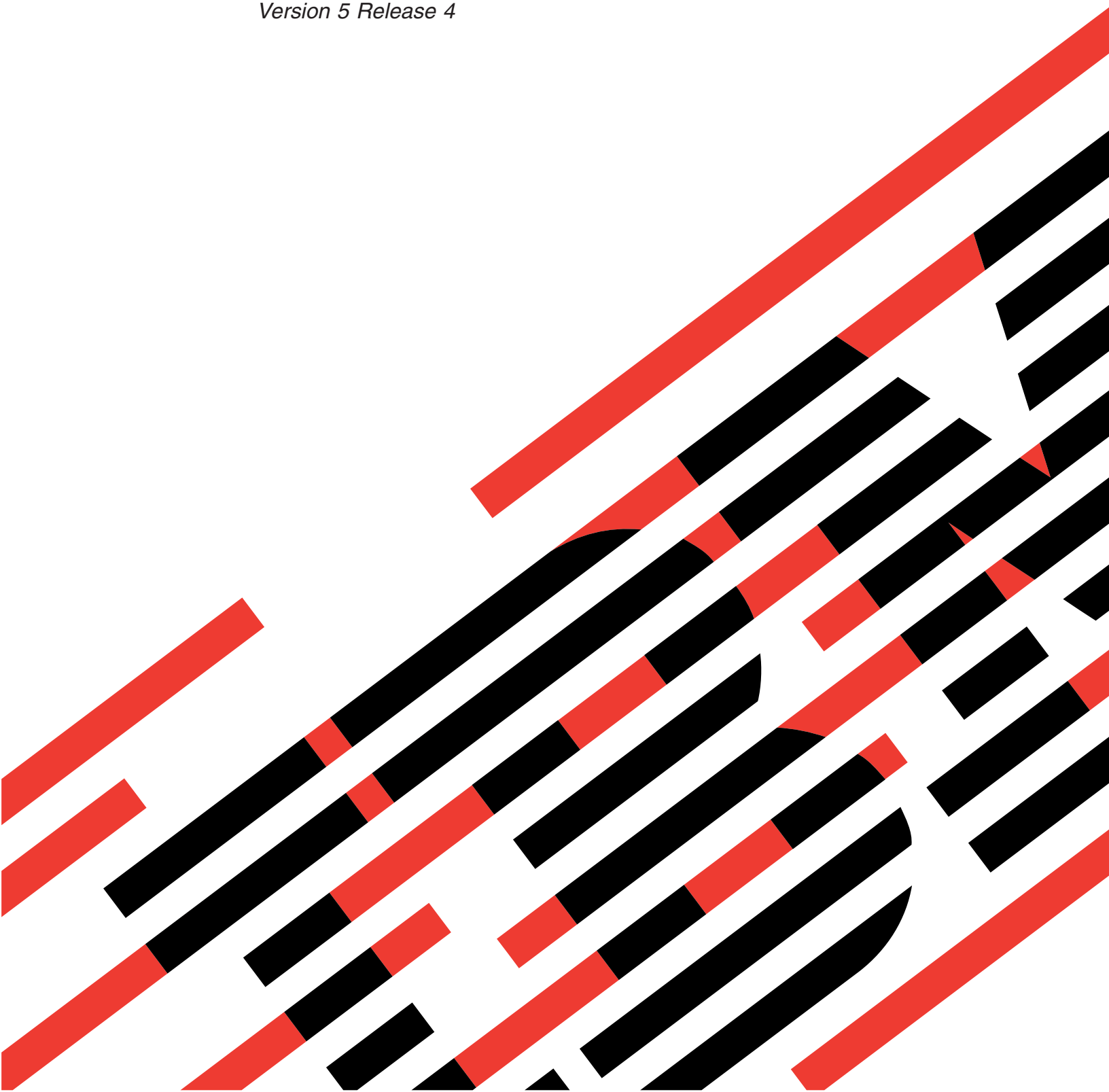
IBM Systems - iSeries

Systems Management
Getting started with Management Central

Version 5 Release 4



IBM Systems - iSeries

Systems Management
Getting started with Management Central

Version 5 Release 4

Note

Before using this information and the product it supports, read the information in "Notices," on page 17.

Seventh Edition (February 2006)

This edition applies to version 5, release 4, modification 0 of IBM i5/OS (product number 5722-SS1) and to all subsequent releases and modifications until otherwise indicated in new editions. This version does not run on all reduced instruction set computer (RISC) models nor does it run on CISC models.

Contents

Management Central

Are you interested in making your system administration tasks simpler, easier, less time-consuming, and much less repetitive? Are you looking to lower your overall total cost of server ownership? iSeries™ Navigator provides the technology you need to do systems management tasks across one or more servers simultaneously.

Click Management Central in iSeries Navigator to find easy-to-use systems management functions that come to you as part of your base operating system. Management Central in iSeries Navigator allows you to manage one or more systems through a single central system. Select a server to use as your central system, then add endpoint systems to your Management Central network. You can create groups of similar or related endpoint systems to make managing and monitoring your systems even easier. Your central system will handle the communications for you. You can even take advantage of such options as scheduling and unattended operations. You'll find that Management Central is flexible and easily manipulated to suit your needs.

With iSeries Navigator for Wireless, administrators have even more flexibility in how they access and interact with Management Central. The iSeries Navigator for Wireless overview contains tips on which devices to use, how to install and configure the required elements, and a comprehensive overview of the functions.

Related information

iSeries Navigator for Wireless overview

Get started with Management Central

To get the most out of Management Central, set up your central system and endpoint systems in a way that makes sense for your business environment. When you have finished these preliminary steps, you are ready to start working with Management Central.

Printable PDF of the section, **Get started with Management Central** (about 234 KB)

Related information

Install iSeries Navigator

Before you begin

This topic series contains information to help you complete a smooth installation and a successful connection to Management Central. It is strongly recommended that you review all of the information in this series before you being the installation process.

Related information

iSeries Navigator service web site

Setting the time zone before upgrading

Experience report: Configuring Management Central Connections for Firewall Environments

TCP/IP setup

TCP/IP troubleshooter

Configure TCP (CFGTCP) prerequisite check list

To ensure a smooth installation and setup of Management Central, you must make sure that the environment is properly prepared. Use the check list in this topic to make sure that everything is ready before you begin installing Management Central.

Prerequisite checklist

1. Your iSeries is current with the latest fixes, service packs for the client, and Java™ PTF group.
2. Read the Frequently Asked Questions at the Navigator service web site.
3. Use the QTIMZON system value to set the Java time zone for any system that is OS/400® V5R2 or earlier. (This is because in any systems V5R3 or later the QTIMZON system value is used for the Java time zone.)
4. Load all clients with iSeries Navigator and the latest service packs. (The release of the client may be at a higher release than the central system.)
5. Determine the IP address of all of the clients that you will be using. If the client has multiple IP address, it might be necessary to set the IP address to be used so that the central system can connect back to the PC. In such a situation, setting the value for QYPS_HOSTNAME in the MgmtCtrl.properties file will identify the IP address to be used. The following steps can help you decide which IP address will work. To do this use the IPCONFIG command from a DOS prompt. Write the addresses down for future reference.
   a. Confirm a valid connection from the PC to the central system. Use the ping command (ping xx.xx.xx.xx, where x=the IP address of the central system) on the PC.
   b. Run IPCONFIG from the command prompt on the PC and record all of the IP Addresses.
   c. From the central system, ping each IP Address.
   d. For the first IP address that works, create the file C:\MgmtCtrl.properties file and add this line: QYPS_HOSTNAME==<ip address on which you performed the ping>.
6. If you are upgrading iSeries Navigator from a previous release, close all open iSeries Navigator windows that might be open and exit iSeries Navigator. Start iSeries Navigator and try to connect to the central system.

Management Central connection considerations

Understanding how Management Central establishes a connection is an important contributing factor toward a successful installation and setup. Whether your system configuration is complex or simple there are many considerations that affect a successful connection.

How Management Central establishes a connection

When the Management Central Java server (QYPSJSVR) starts it obtains the IP address for itself, by long name (system + domain name), from TCP/IP. Typically, the clients that appear under My Connections and the Management Central endpoints are defined by the system name or short name.

The iSeries Navigator lookup frequency default is *Always*. This setting causes a system that is listed under My Connections to use the DNS or the TCP/IP host table (Configure TCP/IP (CFGTCP) option 10) to determine the IP address so that it can connect to the central system. The Host Name Search Priority (Configure TCP/IP (CFGTCP) option 12) option controls how the DNS search is done. If it is *LOCAL, it will search the TCP/IP host table first. If it does not find it there, it will use the DNS. If it is *REMOTE, then the DNS is searched first, followed by the TCP/IP host table.

Connection timeout delay

When the Management Central servers on an endpoint are not running, a connection failure happens right away. However, if the system is down or if a bad IP address is being used, the connection cannot be made and there will be a several minute timeout delay before the connection failure is posted.

Connection tests

Management Central uses the IP address of the system located under My Connection to connect to the Central System. When Management Central performs a connection test it does a ping on the PC of the name that is being used for the Central System (typically short name) and then it returns the same IP

address as a Ping on the Central System by the long name. If this is not successful, then the client cannot connect with the Java server. You can resolve this by overriding the Central System's IP address.

To override the IP address on the Central System use the following character-based command:

```
CALL PGM(QSYS/QYPSCONFIG) PARM(xxxx 'y.y.y.y')
```

Where xxxx is the setting QYPSHOSTNAME and y.y.y.y is the value of the IP address to be used.

Important: Edit the file using the character-based interface. Do not use a mapped drive, or other method.

Lookup frequency

The system environment variable QYPS_DNS sets the Management Central lookup frequency (values 0 = Never, 1 = Always). You can set the QYPS_DNS system variable by using one of these methods:

- Management Central properties window
- The Connection tab on the client
- Use the character-based interface to add an environment variable

  ```
  CALL PGM(QSYS/QYPSCONFIG) PARM(xxxx 'y')
  ```

  Where QYPS_DNS is the setting and y is the value 0 or 1.

It is recommended that the lookup frequency is set to Always. When the lookup frequency is set to Always, the IP address in the properties of the endpoint is ignored and a request for the IP address via the DNS or the Host Table on the central system is made. As a result, if IP addresses are changed or if the DNS or host table is changed, the new IP address is automatically picked up by Management Central.

When the lookup frequency is set to Never, the IP address that is contained in the properties of the endpoint object is used. As a result, it is possible that a client can successfully connect to the central system which uses the IP address that is determined by the My-Connection, but then have a task run to the central system and have a connection failure. Such an event indicates that the Management Central lookup frequency is set to Never and that the IP address in the endpoint for the central system is incorrect. To resolve this situation, edit the IP address for the endpoint on the endpoint properties window.

Note: The Management Central lookup frequency is a different setting than the lookup frequency setting for a system under My Connections.

Connecting to a Java server

When a client connects to a Java server, the Java server uses an authentication procedure that connects back to the PC. Therefore, the central server must be able to ping the PC.

A common connection problem occurs when the PC's address is one that is reserved for private networks (such as when an individual uses VPN from home to gain access to their network behind their router). For example, assume the PC's address is 10.100.46.143 and the IP address of the central system is 164.143.28.82. A connection failure occurs because addresses that start with 10 are not forwarded by routers. In such a situation, you need to find out what the external IP address of the PC is and then set up a client C:\MgmtCtrl.properties file, and then add the line QYPS_HOSTNAME=xxx.xxx.xxx.xxx (where the xxx's are the external IP address of the PC). This causes the Java server use the IP address specified in the properties file to connect to the PC.

Management Central bulk data transfer considerations

A *bulk transfer* is a function that is used in Management Central to transfer data from a source system to a target system (such sending of a package, sending PTFs, and so on). For a successful transfer, the target

system needs to be able to connect back to the source system. The IP address that is used on the target system is determined by the lookup frequency on the target system. If the lookup frequency is Never then the IP address that is used is the one that is provided by the central system for the source system. If the lookup frequency on the target system is set to Always then it will use DNS or the host table to determine the IP address of the source system.

Running Management Central tasks from My Connections

Some of the iSeries Navigator functions use Management Central to obtain information. For example, you can view PTFs that are in Inventory by using **My Connections → Configuration and Service**. If Management Central cannot connect to the central system then the function that you are trying to access will experience a several minute time out delay. This results in a connection failure message. A good practice to follow is to expand Management Central before you attempt to run any Management Central functions that are located under My Connections. By doing so, you will make sure that you can connect to the central system.

To run a Management Central task on a system in My Connections, the system must also be defined as an endpoint under Management Central. To define a system as an endpoint expand **Management Central → Right-click Endpoint Systems → New Endpoint Systems**.

Install Management Central

After you have completed all of the prerequisite tasks, you are ready to install Management Central. This topic series covers the installation steps as well as how the connection function works. If, after you have installed Management Central, you fail to connect successfully, refer to the article series on trouble shooting Management Central connections.

Why the highest release of Management Central is required

Each new release of Management Central contains updated functions, features and fixes that give Management Central the ability to manage a system that has machines that are running different versions of i5/OS™. In order to use these new features, you must have the most current release of Management Central, and the Management Central dependencies.

Check for the most current MC code

You must have the most current Management Central server code, Management Central client code, and Management Central dependencies before you can successfully use Management Central.

Check the Management Central servers for the most current code

The IBM® Software Technical Document,Recommended PTFs for Management Central, document number 360059564, provides a summary of the recommended fixes by release.

To access this page from the IBM web page (www.ibm.com) follow this navigation path.

1. From the menu bar click **Products**.
2. From the Products page, under Servers, click **Midrange (iSeries)**.
3. From the Midrange systems: iSeries page, on the navigation bar that is located on the left side, click **Support**.
4. From the Support for iSeries family page, on the navigation bar that is located on the left side, click iSeries support search.
5. Type in the document number in the **Search for** field and click **Search**.

Check the Management Central client for the most current code

The iSeries Access page provides up-to-date information about the service packs (fixes) for iSeries Access for Windows®. To access this page from the IBM web page (www.ibm.com) follow this navigation path.

1. From the menu bar click **Products**.
2. From the Products page, under Servers, click **Midrange (iSeries)**.
3. From the Midrange systems: iSeries page, on the navigation bar that is located on the left side, click **Software**.
4. From the iSeries Software page click the Overview tab (if not already selected) and click **iSeries Software A-Z**.
5. Under A, click **iSeries Access**.
6. On the iSeries Access page, on the navigation bar that is located on the left side, click **Service Packs (Fixes)**.

Related tasks

"Change the central system setup" on page 13
You can select a different system as your central system at any time. The central system must be a system to which you are directly connected. For the latest iSeries Navigator functions, your central system should be running i5/OS Version 5, Release 4 (V5R4).

Steps for installing and accessing Management Central

Some of the systems management functions that you will want to use are optionally installable components of iSeries Navigator, the graphical user interface (GUI) for iSeries servers.

When you choose the Typical option on the install wizard, the following Management Central functions are installed.

- Tasks (inventory only)
- Endpoint systems
- System groups

If you did not install all of the components that you need when you installed iSeries Navigator, do the following:

1. From the menu bar in iSeries Navigator, select **File → Install Options → Selective Setup**.
2. Use the Selective Setup wizard to install the additional components that you need for systems management functions. To get all the systems management functions, select Configuration and Service, Users and Groups, Commands, Packages and Products, and Monitors.

   When you use the Selective Setup wizard, the components you select will be installed. Any components you deselect during the selective setup will be uninstalled. Be careful not to accidentally uninstall anything while you use the Selective Setup wizard.

When iSeries Navigator has been installed, double-click the desktop icon to start iSeries Navigator. You are now ready to set up your central system.

Related information

iSeries Navigator

Install iSeries Access for Windows

Verify the connection function

The Verify Connection function that is located under Management Central is different from the Verify Connection function that is located under My Connection. This topic discuss the purpose of each function and how they differ from each other.

Verify Connection from My Connection

My Connections → Right-click a server → Diagnostics → Verify Connection

This Verify Connection function pings the different host servers to see if they are up and running correctly and can be reached from the PC. Since it is restricted to single system Navigator functions, it is one of the first things you should rule out when you are troubleshooting a Management Central connection failure. (Many Management Central functions build on the single system functions.) After you have confirmed that the connection to the endpoint systems, under My Connections is successful, then you can proceed to verify the connection from Management Central.

Verify Connection from Management Central

Right-click Management Central → Verify Connection

The Verify Connection function from the Management Central container is a diagnostic tool that checks the most common factors that can cause a failed connection. It then displays the status of these tests. If it reports any failures, you can obtain specific information about the failure as well as recovery information by clicking **Details**. The following is a list of what Management Central verifies.

- The Java setup is correct on the Central System (This includes verifying that certain .jar files are present, and that certain integrated file system file and folder authorities have not been changed
- The required files that were shipped with the operating system have not been deleted from the Central System, are not damaged, and are being journaled
- The TCP/IP configuration on the Central System is valid (This includes verifying that the host name of both the Central System and the PC are in the host tables or in the DNS as appropriate
- That a simple Navigator connection can be made to the Central System
- The VRM, host name, the IP address of the Central system, and the VRM of iSeries Navigator
- That the ports that Management Central uses are not in use by another application on the central system
- That on the central system, the user profiles that are needed to run Management Central have not been deleted, or disabled and that they have valid, unexpired passwords.
- That if SSL is being used on the central system, it is configured correctly and that both the PC and central system are using SSL.
- That the central system isn't marked as a ″secondary system″ in an Management Central High Availability environment (Secondary systems cannot be used as central systems.)
- That the Management Central servers are up and running on the central system
- It reports what types of authentication are supported on the central system

Note:

iSeries Navigator uses the Java toolbox code on the client side (PC) to start the Management Central Verify Connection function. If the toolbox code is not working correctly then the Verify Connection function will not start. If the Java Virtual Machine (JVM) or the toolbox code on the server side is not working correctly, the Verify Connection function will work until the last few checks. The JVM must start before these last few checks can be performed.

Related information

IBM Toolbox for Java

Set up the central system

To manage multiple servers from a single system, you need to have a central system. After you have installed Management Central and connected successfully, you are ready to set up the central system.

The servers in your network are called *endpoint systems*. You select one of these endpoint systems as your central system. After you add endpoint systems to your network and select your central system, you only need to do your system administration tasks once. Your central system will initiate your tasks and store the necessary systems management data. You choose your central system when you first start iSeries Navigator. You can also easily change your central system at any time.

Important: The release of the Central System must be the highest release in the network.

Set up your central system for the first time

To start using iSeries Navigator, double-click the desktop icon and select an iSeries server to connect to and define an iSeries connection. The first server you specify is assigned as your central system. Management Central appears automatically at the top of the list in the left pane of your iSeries Navigator window. The Management Central server is automatically started on the central system.

To access the distributed systems management functions of iSeries Navigator, expand **Management Central**.

For systems running i5/OS V5R3 and later, the Management Central databases are located in libraries QMGTC and QMGTC2. For systems running releases earlier than i5/OS V5R3, the Management Central databases are located in the QUSRSYS library.

To complete an initialization, the Management Central sever requires that QSECOFR is enabled and active. If you use a different profile name with the same kind of authorization as QSECOF, you need to run the following command on the central system.

```
CALL PGM(QSYS/QYPSCONFIG) PARM(QYPSJ_SYSTEM_ID 'XXXXX')
```

(xxxxx is a user ID other than the default of QSECOFR)

In some cases, the central system might have multiple IP addresses by which it can be accessed (CFGTCP option 10). You can use a ping command on the central system to display the IP address that will be returned to Management Central. If this is not the IP address that the clients use to connect to the system, you can override the default IP address with the address that the ping command displayed. You can use the following command to override the default IP address.

```
CALL PGM(QSYS/QYPSCONFIG) PARM(QYPS_HOSTNAME 'w.x.y.z')
```

(w.x.y.z is the IP address that Management Central should use for connection purposes)

If your central system is running OS/400 V5R2 or later (or V5R1 with PTF SI06917), you can right-click **Management Central** and select **Verify Connection** to verify that the central system connection is configured properly. To see detailed information about any Failed message, select the message and click **Details** (or double-click the message).

Note: The Verify Connection function only confirms that Management Central is working properly on the central system. TCP/IP configuration and firewalls also might prevent the Management Central client from successfully connecting to the central system.

For more information about these and other Management Central tasks and topics, refer to the detailed task help that is available from the iSeries Navigator window. Click **Help** from the menu bar and select **iSeries Navigator overview → Management Central**.

Related information

Experience report: Configuring Management Central Connections for Firewall Environments

TCP/IP troubleshooter

TCP/IP setup

SSL scenarios

Management Central settings and options

If you are migrating from a release that is earlier than V5R3, you should note that the system environment variables were moved. This topic explains where you can find the client and server environment variables for systems running a release of V5R3 or later.

/QIBM/UserData/OS400/Mgtc/Config/McCSConfig.properties

QYPS_EARLIEST_RELEASE
QYPS_MAXPTF_SIZE
QYPS_FTP_DISCOVERY
QYPS_DISCOVERY_TIMEOUT
QYPS_DISC_LCLSUBNET
QYPS_SNMP_DISCOVERY
QYPS_IP_DISCOVERY
QYPS_DISCOVERY_STARTUP
QYPS_MAX_SOCKETS
QYPS_MAX_CONTIMOUT
QYPS_RETRY_TIMEOUT
QYPS_RETRY_INTERVAL
QYPS_AUTORETRY
QYPS_SOCKETTIMEOUT
QYPS_COLLECTPTF_IFCHANGED
QYPS_DNS
QYIV_QUERY_MAX_SIZE
QYPSJ_SAVF_RECORDS
QYPSJ_TOOLBOX_TRACE
QYPS_LOCATION
QYPS_LOCATION2
QYPSJ_CONNECT_INTERVAL

/Qibm/UserData/OS400/Mgtc/Config/McCSSecure.properties

(SSL setup)

QYPS_AUTH_LEVEL
QYPS_SSL

/Qibm/UserData/OS400/Mgtc/Config/McEPConfig.properties

QYPS_TRACE
QYPSJ_TRACE
QYPSJ_SYSTEM_ID
QYPS_MAX_TRANSFERS
QYPS_HOSTNAME
QYPS_MINIMUM_PORT
QYPS_MAXIMUM_PORT

/Qibm/UserData/OS400/Mgtc/Config/McEPSecure.properties

QYPS_USER_PASSWORD
QYPS_BASIC_AUTH
QYPS_TRUST_LEVEL
QYPS_KERBEROS_PRINCIPAL
QYPS_KERBEROS_CONFIG

QYPSJ_SYSTEM_ID
QYPS_ID_MAPPING_ONLY
QYPS_USE_ID_MAPPING

Settings

iSeries Navigator allows you to manage multiple servers from a single system in a TCP/IP network environment. Some aspects of your TCP/IP environment may require changes to your Management Central server configuration. For example, if you are using a firewall or if you want to use SSL encryption for Management Central server communications, you might need to change some of your Management Central server settings.

Table 1. Management Central settings set via iSeries Navigator

Name	Description	Values	iSeries Navigator Field Name(Right-click Management Central → Properties → Connection tab)
QYPS_AUTORETRY	Specifies whether to automatically restart monitors on failed systems.	0=No, 1=Yes	Automatically restart monitors on failed systems
QYPS_COLLECTPTF_IFCHANGED	Update fixes inventory only if changes have occurred	0 = NO, 1 = YES; 0 is the default	When collecting inventory, only update when changes have occurred
QYPS_DNS	IP address lookup frequency	0 = Never, 1 = Always,	IP address lookup frequency
QYPS_MAX_CONTIMOUT	Maximum time (in seconds) to wait for a connection to a system to be established	1 to 3600 (The default value is 180 seconds.)	While connected to endpoint systems
QYPS_MAX_SOCKETS	Maximum number of sockets that can be created on a system	200 (This is the default value.)	Maximum connections
QYPS_MAXPTF_SIZE	Maximum data transfer size	-1 = No maximum size	Maximum data transfer size (MB)
QYPS_RETRY_INTERVAL	Specifies how often (in minutes) to attempt a monitor restart	5 (This is the default value.)	How often to attempt restart
QYPS_RETRY_TIMEOUT	Specifies how long (in minutes) to attempt a monitor restart	180 (This is the default value.)	How long to attempt restart
QYPS_SOCKETTIMEOUT	Maximum time (in seconds) to wait on a socket to return from a request	30 seconds (This is the default value.)	When connecting to endpoint systems

Table 2. Management Central settings set via character-based interface

Name	Description	Values	Use the character-based interface
QYIV_QUERY_MAX_SIZE	Maximum number of records in the Inventory query	200	
QYPS_HOSTNAME	The host name or IP address that you want the endpoints and the PC to connect to when they need to make a new connection back to the system. **Note:** If you use a host name, then you are relying on the endpoint or the PC to resolve the host name through their host table or DNS.		
QYPS_LOCATION	Library name where the Management Central databases are found	QMGTC	
QYPS_LOCATION2	Second library name where the Management Central databases are found	QMGTC2	
QYPS_ID_MAPPING_ONLY	Indicates whether only the Enterprise Identity Mapping (EIM) should be used for authentication	0=No, 1=Yes	
QYPS_MAXIMUM_PORT	Used by BDT (Bulk Data Transfer) QYPSBDTSVR job . Minimum of range of port number to be used.		

Table 2. Management Central settings set via character-based interface (continued)

Name	Description	Values	Use the character-based interface
QYPS_MINIMUM_PORT	Used by BDT (Bulk Data Transfer) QYPSBDTSVR job . Minimum of range of port number to be used.	Name of host server	
QYPS_TRACE	C++ server tracing	-1 to turn Off; or 0 to turn On	
QYPS_USE_ID_MAPPING	Java server tracing	-1 to turn Off; or 2 to turn On	
QYPSJ_CONNECT_INTERVAL	How often (in seconds) to do the heartbeat to check connections.	60	
QYPSJ_PORT	Port on which the Java server is listening to for incoming client requests	5544 (This is the default value.)	
QYPSJ_SAVF_RECORDS	Maximum number of records in the Java save file	100	
QYPSJ_SYSTEM_ID	User profile with all object authority	User profile which the Java server runs as for certain tasks. This profile must have *SECOFR class authority. QSECOFR is the default, or you can specify the user profile name.	
QYPSJ_TOOLBOX_TRACE	Indicates whether to turn Toolbox trace on	0=Off, 1=On	
QYPSSRV_PORT	Port on which the C++ server is listening to for incoming client requests	5555. (This is the default value.)	
QYPSJ_TRACE	Port on which the C__ server is listening to for incoming client requests	Default 5555	

Table 3. Management Central settings set via iSeries Navigator

Name	Description	Values	iSeries Navigator Field Name (Management Central → Right-click Endpoint Systems → Properties)
QYPS_DISC_LCLSUBNET	Discover local subnet	0 = No, 1 = Yes	
QYPS_DISCOVERY_STARTUP	Search every time the Management Central server starts	0 = No, 1 = Yes	
QYPS_DISCOVERY_TIMEOUT	Discovery timeout (in seconds)	15 (This is the default value.)	Timeout (seconds)
QYPS_EARLIEST_RELEASE	Earliest operating system release to search for	V5R4M0, this is the default	Earliest operating system release to search for
QYPS_FTP_DISCOVERY	Run discovery using File Transfer Protocol	0 = No, 1 = Yes	How to verify systems, FTP check box
QYPS_IP_DISCOVERY	Run discovery using Internet Protocol	0 = No, 1 = Yes	
QYPS_SNMP_DISCOVERY	Run discovery using Simple Network Mail Protocol	0 = No, 1 = Yes	How to verify systems, SNMP check box

The following table contains Property file (/Qibm/UserData/OS400/Mgtc/Config/McConfig.properties) settings that you might need to change in order to accommodate your system's needs. Unless it is otherwise indicated, use the character-based interface to make these changes.

Table 4. Management Central property file parameters

Parameter	Description	Values	
QYPS_SSL	Turns the Secure Sockets Layer (SSL) on or off.	0 = Off, 1 = On	iSeries Navigator Field Name**(Right-click Management Central → Properties → Security tab**) Field name = Use Secure Sockets Layer (SSL)
QYPS_AUTH_LEVEL	SSL authentication level. This value works with the QYPS_SSL.	0 = off (This is the default. It can only connect to a server without SSL), 1 = Sever Authentication on (This means it can connect to server with or without SSL.)	iSeries Navigator **(Right-click Management Central → Properties → Security tab**) Field name = Authentication level

Table 4. Management Central property file parameters (continued)

Parameter	Description	Values	
QYPS_USER_PASSWORD	Require password on endpoint systems	0 = No, 1 = Yes	iSeries Navigator **(Right-click Management Central → Properties → Security tab**) Field name = Use profile and password authentication
QYPSJ_SYSTEM_ID	The user profile with which the Java Server runs as, for certain tasks	QSECOFR (This is the default value.) You can also specify a user profile name, however its profile must have *SECOFR class authority.	

Add endpoint systems to your Management Central network

An endpoint system is any system or logical partition in your TCP/IP network that you choose to manage through your central system.

When you add a connection to a system from iSeries Navigator (by clicking **File → Connection to Servers → Add connection** while your current environment is selected in the left pane), the system is added to the list under your current active environment (typically named My Connections). Alternatively, when you add a new endpoint system, the system name is added to the list of Endpoint Systems under Management Central.

When you perform an action on a system under My Connections, a direct connection from the client (your PC) to the system is required, and actions are performed on one system at a time. In contrast, Management Central allows systems management tasks to be performed on multiple systems (in the Endpoint Systems list) and only one client connection (to the central system) is required.

The central system handles the connections to the endpoint systems. The Management Central property setting for the Lookup Frequency controls how the IP address for an endpoint system is determined. If it is set to NEVER then the IP address that is stored in the endpoint object is used. If it is set to ALWAYS, then the TCP/IP, on the server provides the IP address for the system name that is specified.

Note: If you are adding endpoint systems that are running OS/400 V5R1, you must have the following fixes (also known as PTFs) installed on the V5R1 system: SI01375, SI01376, SI01377, SI01378, and SI01838. Without these fixes, you will not be able to use all the systems management functions on the endpoint system.

To add one or more endpoint systems, do the following:

1. Right-click **Endpoint Systems** and select **New Endpoint System**.
2. Enter the name of the system and click **OK**.

The endpoint systems that you added appear automatically under **Endpoint Systems** in your iSeries Navigator window. After you have added an endpoint system, you can view its properties. You can also change the description or the IP address as needed.

Next, you can create system groups to help you manage different sets of endpoint systems. The new system groups will appear under Management Central in iSeries Navigator.

For more information about these and other Management Central tasks and topics, refer to the detailed task help that is available from the iSeries Navigator window. Click **Help** from the menu bar and select **iSeries Navigator overview → Management Central**.

How to completely remove endpoints

This topic answers the question, "Why, when I delete an endpoint from Management Central, it later reappears?"

When connecting to a target system, Management Central requires and uses endpoint objects. Additionally, many Management Central functions appear under systems that are listed under My Connections. Thus, whenever a user creates a system under My Connections, an endpoint object is saved in the database on the central system as well as the client PC.

If you delete the endpoint from Management Central only the entry in the central system database is deleted. You must also delete the system from all clients that have that system listed under My Connections. Otherwise, the next time user, that still has that system listed under My Connections, starts iSeries Navigator the endpoint will be automatically added again to Management Central

Therefore, to completely remove an endpoint that is also defined as a My Connection system, all users that have the system defined must remove the My connection system so it will not be automatically added.

Create system groups in your Management Central network

A *system group* is a collection of endpoint systems that you define. If you are working with multiple systems or multiple logical partitions, creating a system group allows you to perform tasks on all the systems without selecting each endpoint system. Just select the system group you created and start your task.

Endpoint systems can belong to several system groups at the same time. After you have created a system group, you can manage the entire group from your central system as if it were a single system.

To create a system group, follow these steps:

1. Open **Management Central** from your **iSeries Navigator** window.
2. Right-click **System Groups** and select **New System Group**.
3. On the **New System Group** window, specify a unique name for the new system group. You can also enter a brief description that will help you later identify this group in a list of system groups.
4. From the **Available systems** list, select the endpoint systems that you want to include in this new group. Click the **Add** button to add the systems to the **Selected systems** list.
5. If you want to give other users the ability to view or change this system group, use sharing. Click the **Sharing** tab and specify **Read-only** or **Full** sharing. If you specify **None**, other users will not be able to view or change this system group unless they have special authority, which is administered under Host Applications in Application Administration. Users with this special authority, called Management Central Administration Access, can view all tasks, definitions, monitors, and system groups under Management Central in the iSeries Navigator window.
6. Click **OK** to create the new system group.

The system group you create will include all the endpoint systems you entered. You may decide later that you want to edit that list of endpoint systems. You can always add more endpoint systems or remove endpoint systems from your system group.

You can delete system groups from Management Central. When you delete a system group or remove endpoint systems from a system group, only the system group is changed. The endpoint systems that were in the system group are still listed under **Endpoint Systems** in the iSeries Navigator window. If you delete an endpoint system from the **Endpoint Systems** list, that endpoint system is removed from all system groups.

For more information about these and other Management Central tasks and topics, refer to the detailed task help that is available from the iSeries Navigator window. Click **Help** from the menu bar and select **iSeries Navigator overview → Management Central**.

Related information

Management Central and Application Administration

Change the central system setup

You can select a different system as your central system at any time. The central system must be a system to which you are directly connected. For the latest iSeries Navigator functions, your central system should be running i5/OS Version 5, Release 4 (V5R4).

If your PC is running V5R2 or V5R3 iSeries Navigator, and you want to select a central system that is running OS/400 V5R1, you must have the following fixes (also known as PTFs) installed on the V5R1 system: SI01375, SI01376, SI01377, SI01378, and SI01838. Without these fixes, you will not be able to connect to the V5R1 system as a central system.

To change your central system, follow these steps:

1. Right-click Management Central and select **Change Central System**.
2. Use the **Change Central System** window to choose a system from your list of connected systems.
3. If the system you want to use as your central system is not currently connected to your iSeries Navigator network, right-click your active environment (typically ″My Connections″) and choose **Connection to Servers → Add connection**. When the new system is connected, you can change your central system to the new system.

After you have added endpoint systems and created system groups, those endpoint systems and system groups will appear under Management Central as well. Once you have set up your central system, you are ready to do the other tasks necessary for setting up Management Central.

Important: The central system that you use should be equal to or at a later release than the releases of the endpoints that are being used.

For more information about these and other Management Central tasks and topics, refer to the detailed task help that is available from the iSeries Navigator window. Click **Help** from the menu bar and select **iSeries Navigator overview → Management Central**.

Troubleshooting Management Central connections

Several factors can prevent a connection to the Management Central server. This topic contains a list of steps that you can take to troubleshoot a failed connection.

First and foremost, make sure that the central system is running on the highest operating system release in the network. Problems can occur because there are clients in the network that are running an operating system that is at a higher release than the central system.

Related information

Scenario: Secure all connections to your Management Central server with SSL

Experience report: Configuring Management Central Connections for Firewall Environments

Digital Certificate Manager

Failed connection to the central system

1. From the PC, verify that you can ping your central system using the name or IP address listed in iSeries Navigator as your central system. If this is unsuccessful then there is something wrong with either your network, or your DNS or host table. You must fix this before you can connect.
2. From the central system, make sure that you can ping your PC using the IP address of your PC. If this is unsuccessful, you will not be able to use some of the Management Central functions. For more information, see the Information Center experience report, ″Configuring Management Central Connections for Firewall Environments″.
3. Verify the central system connection. (From iSeries Navigator expand **My Connections → Right-click the server that is your central system → Verify Connections**.) If this reports any errors, click **Details**. This opens a window that displays information about what happened.

4. Use the Verify Connection function that is located under Management Central to further trouble shoot the problem. (From iSeries Navigator right-click **Management Central → Verify Connection**.) If this reports any errors, click **Details**. This opens a window that displays information about what happened.

What to do if you still cannot connect

If you still cannot connect use the following procedure to further troubleshoot the problem:

1. Verify that the Management Central server QYPSJSVR is running on the Central System.
   a. In iSeries Navigator, expand **My Connections → server (that you are using as the central system) → Network → Servers → TCP/IP**.
   b. Look at the Management Central item to see if the server is started. If necessary, right-click Management Central under TCP/IP, and click **Start**.
   c. If the server still fails to start, view the job logs for possible problems, or continue with the next items to check for some common problems that can cause the servers not to start.
2. Check the TCP/IP configuration on the central system.
   a. It is important that the Central System is able to ping itself using both the fully qualified domain name and the short name. If pinging either of these names fails, you will need to add the name and IP address to either the system's host table or DNS. Make sure that the IP address used in these pings is one that the PC can contact.
3. If you are using SSL with Management Central, verify that it is set up correctly. Make sure to configure your Central System, all your endpoint systems, as well as iSeries Navigator on your PC.
4. Check the QSECOFR profile.
   a. Management Central requires a profile with *ALLOBJ and *SECOFR authority enabled, and a valid password must be set so that it does not expire.

      Important: You must make this change via the character-based interface, otherwise the server might not be able to read the file.

      By default, Management Central uses the QSECOFR profile. Thus if this default has not been changed, then you can enable QSECOFR and set the password to never expire. (If you choose not to set the password to never expire then you must be diligent about keeping the password active. This is done by always changing the current password **before** it expires.) If you are using a customized profile other than QSECOFR then enable it and set the password to never expire. To change QSECOFR, open the properties file: "/QIBM/UserData/OS400/MGTC/config/McConfig.properties". Change the parameter "QYPSJ_SYSTEM_ID = QSECOFR" to "QYPSJ_SYSTEM_ID = YOURPROFILE" (where YOURPROFILE is the profile name replacing QSECOFR).
   b. Or you can run

      ```
      CALL PGM(QSYS/QYPSCONFIG) PARM(xxxx 'yyyy')
      ```

      where xxxx is QYPSJ_SYSTEM_ID and yyyy is the name of the profile to be used.
5. If both of the Management Central servers on the central system are started successfully and you've done the above troubleshooting, but you still can't connect from iSeries Navigator, then most likely the problem is either TCP/IP configuration related, or firewall related. In either case, use the Configuring Management Central Connections for Firewall Environments experience report to troubleshoot this problem. A few important notes are listed below:
   - The Central System needs to be able to initiate a connection with iSeries Navigator on the PC, so it is important that the Central System can ping the IP address of the PC.
   - The PC needs to be able to initiate a connection with iSeries Navigator that is using the following IPs:
     – The name or IP being used as the central system name in iSeries Navigator (the name of the system under my connections).

– The IP address that the central system gets when it pings itself.

Note: The initial connection to the central system uses the name or IP specified in iSeries Navigator for the central system. However during this initial connection, the central system discovers its own IP address and sends that IP to the PC. The PC uses that IP address for all further communications. The ports that Management Central uses need to be open in any firewalls that are being used.

Failed connection from PC to the central system

1. Right-click Management Central and run Verify Connection.
2. Make sure that the single socket layer (SSL) for the Management Central servers is turned on. Look in /qibm/userdata/os400/mgtc/config/McConfig.properties and confirm that QYPS_SSL>1 or QYPS_AUTH_LEVEL>1. If you change these values, remember to restart the Management Central servers.
3. If you are running OS/400 V5R2, did the QYPSSRV job fail to start? If it failed to start then the Digital Certificate Manager (DCM) configuration was not done correctly. Make sure that you have assigned your certificate the Management Central Application identification as well as the host server IDs.
4. Is there a padlock icon next to the central system? If not, then the client is not using SSL to connect. Under My Connections, right-click the central system, go to the Secure Sockets tab, and then choose to use SSL. Then click **OK**. You must close iSeries Navigator and restart it before this value takes affect.
5. On that same Secure Sockets tab as mentioned in step 3, there is a button to Download the CA to your PC. Make sure that you have done this, using the operating system that you CREATED the CA on (not necessarily the central system).
6. On the same Secure Sockets tab mentioned in the above bullet, there is a Verify SSL Connection. Run this and look at the results.
7. If you are running OS/400 V5R2 verify that the file QIBM\ProdData\OS400\Java400\jdk\lib\security\java.security has the following properties defined as these can cause a connection problem.
   - os400.jdk13.jst.factories=true
   - ssl.SocketFactory.provider=com.sun.net.ssl.internal.ssl.SSLSocketFactoryImpl
8. If you are running OS/400 V5R2 on the client, on your PC, look at c:\Documents and Settings\All Users\Documents\ibm\client access\classes\com\ibm\as400\access\KeyRing.class. Is it size 0? If so, delete the file and download the Certificate Authority.

Failed connection from central system to endpoint

In addition to following the steps for troubleshooting a failed connection from the PC to the central system, you should also view the job log on the central system. It should give a reason for why the connection was rejected. (For example: (CPFB918) Connection to system mysystem.mydomain.com rejected. Authentication level 0. Reason Code 99. This means that the SSL is not active for the endpoint. Instead, it is at authentication level 0.) You can find the meanings for negative reason codes in /QSYS.LIB/QSYSINC.LIB/H.FILE/SSL.MBR.

Note: Endpoint systems do not require a padlock.

Additional considerations

Firewall considerations

All communication is TCP initiated from the PC to the central system. You can specify the exact port to use by adding the following line to the C:\MgmtCtrl.properties file:

```
QYPSJ_LOCAL_PORT=xxxx
```

where xxxx is the port number. The port number should be greater than 1024 and less than 65535. Additionally, the port number must not be used by another application on the PC. The port must be open through the firewall. Should the firewall require it, all sockets must be open.

Work with Management Central

After Management Central has been set up, you can use it to streamline your server administration tasks.

Code license and disclaimer information

IBM grants you a nonexclusive copyright license to use all programming code examples from which you can generate similar function tailored to your own specific needs.

| SUBJECT TO ANY STATUTORY WARRANTIES WHICH CANNOT BE EXCLUDED, IBM, ITS
| PROGRAM DEVELOPERS AND SUPPLIERS MAKE NO WARRANTIES OR CONDITIONS EITHER
| EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OR
| CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND
| NON-INFRINGEMENT, REGARDING THE PROGRAM OR TECHNICAL SUPPORT, IF ANY.

| UNDER NO CIRCUMSTANCES IS IBM, ITS PROGRAM DEVELOPERS OR SUPPLIERS LIABLE FOR
| ANY OF THE FOLLOWING, EVEN IF INFORMED OF THEIR POSSIBILITY:

| 1. LOSS OF, OR DAMAGE TO, DATA;
| 2. DIRECT, SPECIAL, INCIDENTAL, OR INDIRECT DAMAGES, OR FOR ANY ECONOMIC
| CONSEQUENTIAL DAMAGES; OR
| 3. LOST PROFITS, BUSINESS, REVENUE, GOODWILL, OR ANTICIPATED SAVINGS.

| SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF DIRECT,
| INCIDENTAL, OR CONSEQUENTIAL DAMAGES, SO SOME OR ALL OF THE ABOVE LIMITATIONS
| OR EXCLUSIONS MAY NOT APPLY TO YOU.

Appendix. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation

Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

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.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

| AIX
| AIX 5L
| e(logo)server
| eServer
| i5/OS
| IBM
| iSeries
| pSeries
| xSeries
| zSeries

| Intel, Intel Inside (logos), MMX, and Pentium are trademarks of Intel Corporation in the United States,
| other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

| Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.

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 IBM.

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 IBM.

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM 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 IBM, 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.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE 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