2. Move the cursor to the user for whom you want to verify or set the privileges, enter 7 on the same line, and press Enter.
3. Enter 2 on the line for the partition, and press Enter to grant permission to the mode functions. You only need to verify or set the privilege for the **Partition remote panel key** entry, which is the partition currently being used.
4. Press F3 to return to the DST or SST main menu.

Related tasks

Unlocking service tools device IDs in SST

Related information

Access service tools using SST

Access service tools using DST

Accessing the control panel functions using the virtual control panel

To use a virtual control panel (VCP) to select and activate functions on the control panel, you must install and establish a connection between the VCP configuration and the server.

If you have not installed a VCP, see Setting up the virtual control panel.

To connect to the VCP, do the following steps:

1. Start a connection to the console.
2. Sign in, and wait for the emulator window to be displayed.
3. Start a connection for the VCP.
4. Enter the following information only if this field was presented along with the DST user ID and password fields. In the Service Device Sign-on window, enter your password in the **Access password** field. This password is the same password used in step 4m on page 105 of the procedure to set up the virtual control panel.
5. Enter any service tools user ID and password.

Related tasks

Setting up the virtual control panel

Related information for Capacity on Demand

Product manuals, Web sites, and information center topics contain information related to the Capacity on Demand topic. You can view or print any of the PDF files.

Manuals

- System p® 650, 670, 690 Planning Guide for Capacity Upgrade on Demand  (643 KB) This guide provides information that is needed when you are planning to purchase an System p 6*xx* server with Capacity Upgrade on Demand (CUoD) features.
- System i On/Off Capacity on Demand Planning Guide  (265 KB) This guide explains in detail all the aspects of planning for, purchasing, and managing an System i 8*xx* server with On/Off Capacity on Demand.
- System i Capacity Upgrade on Demand Planning Guide  (119 KB) This guide explains in detail all the aspects of planning for, purchasing, and managing an System i 8*xx* server with Capacity Upgrade on Demand (CUoD).
- System i V5R1/V5R2 Planning Guide for Capacity Upgrade on Demand  (96 KB) This guide explains in detail all the aspects of planning for, purchasing, and managing an System i 8*xx* server with Capacity Upgrade on Demand (CUoD).

Web sites

- Resource Link Web site at http://www.ibm.com/servers/resourcelink  - Provides the entire POWER6 library.
- Capacity on Demand  (www.ibm.com/servers/eserver/iseries/ondemand/cod) - Describes the various Capacity on Demand offerings.
- Capacity Upgrade on Demand for System p servers  (http://www.ibm.com/servers/eserver/pseries/ondemand/cod/) - Describes Capacity Upgrade on Demand for processors and memory.

Other information

- Partitioning the server
- Hardware Management Console
- Electronic Service Agent™

Appendix. Accessibility features

Accessibility features help users who have a physical disability, such as restricted mobility or limited vision, to use information technology products successfully.

The following list includes the major accessibility features:

- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Keys that are tactilely discernible and do not activate just by touching them
- Industry-standard devices for ports and connectors
- The attachment of alternative input and output devices

IBM and accessibility

See the IBM Accessibility Center at http://www.ibm.com/able/ for more information about the commitment that IBM has to accessibility.

Notices

This information was developed for products and services offered in the U.S.A.

The manufacturer may not offer the products, services, or features discussed in this document in other countries. Consult the manufacturer's representative for information on the products and services currently available in your area. Any reference to the manufacturer's product, program, or service is not intended to state or imply that only that product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any intellectual property right of the manufacturer may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any product, program, or service.

The manufacturer 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 the manufacturer.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: THIS INFORMATION IS PROVIDED "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. The manufacturer 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 Web sites not owned by the manufacturer 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 product and use of those Web sites is at your own risk.

The manufacturer 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 products not produced by this manufacturer was obtained from the suppliers of those products, their published announcements or other publicly available sources. This manufacturer has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to products not produced by this manufacturer. Questions on the capabilities of products not produced by this manufacturer should be addressed to the suppliers of those products.

All statements regarding the manufacturer's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

The manufacturer's prices shown are the manufacturer'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 in softcopy, the photographs and color illustrations may not appear.

The drawings and specifications contained herein shall not be reproduced in whole or in part without the written permission of the manufacturer.

The manufacturer has prepared this information for use with the specific machines indicated. The manufacturer makes no representations that it is suitable for any other purpose.

The manufacturer's computer systems contain mechanisms designed to reduce the possibility of undetected data corruption or loss. This risk, however, cannot be eliminated. Users who experience unplanned outages, system failures, power fluctuations or outages, or component failures must verify the accuracy of operations performed and data saved or transmitted by the system at or near the time of the outage or failure. In addition, users must establish procedures to ensure that there is independent data verification before relying on such data in sensitive or critical operations. Users should periodically check the manufacturer's support websites for updated information and fixes applicable to the system and related software.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

eServer
Hummingbird
i5/OS
IBM
iSeries
POWER
System i
System i5

Pentium is a trademark of Intel® Corporation in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product or service names may be trademarks or service marks of others.

Electronic emission notices

Class A Notices

The following Class A statements apply to the IBM System i models with the exception of those that are specifically identified as Class B.

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 instruction 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 or by 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.

Industry Canada Compliance Statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A respecte est conforme à la norme NMB-003 du Canada.

European Community Compliance Statement

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC 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 A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

European Community contact:
IBM Technical Regulations
Pascalstr. 100, Stuttgart, Germany 70569
Tele: 0049 (0)711 785 1176
Fax: 0049 (0)711 785 1283
E-mail: tjahn@de.ibm.com

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.

VCCI Statement - Japan

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。

The following is a summary of the VCCI Japanese statement in the box above.

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.

Electromagnetic Interference (EMI) Statement - People's Republic of China

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。

Declaration: 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 action.

Electromagnetic Interference (EMI) Statement - Taiwan

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。

The following is a summary of the EMI Taiwan statement above.

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.

IBM Taiwan Contact Information:

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

Electromagnetic Interference (EMI) Statement - Korea

이 기기는 업무용으로 전자파적합등록을 한 기기이오니 판매자 또는 사용자는 이점을 주의하시기 바라며, 만약 잘못 판매 또는 구입하였을 때에는 가정용으로 교환하시기 바랍니다.

Please note that this equipment has obtained EMC registration for commercial use. In the event that it has been mistakenly sold or purchased, please exchange it for equipment certified for home use.

Germany Compliance Statement

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG 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 2004/108/EG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) 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 des EMVG ist die IBM Deutschland GmbH, 70548 Stuttgart.

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

Electromagnetic Interference (EMI) Statement - Russia

ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать
радиопомехи, для снижения которых необходимы
дополнительные меры

Terms and conditions

Permissions for the use of these publications is granted subject to the following terms and conditions.

Personal Use: You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of these publications, or any portion thereof, without the express consent of the manufacturer.

Commercial Use: You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of the manufacturer.

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any data, software or other intellectual property contained therein.

The manufacturer reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by the manufacturer, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

THE MANUFACTURER MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THESE PUBLICATIONS ARE PROVIDED ″AS-IS″ AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Printed in USA