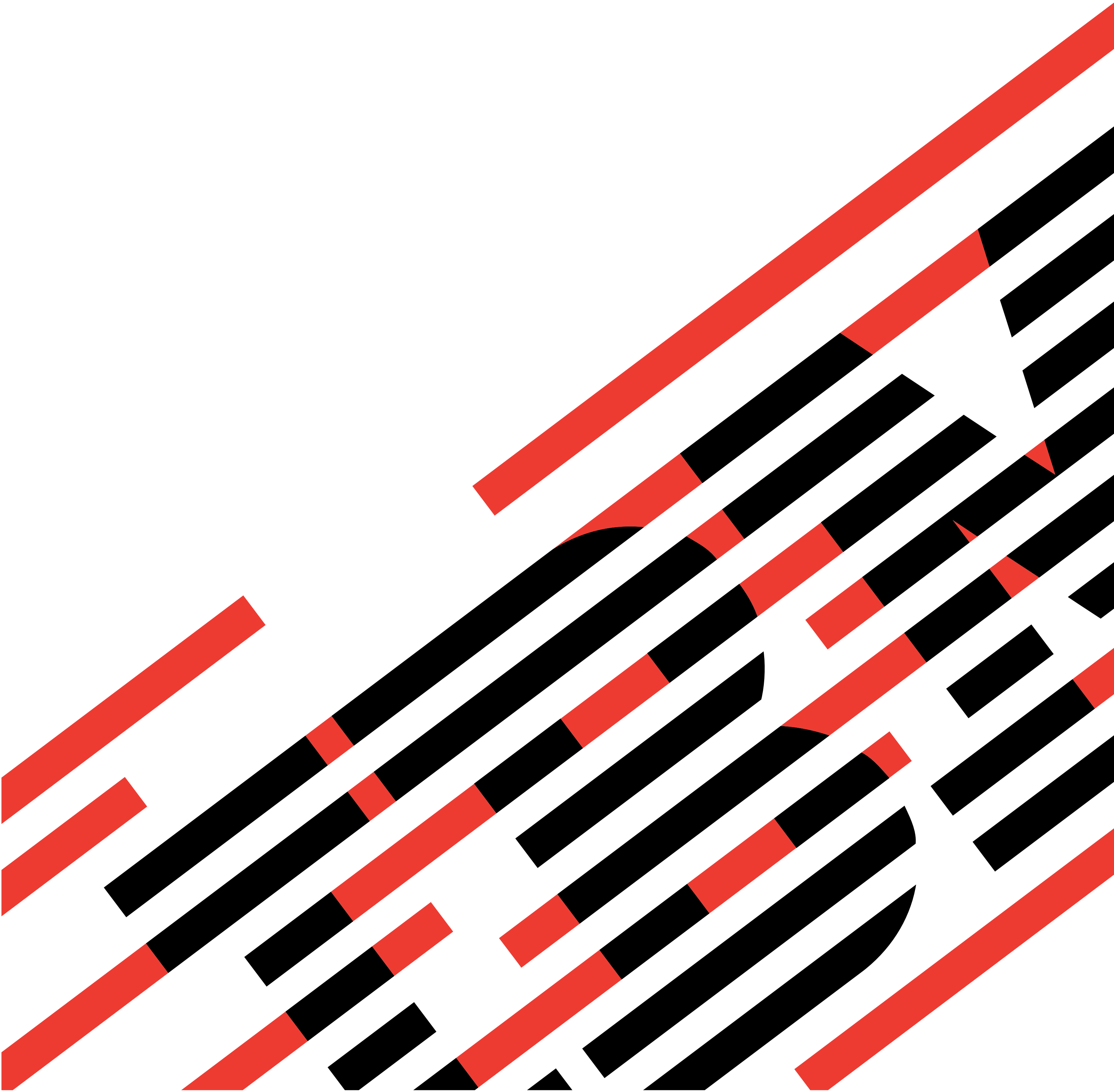
IBM

eserver

iSeries

Service tools user IDs and passwords

Version 5



eserver

iSeries

Service tools user IDs and passwords

Version 5

Note

Before using this information and the product it supports, read the information in "Notices," on page 35 and the manual *IBM eServer Safety Information,*, G229-9054.

Third Edition (August 2005)

This edition applies to version 5, release 3, modification 0 of IBM Operating System/400 (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

Chapter 1. Service tools user IDs and passwords 1

Chapter 2. What’s new for V5R3 3

Chapter 3. Print this topic 5

Chapter 4. Concepts for service tools user IDs and passwords. 7

Terminology for service tools user IDs and passwords 7
DST and SST access methods 9
Service tools user IDs 9
Password policies for service tools user IDs. . . . 11
Service tools server 11

Chapter 5. Manage service tools user IDs and passwords 13

Access service tools. 13
  Access service tools using DST 13
  Access service tools using SST 14
  Access service tools using iSeries Navigator . . 14
Manage service tools user IDs 15
  Configure service tools user IDs 15
  Change service tools user IDs and passwords . . 20
  Recover or reset QSECOFR passwords 23
  Save and restore service tools security data . . . 24
  Recommendations for managing service tools user IDs 25
Configure the service tools server 26
  Configure the service tools server for DST . . . 26
  Configure the service tools server for OS/400 . . 27
Monitor service function use. 28

Chapter 6. Troubleshoot service tools user IDs and passwords 31

Chapter 7. Related information for service tools 33

Appendix. Notices 35

Trademarks 36
Communications statements 36
  Federal Communications Commission (FCC) statement 36
  Federal Communications Commission (FCC) statement 39
Terms and conditions for downloading and printing publications 40
Product recycling and disposal 40
Battery return program 41
IBM Cryptographic Coprocessor Card Return Program 41

Chapter 1. Service tools user IDs and passwords

Service tools are used to configure, manage, and service your server or logical partitions. Service tools are used to manage logical partitions on 8xx servers. If you want to manage logical partitions on servers other than model 8*xx*, you must use the Hardware Management Console for eServer™ (HMC).

Service tools can be accessed from dedicated service tools (DST) or system service tools (SST). Service tools user IDs are required to access DST, SST, and to use the iSeries™ Navigator functions for logical partition (LPAR) management and disk unit management.

Service tools user IDs have been referred to as DST user profiles, DST user IDs, service tools user profiles, or a variation of these names. Within this topic, the term **service tools user IDs** is used.

The following information will help you understand and use service tools user IDs and passwords:

Chapter 2, "What's new for V5R3," on page 3
Find out what has changed for V5R3, as well as any late-breaking information.

Chapter 3, "Print this topic," on page 5
Print a PDF of all the information included in the Service tools user IDs and passwords topic.

Chapter 4, "Concepts for service tools user IDs and passwords," on page 7
This topic contains general information that needs to be understood before beginning to manage service tools user IDs and passwords, including definitions of the service tools terms used throughout this topic.

Chapter 5, "Manage service tools user IDs and passwords," on page 13
Learn how to manage service tools user IDs and passwords on your server.

Troubleshoot
Troubleshoot common service tools user ID and password problems.

Related information
View and print information related to the Service tools user IDs and passwords topic.

Chapter 2. What’s new for V5R3

This topic highlights functional and documentation changes to Service tools user IDs and passwords.

Added menu option to SST

The System Service Tools (SST) menu provides the new option Work with service tools user IDs and Devices. This option allows you to work with service tools user IDs, work with service tools device IDs, work with consoles, and configure service tools LAN adapters. Use this new option when performing the following tasks:

- “Configure service tools user IDs using SST” on page 18
- “Configure the service tools server using SST” on page 26

LPAR management

Service tools are used to manage logical partitions on 6xx servers. If you want to manage logical partitions on eServer hardware, you must use the Hardware Management Console for eServer (HMC).

Documentation changes

The Service tools user IDs and passwords topic was partially reorganized for your convenience. For V5R3, tasks include separate instructions based on whether the task is completed using DST or SST.

How to see what’s new or changed

To help you see where technical changes have been made, this information uses:

- The » image to mark where new or changed information begins.
- The « image to mark where new or changed information ends.

To find other information about what’s new or changed this release, see the Memo to Users.

Chapter 3. Print this topic

To view or download the PDF version of this document, select Service tools user IDs and passwords (200 KB).

You can view or download the related topic Operations Console (1,105 KB). The topic PDF contains information about planning, setting up, managing, and troubleshooting Operations Console.

Other information

You can also view or print any of the following manuals:

- Tips and Tools for Securing Your iSeries (1420 KB)
- iSeries Service Functions (1780 KB)
- iSeries Security Reference (4260 KB)

Saving PDF files

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

1. Right-click the PDF in your browser (right-click the link above).
2. Click **Save Target As...** if you are using Internet Explorer. Click **Save Link As...** if you are using Netscape Communicator.
3. Navigate to the directory in which you would like to save the PDF.
4. Click **Save**.

Downloading Adobe Acrobat Reader

You need Adobe Acrobat Reader to view or print these PDFs. You can download a copy from the Adobe Web site (www.adobe.com/products/acrobat/readstep.html) .

Chapter 4. Concepts for service tools user IDs and passwords

The following concepts provide the basic information you need to get started with service tools user IDs and passwords:

"Terminology for service tools user IDs and passwords"
This information contains definitions of the service tools terms used throughout this topic.

"DST and SST access methods" on page 9
This information describes the differences in access methods for DST and SST.

"Service tools user IDs" on page 9
This information describes service tools user IDs and functional privileges.

"Password policies for service tools user IDs" on page 11
This information describes the password policies for service tools user IDs.

"Service tools server" on page 11
This information describes the service tools server.

Terminology for service tools user IDs and passwords

The following definitions will help you understand the service tools user IDs and passwords information:

Data Encryption Standard (DES)
A type of reversible encryption algorithm. DES uses two pieces of information, the data to be encrypted and the key to use to encrypt the data. If you supply DES with the encrypted data and the encryption key, you can decrypt the data and get the original data.

dedicated service tools (DST)
Dedicated service tools (DST) are service functions that are available only from the console and can run when the operating system is not available, as well as when the operating system is available.

default password
When the password is the same as the service tools user ID. For example, the IBM-supplied QSECOFR service tools user ID is shipped with a default password of QSECOFR.

disabled password
A password that has been marked as being unable to sign on with it because you have had too many invalid sign-on attempts. You will not be able to sign on using a disabled password.

expired password
A password that has not been changed within 180 days or more. You can still sign on using an expired password, but you must change the password at the time of sign-on.

functional privileges
The ability to grant or revoke access to individual service tools functions.

locked
The mechanism used to control programmatic changes to certain functions. If a function is ″locked″ it cannot be changed through normal user interfaces. You must unlock it in order to change it.

OS/400® user profiles
User profiles that are created with the CRTUSRPRF (Create User Profile) CL command or iSeries Navigator, and are used to sign on to OS/400.

password levels
Within DST, a password level can be set. The password level specifies whether Data Encryption Standard (DES) or Secure Hash Algorithm (SHA) encryption is used when storing passwords. The default level is DES.

Secure Hash Algorithm (SHA)
An encryption method in which data is encrypted in a way that is mathematically impossible to reverse. Different data can possibly produce the same hash value, but there is no way to use the hash value to determine the original data.

service functions
Service functions are specific capabilities within service tools. Service functions are typically used for problem analysis and problem solving, often with the assistance of IBM® support. Examples of service functions include Licensed Internal Code trace, Licensed Internal Code log, and the display, alter, dump function.

service tools
Functions that are used to configure, manage, and service important operational aspects of the server. Service tools allow you to do such tasks as configure your logical partitions, manage your disk units, and troubleshoot problems. Service tools are accessed through dedicated service tools (DST), system service tools (SST), and other service-related CL commands. Improper use of service tools can damage your server.

service tools device IDs
Used with LAN console to control access to the system.

service tools server
The service tools server allows you to use your PC to perform service tools functions through TCP/IP.

service tools user IDs
A user ID that is required to access DST, SST, iSeries Navigator (for logical partitions and disk unit management), and Operations Console. Service tools user IDs are created through DST or SST, and they are separate from OS/400 user profiles.

system service tools (SST)

System service tools (SST) allow you to access service functions from OS/400. Service tools are accessed using the STRSST (Start SST) CL command.

DST and SST access methods

Dedicated service tools (DST) and system service tools (SST) are both used to access service tools and service functions. DST is available when the Licensed Internal Code has been started, even if OS/400 has not been loaded. SST is available from OS/400.

Service tools are used to do any of the following:

- Diagnose server problems
- Add hardware resources to the server
- Manage disk units
- Manage logical partition (LPAR) activities, including memory
- Review the Licensed Internal Code and product activity logs
- Trace Licensed Internal Code
- Perform main storage dumps
- Manage system security
- Manage other service tools user IDs

The following table outlines the basic differences in access methods between DST and SST.

Characteristic	DST	SST
How to access	Physical access through console during a manual IPL or by selecting option 21 on the control panel.	Access through interactive job with the ability to sign on with QSECOFR or the following authorizations: • Authorized to STRSST (Start SST) CL command. • Service special authority (*SERVICE). • Functional privilege to use SST.
When available	Available even when the server has limited capabilities. OS/400 is not required to access DST.	Available when OS/400 has been started. OS/400 is required to access SST.
How to authenticate	Requires service tools user ID and password.	Requires service tools user ID and password.

Service tools user IDs

Service tools user IDs are user IDs that are required to access service functions through dedicated service tools (DST), system service tools (SST), iSeries Navigator (for logical partitions and disk unit management), and Operations Console. Service tools user IDs are created through DST or SST and are separate from OS/400 user profiles.

IBM provides the following service tools user IDs:

- QSECOFR
- QSRV
- 22222222
- 11111111

The passwords for service tools user IDs QSECOFR, QSRV, and 22222222 are shipped as expired. All service tools passwords are shipped in uppercase.

You can create a maximum of 100 service tools user IDs (including the four IBM-supplied user IDs). See Tips and Tools for Securing Your iSeries for more information about the specific authorities granted to the IBM-provided service tools user IDs. The IBM-supplied 11111111 service tools user ID is useful when upgrading Operations Console. See the Operations Console topic for more information.

> **Note:** When IBM ships a server, there is a QSECOFR OS/400 user profile and a QSECOFR service tools user ID. These are not the same. They exist in different locations and are used to access different functions. Your QSECOFR service tools user ID can have a different password from your QSECOFR OS/400 user profile. Service tools user IDs have different password policies than OS/400 user profiles.

Creating additional service tools user IDs allows a security administrator to manage and audit the use of service tools without giving out the passwords to the IBM-supplied service tools user IDs. You can create additional service tools user IDs using dedicated service tools (DST) or system service tools (SST).

Service tools user IDs can have expiration dates, which allow you to minimize your server's security risk. For example, you can create a service tools user ID that is expired for an employee. The first time the employee uses the ID, the employee must change the ID. You can disable the user ID if a user terminates employment with the company, minimizing a former employee's potential to maliciously access service tools.

Functional privileges for service tools user IDs

The ability for a service tools user ID to access individual service functions can be granted or revoked. This is called a **functional privilege**. You can set up functional privileges that will control which service functions can be accessed by any service tools user ID. Here are some examples of how you may want to use functional privileges:

- You can allow one user to take communications and Licensed Internal Code traces and give a different user the functional privilege to manage disk units.
- You can create a service tools user ID with the same functional privileges as the IBM-supplied QSECOFR service tools user ID. You can then disable the IBM-supplied QSECOFR service tools user ID. This will prevent people from using the known QSECOFR user ID and help protect your server from security risks.

Functional privileges can be managed using DST or SST. A Start Service Tools privilege allows a service tools user ID to access DST, but be restricted from accessing SST.

Before a user is allowed to use or perform a service function, a functional privilege check is performed. If a user has insufficient privileges, access to the service function is denied. There is an audit log to "Monitor service function use" on page 28 by service tools users.

Like service tools user IDs, device IDs also have permissions that can be granted or revoked and can prevent functions from working. Device IDs can be accessed using SST. For more information about device IDs and device IDs with Operations Console see Tips and Tools for Securing Your iSeries and Secure your Operations Console configuration.

Password policies for service tools user IDs

Service tools user IDs are separate from OS/400 user profiles. Passwords for service tools user IDs are encrypted at different levels for security. The default password level uses Data Encryption Standard (DES) encryption. You should use DES encryption if you have pre-V5R1 clients using iSeries Navigator to connect to service functions such as logical partitions and disk unit management.

You can change the password level to use Secure Hash Algorithm (SHA) encryption, which is mathematically impossible to reverse and provides stronger encryption and a higher level of security. Once you change to SHA encryption, however, you cannot change back to DES encryption. If you change to SHA encryption, you will no longer be able to connect to the service tools server with pre-V5R1 clients such as Operations Console. You will need to upgrade any clients that will be using these functions when you upgrade your password level to SHA.

DES encryption

When you use DES encryption, service tools user IDs and passwords have the following characteristics:

- 10-digit, uppercase user IDs.
- 8-digit, case-sensitive passwords. When you create a user ID and password, the minimum required for the password is 1 digit. When you change a password, the minimum required is 6 digits.
- Passwords for user IDs do not expire after 180 days. By default, the initial passwords for IBM-supplied service tools user IDs, however, are shipped as expired. The exception to this is the user ID 11111111. This user ID is not expired.

SHA encryption

When you use SHA encryption, service tools user IDs and passwords have the following characteristics:

- 10-digit, uppercase user IDs.
- 128-digit case-sensitive passwords. When you create a user ID and password, the minimum required for the password is 1 digit. When you change a password, the minimum required is 6 digits.
- Passwords for user IDs expire after 180 days.
- By default, passwords are initially set as expired (unless explicitly set on the display to No).
- Passwords can be set as expired by a security administrator.

To change to use SHA encryption, access DST and perform the following steps:

1. Sign on to DST using your service tools user ID. The Use dedicated service tools (DST) display appears.
2. Select option 5 (Work with DST environment) and press Enter. The Work with DST Environment display appears.
3. Select option 6 (Service tools security data) and press Enter.
4. Select option 6 (Password level) and press Enter. Press Enter again if you are ready to go to the new password level.

Service tools server

The service tools server allows you to use your PC to perform service functions through TCP/IP. In order to use the service tools server to perform GUI-based logical partitions (LPAR) or disk management activities, you need to make the service tools server available. You can “Configure the service tools server” on page 26 for DST, OS/400, or both. Once configured, authorized users can use functions such as LPAR or disk management in iSeries Navigator.

Notes:

1. You will be unable to access any iSeries Navigator service functions until you have configured and started the service tools server.
2. If your server model is not 8*xx*, you must use the Hardware Management Console (HMC) to manage OS/400 partitions.

Chapter 5. Manage service tools user IDs and passwords

To develop an effective strategy for managing and maintaining service tools user IDs and passwords, use the following topics:

"Access service tools"
Access service tools using DST, SST, and iSeries Navigator.

"Manage service tools user IDs" on page 15
Configure service tools user IDs, change service tools user IDs and passwords, recover or reset QSECOFR passwords, and save and restore service tools security data.

"Configure the service tools server" on page 26
Configure the service tools server for DST, OS/400, or both.

"Monitor service function use" on page 28
Use the audit log to monitor service function use.

Access service tools

You can access service tools using DST, SST, and iSeries Navigator. Once you have accessed service tools, the service functions available to you depend on the functional privileges you have. If you have the appropriate functional privileges, you can "Manage service tools user IDs" on page 15 from SST or DST.

Access service tools using one of the following methods:

- "Access service tools using DST"
- "Access service tools using SST" on page 14
- "Access service tools using iSeries Navigator" on page 14

Access service tools using DST

The service tools user ID you use to access service tools with DST needs to have the functional privilege to use the DST environment.

There are two methods for starting DST. The first is to access DST through function 21 from the system control panel. The second method is to use a manual IPL.

To access service tools using DST from the **control panel**, complete the following steps:

1. Put the control panel in manual mode.
2. Use the control panel to select function 21 and press Enter. The DST Sign On display appears on the console.
3. Sign on to DST using your service tools user ID and password. The Use dedicated service tools (DST) display appears.
4. Select the appropriate option from the list and press Enter.
   - Select option 5 (Work with DST environment) to get to additional options for working with service tools user IDs.
   - Select option 7 (Start a service tool) to start any of the service tools available from DST.
   - Select any of the other options, as appropriate.

To access service tools using DST from a **manual IPL**, complete the following steps:

1. Put the control panel in manual mode.
2. If the server is powered off, turn the server on.
3. If the server is powered on to OS/400 enter the command PWRDWNSYS *IMMED RESTART(*YES) on an OS/400 command line to turn off the system and restart it.
4. Sign on to DST using your service tools user ID and password. The Use dedicated service tools (DST) display appears.
5. Select the appropriate option from the list and press Enter.
   - Select option 5 (Work with DST environment) to get additional options for working with service tools user IDs.
   - Select option 7 (Start a service tool) to start any of the service tools available from DST.
   - Select any of the other options, as appropriate.

Access service tools using SST

The service tools user ID you use to access SST needs to have the functional privilege to use SST. The OS/400 user profile needs to have the following authorizations:

- Authorized to the CL command STRSST
- Have service special authority (*SERVICE)

To access service tools using SST, complete the following steps:

1. Type STRSST (Start SST) on an OS/400 command line. The Start SST Sign On display appears.
2. Enter the following information:
   - **Service Tools User ID:** Sign on using your service tools user ID. For more information about how to create a service tools user ID, see "Configure service tools user IDs" on page 15.
   - **Password:** The password associated with this user ID.
3. Press Enter.

Access service tools using iSeries Navigator

You can access service tools using iSeries Navigator when the server has been powered on to DST or when OS/400 is running.

To access service tools using iSeries Navigator when the server has been powered on to **DST**, make sure the "Service tools server" on page 11 is configured for DST and has been started, and then complete the following steps:

1. In iSeries Navigator, select **My Connections** or your active environment.
2. Select **Open iSeries Navigator service tools window** in the Taskpad window. If the Taskpad window is not displayed, select **View** and select **Taskpad**.
3. Once you select the Taskpad item, you will need to type the IP address of the server to which you want to connect.

To access service tools using iSeries Navigator when the server is running **OS/400**, make sure the "Service tools server" on page 11 is configured for OS/400 and has been started, and then complete the following steps:

1. In iSeries Navigator, expand **My Connections** or your active environment.
2. Select the iSeries server with which you want to work.
3. Select the specific service function with which you want to work.
   - For logical partition management, expand **Configuration and Service**. Select **Logical Partitions**.
   - For disk unit management, expand **Configuration and Service**. Expand **Hardware**. Expand **Disk Units**.
4. You will be prompted to sign on using your service tools user ID.

Manage service tools user IDs

To develop an effective strategy for managing and maintaining service tools user IDs, you need to do the following:

"Configure service tools user IDs"
Create, change the functional privileges for, change the description of, display, enable, disable, or delete service tools user IDs.

"Change service tools user IDs and passwords" on page 20
Change service tools user IDs and passwords using DST or SST, STRSST (Start SST), or the Change Service Tools User ID (QSYCHGDS) API.

"Recover or reset QSECOFR passwords" on page 23
Recover or reset the passwords for both the QSECOFR OS/400 user profile and the QSECOFR service tools user ID.

"Save and restore service tools security data" on page 24
Save and restore critical service tools security data.

"Recommendations for managing service tools user IDs" on page 25
Learn about IBM's recommendations for managing service tools user IDs.

Configure service tools user IDs

You can create, change, delete, and display service tools user IDs from dedicated service tools (DST) or system service tools (SST). After you have configured the service tools user IDs, you can "Change service tools user IDs and passwords" on page 20.

Configure service tools user IDs using DST or SST:

- "Configure service tools user IDs using DST"
- "Configure service tools user IDs using SST" on page 18

Configure service tools user IDs using DST

You can create, change, display, enable, disable, or delete service tools user IDs from DST. After you have configured the service tools user IDs, you can "Change service tools user IDs and passwords using DST" on page 21.

Create, change, display, enable, disable, or delete service tools user IDs:

- "Create a service tools user ID using DST"
- "Change the functional privileges for a service tools user ID using DST" on page 16
- "Change the description for a service tools user ID using DST" on page 16
- "Display a service tools user ID using DST" on page 17
- "Enable a service tools user ID using DST" on page 17
- "Disable a service tools user ID using DST" on page 17
- "Delete a service tools user ID using DST" on page 17

Create a service tools user ID using DST: To create a service tools user ID from DST, complete the following steps:

1. Start DST.
2. Sign on to DST using your service tools user ID and password.
3. When the Use dedicated service tools (DST) display appears, select option 5 (Work with DST environment) and press Enter. The Work with DST Environment display appears.

4. From the Work with DST Environment display, select option 3 (Service tools user IDs) to work with service tools user IDs. The Work with Service Tools User IDs display appears.
5. Type 1 (Create) on the Work with Service Tools User IDs display, type the new service tools user ID in the field provided and press Enter. The Create Service Tools User ID display appears.

   Note: User IDs can be from 1-10 characters. They should be in uppercase and can include letters and numbers, as well as the special characters #, @, $, or _. Special characters are allowed for the first character in the user ID. User IDs cannot include spaces between characters.
6. Enter information about the new user ID:
   - **Username:** You will see the name of the new service tools user ID.
   - **Password:** This password will be used by the new user ID. The password must be at least 1 character in length. No other password rules apply.
   - **Allow user ID access before storage management recovery:** The default for this field is 2 (No).
   - **Set password to expired:** The default for this field is 1 (Yes).
   - **Description:** This is an optional field, which can be used for more detailed information about the owner of the user ID, such as name, department, and telephone number.
7. Once all information about the user ID has been entered, you can choose one of two options:
   - To create the user ID with the default functional privileges, press Enter.
   - To change the default functional privileges, press F5 to go to the Change Service Tools User ID Privileges display. This display lists all service tools to which privilege may be granted. See "Change service tools user IDs and passwords using DST" on page 21 for more information about changing functional privileges.

Change the functional privileges for a service tools user ID using DST: To change the functional privileges for a service tools user ID from DST, complete the following steps:

1. Start DST.
2. Sign on to DST using your service tools user ID and password.
3. When the Use dedicated service tools (DST) display appears, select option 5 (Work with DST environment) and press Enter. The Work with DST Environment display appears.
4. From the Work with DST Environment display, select option 3 (Service tools user IDs) to work with service tools user IDs. The Work with Service Tools User IDs display appears.
5. On the Work with Service Tools User IDs display, select the user ID to change and type 7 (Change privileges) in the Option field. The Change Service Tools User Privileges display appears.
   a. Type 1 (Revoke) in the Option field next to the functional privileges you want to remove from the user ID.
   b. Type 2 (Grant) in the Option field next to the functional privileges you want to add to the user ID.
6. Press Enter to enable these changes. If you press F3 (Exit) before pressing Enter, the changes will not take effect. If you press F9 (Defaults), the functional privileges are reset to the default values.

Change the description for a service tools user ID using DST: To change the description for a service tools user ID from DST, complete the following steps:

1. Start DST.
2. Sign on to DST using your service tools user ID and password. When the Use dedicated service tools (DST) display appears, select option 5 (Work with DST environment) and press Enter. The Work with DST Environment display appears.
3. From the Work with DST Environment display, select option 3 (Service tools user IDs) to work with service tools user IDs. The Work with Service Tools User IDs display appears.
4. On the Work with Service Tools User ID display, select the user ID description to change and type 8 (Change description) in the Option field.

5. In the Description field, enter a new description for the user ID. This may include the user's name, department, and telephone number.

Display a service tools user ID using DST: To display a service tools user ID from DST, complete the following steps:

1. Start DST.
2. Sign on to DST using your service tools user ID and password. When the Use dedicated service tools (DST) display appears, select option 5 (Work with DST environment) and press Enter. The Work with DST Environment display appears.
3. From the Work with DST Environment display, select option 3 (Service tools user IDs) to work with service tools user IDs. The Work with Service Tools User IDs display appears.
4. On the Work with Service Tools User IDs display, select the user ID you want to display and type 4 (Display) in the Option field. The Display Service Tools User ID display appears. This display shows information relating to the user ID, including the following:
   - Previous sign on (date and time)
   - Sign-on attempts not valid
   - Status
   - Date password last changed
   - Allow user ID access before storage management recovery (Yes or No)
   - Date password expires
   - Password set to expire (Yes or No)
5. Press F5 (Display privileges) to view the functional privileges associated with this user ID. The Display Service Tools User Privileges display appears. This display lists all functional privileges and the user's status for each. You cannot make changes to the user ID from this display.

Enable a service tools user ID using DST: To enable a service tools user ID from DST, complete the following steps:

1. Start DST.
2. Sign on to DST using your service tools user ID and password. When the Use dedicated service tools (DST) display appears, select option 5 (Work with DST environment) and press Enter. The Work with DST Environment display appears.
3. From the Work with DST Environment display, select option 3 (Service tools user IDs) to work with service tools user IDs. The Work with Service Tools User IDs display appears.
4. On the Work with Service Tools User ID display, select the user ID you want to enable and type 5 (Enable) in the Option field. The Enable Service Tools User ID display appears.
5. Press Enter to confirm your choice to enable the service tools user ID you selected.

Disable a service tools user ID using DST: To disable a service tools user ID from DST, complete the following steps:

1. Start DST.
2. Sign on to DST using your service tools user ID and password. When the Use dedicated service tools (DST) display appears, select option 5 (Work with DST environment) and press Enter. The Work with DST Environment display appears.
3. From the Work with DST Environment display, select option 3 (Service tools user IDs) to work with service tools user IDs. The Work with Service Tools User IDs display appears.
4. On the Work with Service Tools User ID display, select the user ID you want to disable and type 6 (Disable) in the Option field. The Disable Service Tools User ID display appears.
5. Press Enter to confirm your choice to disable the service tools user ID you selected.

Delete a service tools user ID using DST: You can delete a service tools user ID from DST.

Note: IBM-supplied service tools user IDs cannot be deleted.
To delete a service tools user ID, complete the following steps:

1. Start DST.
2. Sign on to DST using your service tools user ID and password. When the Use dedicated service tools (DST) display appears, select option 5 (Work with DST environment) and press Enter. The Work with DST Environment display appears.
3. From the Work with DST Environment display, select option 3 (Service tools user IDs) to work with service tools user IDs. The Work with Service Tools User IDs display appears.
4. On the Work with Service Tools User ID display, select the user ID you want to delete and type 3 (Delete) in the Option field. The Delete Service Tools User ID display appears.
5. You are prompted for confirmation of your choice to delete the user ID.
   - Press Enter to delete the user ID.
   - Press F12 (Cancel) to cancel the action and return to the Work with Service Tools User ID display.

Configure service tools user IDs using SST

You can create, change, display, enable, disable, or delete service tools user IDs from SST. After you have configured the service tools user IDs, you can "Change service tools user IDs and passwords using SST" on page 21.

Create, change, display, enable, disable, or delete service tools user IDs:

- "Create a service tools user ID using SST"
- "Change the functional privileges for a service tools user ID using SST" on page 19
- "Change the description for a service tools user ID using SST" on page 19
- "Display a service tools user ID using SST" on page 19
- "Enable a service tools user ID using SST" on page 20
- "Disable a service tools user ID using SST" on page 20
- "Delete a service tools user ID using SST" on page 20

Create a service tools user ID using SST: To create a service tools user ID from SST, complete the following steps:

1. Start SST.
2. Sign on to SST using your service tools user ID and password.
3. When the System Service Tools (SST) main menu appears, select option 8 (Work with service tools user IDs and devices).
4. From the Work With Service Tools User IDs And Devices display, select option 1 (Service tools user IDs).
5. Type 1 (Create) on the Service Tools User IDs display, and type the new service tools user ID in the field provided and press Enter. The Create Service Tools User ID display appears.

   Note: User IDs can be from 1-10 characters. They should be in uppercase and can include letters and numbers, as well as the special characters #, @, $, or _. Special characters are allowed for the first character in the user ID. User IDs cannot include spaces between characters.
6. Enter information about the new user ID:
   - **Username:** You will see the name of the new service tools user ID.
   - **Password:** This password will be used by the new user ID. The password must be at least 1 character in length. No other password rules apply.
   - **Allow user ID access before storage management recovery:** The default for this field is 2 (No).
   - **Set password to expired:** The default for this field is 1 (Yes).
   - **Description:** This is an optional field, which can be used for more detailed information about the owner of the user ID, such as name, department, and telephone number.

7. Once all information about the user ID has been entered, you can choose one of two options:
   - To create the user ID with the default functional privileges, press Enter.
   - To change the default functional privileges, press F5 to go to the Change Service Tools User ID Privileges display. This display lists all service tools to which privilege may be granted. See "Change service tools user IDs and passwords using SST" on page 21 for more information about changing functional privileges.

Change the functional privileges for a service tools user ID using SST: To change the functional privileges for a service tools user ID from SST, complete the following steps:

1. Start SST.
2. Sign on to SST using your service tools user ID and password. When the System Service Tools (SST) main menu appears, select option 8 (Work with service tools user IDs and devices).
3. From the Work With Service Tools User IDs And Devices display, select option 1 (Service tools user IDs).
4. On the Service Tools User IDs display, select the user ID to change and type 7 (Change privileges) in the Option field. The Change Service Tools User Privileges display appears.
   a. Type 1 (Revoke) in the Option field next to the functional privileges you want to remove from the user ID.
   b. Type 2 (Grant) in the Option field next to the functional privileges you want to add to the user ID.
5. Press Enter to enable these changes. If you press F3 (Exit) before pressing Enter, the changes will not take effect. If you press F9 (Defaults), the functional privileges are reset to the default values.

Change the description for a service tools user ID using SST: To change the description for a service tools user ID from SST, complete the following steps:

1. Start SST.
2. Sign on to SST using your service tools user ID and password. When the System Service Tools (SST) main menu appears, select option 8 (Work with service tools user IDs and devices).
3. From the Work With Service Tools User IDs And Devices display, select option 1 (Service tools user IDs).
4. On the Service Tools User IDs display, select the user ID description to change and type 8 (Change description) in the Option field.
5. In the Description field, enter a new description for the user ID. This may include the user's name, department, and telephone number.

Display a service tools user ID using SST: To display a service tools user ID from SST, complete the following steps:

1. Start SST.
2. Sign on to SST using your service tools user ID and password. When the System Service Tools (SST) main menu appears, select option 8 (Work with service tools user IDs and devices).
3. From the Work With Service Tools User IDs And Devices display, select option 1 (Service tools user IDs).
4. On the Service Tools User IDs display, select the user ID you want to display and type 4 (Display) in the Option field. The Display Service Tools User ID display appears. This display shows information relating to the user ID, including the following:
   - Previous sign on (date and time)
   - Sign-on attempts not valid
   - Status
   - Date password last changed
   - Allow user ID access before storage management recovery (Yes or No)
   - Date password expires

- Password set to expire (Yes or No)

5. Press F5 (Display privileges) to view the functional privileges associated with this user ID. The Display Service Tools User Privileges display appears. This display lists all functional privileges and the user's status for each. You cannot make changes to the user ID from this display.

Enable a service tools user ID using SST: To enable a service tools user ID from SST, complete the following steps:

1. Start SST.
2. Sign on to SST using your service tools user ID and password. When the System Service Tools (SST) main menu appears, select option 8 (Work with service tools user IDs and devices).
3. From the Work With Service Tools User IDs And Devices display, select option 1 (Service tools user IDs).
4. On the Service Tools User IDs display, select the user ID you want to enable and type 5 (Enable) in the Option field. The Enable Service Tools User ID display appears.
5. Press Enter to confirm your choice to enable the service tools user ID you selected.

Disable a service tools user ID using SST: To disable a service tools user ID from SST, complete the following steps:

1. Start SST.
2. Sign on to SST using your service tools user ID and password. When the System Service Tools (SST) main menu appears, select option 8 (Work with service tools user IDs and devices).
3. From the Work With Service Tools User IDs And Devices display, select option 1 (Service tools user IDs).
4. On the Service Tools User IDs display, select the user ID you want to disable and type 6 (Disable) in the Option field. The Disable Service Tools User ID display appears.
5. Press Enter to confirm your choice to disable the service tools user ID you selected.

Delete a service tools user ID using SST: You can delete a service tools user ID from SST.

Note: IBM-supplied service tools user IDs cannot be deleted.
To delete a service tools user ID, complete the following steps:

1. Start SST.
2. Sign on to SST using your service tools user ID and password. When the System Service Tools (SST) main menu appears, select option 8 (Work with service tools user IDs and devices).
3. From the Work With Service Tools User IDs And Devices display, select option 1 (Service tools user IDs).
4. On the Service Tools User IDs display, select the user ID you want to delete and type 3 (Delete) in the Option field. The Delete Service Tools User ID display appears.
5. You are prompted for confirmation of your choice to delete the user ID.
   - Press Enter to delete the user ID.
   - Press F12 (Cancel) to cancel the action and return to the Work with Service Tools User ID display.

Change service tools user IDs and passwords

This information explains how to change service tools user IDs and passwords. You should have already "Configure service tools user IDs" on page 15 and you may want to review the "Recommendations for managing service tools user IDs" on page 25 before changing any existing service tools user IDs and passwords.

> **Attention**: If you lose or forget the passwords for all OS/400 security officer profiles and all security service tools user IDs, you may need to install and initialize your system from distribution media in order to recover them. Contact your service provider for assistance. If you know either the OS/400

security officer profile password or the security service tools user ID password, the topic "Recover or reset QSECOFR passwords" on page 23 tells how to recover the password you do not know.

There are various ways to change the service tools user IDs and passwords. You can use DST or SST, STRSST (Start SST) and F9, or the Change Service Tools User ID (QSYCHGDS) API.

Change service tools user IDs and passwords:

- "Change service tools user IDs and passwords using DST"
- "Change service tools user IDs and passwords using SST"
- "Change service tools user IDs and passwords using STRSST or Change Service Tools User ID (QSYCHGDS) API" on page 22

Change service tools user IDs and passwords using DST

Complete the following steps to change a service tools user ID password using DST:

1. Start DST.
2. Sign on to DST using your service tools user ID and password. The Use dedicated service tools (DST) display appears.
3. Select option 5 (Work with DST environment) and press Enter. The Work with DST Environment display appears.
4. From the Work with DST Environment display, select option 3 (Service tools user IDs) to work with service tools user IDs. The Work with Service Tools User IDs display appears.
5. On the Work with Service Tools User ID display, find the user ID to change and type 2 (Change password) in the Option field.
   a. If you have the service tool security privilege that allows you to change other service tools user IDs, the Change Service Tools User Password for Another User display appears. The service tools user ID name is displayed. Verify that this is the user ID name you want to change. Complete the following fields:
      - **New password:** Enter a new password. This password cannot be one of your 18 previous passwords for this service tools user ID.
      - **Set Password to expired:** Type 1 (Yes) or 2 (No) in this field. The default value is 1 (Yes).

   b. If you do not have the system administrative privilege that allows you to change other service tools user IDs, the Change Service Tools User Password display appears. Complete the following fields:
      - **Current password:** Enter the password currently in use for the service tools user ID.
      - **New password:** Enter a new password. This password cannot be one of your 18 previous passwords for this service tools user ID.
      - **New password (to verify):** Enter the new password again.
6. Press Enter to complete the change. If your new password was not accepted, you may not have complied with the password policies for service tools user IDs. Review these policies and make sure you comply with them when choosing a service tools user ID password.

Change service tools user IDs and passwords using SST

Complete the following steps to change a service tools user ID password using SST:

1. Start SST.
2. Sign on to SST using a service tools user ID and password that has the service tool security privilege. The System Service Tools (SST) main menu appears.
3. From the System Service Tools (SST) main menu, select option 8 (Work with service tools user IDs and devices).
4. From the Work With Service Tools User IDs And Devices display, select option 1 (Service tools user IDs).

| 5. On the Service Tools User IDs display, find the user ID to change and type 2 (Change password) in the Option field.
6. The Change Service Tools User Password for Another User display appears. The service tools user ID name is displayed. Verify that this is the user ID name you want to change and complete the following fields:
   - **New password:** Enter a new password. This password cannot be one of your 18 previous passwords for this service tools user ID.
   - **Set Password to expired:** Type 1 (Yes) or 2 (No) in this field. The default value is 1 (Yes).
7. Press Enter to complete the change. If your new password was not accepted, you may not have complied with the password policies for service tools user IDs. Review these policies and make sure you comply with them when choosing a service tools user ID password.

Change service tools user IDs and passwords using STRSST or Change Service Tools User ID (QSYCHGDS) API

You can change your service tools user ID password using STRSST or the Change Service Tools User ID (QSYCHGDS) API.

Change your service tools user ID password using STRSST

To change your service tools user ID password using STRSST, complete the following steps:

1. On the STRSST command sign-on panel, type your service tools user ID and press F9 (Change Password). The Change Password display appears.
2. From the Change Password display, enter your current password, your new password, and the new password again to verify it. This password cannot be one of your 18 previous passwords. If you try to use a previous password, you will get an error message. Press Enter.

If all passwords were typed correctly and your new password was accepted, you will be able to sign on with your new password. If your new password was not accepted, you may not have complied with the password policies for service tools user IDs. Review these policies and make sure you comply with them when choosing a service tools user ID password.

Change service tools user IDs and passwords using Change Service Tools User ID (QSYCHGDS) API

The Change Service Tools User ID (QSYCHGDS) API allows you to change your service tools user ID and password or, if you have sufficient privileges, the service tools user ID and password for another user. This API also can be useful if you have several iSeries servers and you need to manage service tools user IDs across all of those servers.

Change default and expired passwords

To change default and expired service tools passwords, complete the following steps:

1. Allow default and expired passwords to be changed:
   a. Start SST or DST
   b. Select Work with System Security.
   c. From the Work with System Security display, change the setting of the Allow a service tools user ID with a default and expired password field from No to Yes.
2. Change a default and expired password:
   a. Start SST
   b. Sing on to SST using a service tools user ID with a default and expired password.
   c. When the message ″Password has expired″ appears, press F9 to change the password.
   d. When the service tools user ID name is displayed, complete the following fields:
      - **New password:** Enter a new password.

- **New password (to verify):** Enter the new password again..

e. Press Enter.

Recover or reset QSECOFR passwords

When IBM ships a server, both a QSECOFR OS/400 user profile and a QSECOFR service tools user ID are supplied. These are not the same. They exist in different locations and are used to access different functions. Your QSECOFR service tools user ID can have a different password from your QSECOFR OS/400 user profile. Service tools user IDs have different password policies than OS/400 user profiles.

If you lose or forget the passwords for both the QSECOFR OS/400 user profile and the QSECOFR service tools user ID, you may need to install your operating system again to recover them. Contact your service provider for assistance. If you know either of these passwords, this information tells you how to recover the password you do not know.

Reset the QSECOFR OS/400 user profile password

If you know the QSECOFR service tools user ID, you can use it to reset the QSECOFR OS/400 user profile to its initial value (QSECOFR). This procedure requires you to perform an initial program load (IPL) on your server. The change does not take affect until after the IPL. Complete the following steps to reset the QSECOFR OS/400 user profile:

1. Start DST.
2. Enter the QSECOFR service tools user ID and password on the DST Sign-On display.
3. Select option 5 (Work with DST environment) from the Use DST menu.
4. Select option 6 (Work with Service Tools Security Data) from the Work with DST Environment menu. You will see the Work with Service Tools Security Data menu:

```
+--------------------------------------------------------------------------------+
|                     Work with Service Tools Security Data                      |
|                                                         System: ____________   |
|  Select one of the following:                                                  |
|           1. Reset operating system default password                           |
|           2. Change operating system install security                          |
|           3. Work with service tools security log                              |
|           4. Restore service tools security data                               |
|           5. Save service tools security data                                  |
|           6. Password level                                                    |
|  Selection                                                                     |
+--------------------------------------------------------------------------------+
```

5. Select option 1 (Reset operating system default password). The Confirm Reset of System Default Password display appears.
6. Press Enter to confirm the reset. A confirmation message appears telling you that the system has set the operating system password override.
7. Continue pressing F3 (Exit) to return to the Exit DST menu.
8. Select option 1 (Exit DST). The IPL or Install the System menu appears.

9. Select option 1 (Perform an IPL). The system continues with a manual IPL. If you need additional information about performing an IPL, see the Start and stop the server topic.
10. When the IPL completes, return the keylock switch or electronic keystick to the Auto position, if applicable.
11. Sign on to OS/400 as QSECOFR. Use the CHGPWD command to change the QSECOFR password to a new value. Store the new value in a safe place.

    Attention: Do not leave the QSECOFR password set to the default. This is a security exposure because this is the value shipped with every iSeries server and is commonly known.

Reset the QSECOFR service tools user ID and password

If you know the password for the QSECOFR OS/400 user profile, you can use it to reset the password for the IBM-supplied service tools user ID that has service tools security privilege (QSECOFR) to the IBM-supplied default value by completing the following steps:

1. Ensure that the server is in normal operating mode, not DST.
2. Sign on at a workstation using the QSECOFR OS/400 user profile.
3. On a command line, type `CHGDSTPWD` (Change IBM Service Tools Password). Then press F4 (Do not press Enter.).You see the Change IBM Service Tools Password (CHGDSTPWD) display:

```
+--------------------------------------------------------------------------------+

|                   Change IBM Service Tools Pwd (CHGDSTPWD)                     |

|                                                                                |

|Type choices, press Enter.                                                      |

|                                                                                |

|Password . . . . . . . . . . . .  *DEFAULT             *SAME, *DEFAULT          |

|                                                                                |

+--------------------------------------------------------------------------------+
```

4. Type `*DEFAULT` and press the Enter key. This sets the IBM-supplied service tools user ID that has service tools security privilege and its password to QSECOFR.

    Attention: Do not leave the QSECOFR service tools user ID and password set to the default value. This is a security exposure because this is the value shipped with every iSeries server and is commonly known. See the “Recommendations for managing service tools user IDs” on page 25 for more information.

Save and restore service tools security data

The service tools security data is saved as part of a save system (SAVSYS) or save Licensed Internal Code. The service tools security data can also be saved manually from DST. You can work with service tools security data from DST.

Save service tools security data

To save service tools security data using DST, complete the following steps:

1. From the Work with DST Environment display, select option 6 (Service tools security data).
2. From the Work with Service Tools Security Data display, select option 5 (Save service tools security data). The Save Service Tools Security Data display appears.
3. Make sure the device is available and then select one of the available options:

- Tape
  a. Press Enter to save. The Work with Tape Devices display appears.
  b. You can select, deselect, or display details on any of the tape devices that appear. Enter the appropriate value in the Option field next to the tape device to which you want to save the security data.
- Optical
  a. Press Enter to save. The Work with Optical Devices display appears.
  b. You can select, deselect, or display details on any of the optical devices that appear. Enter the appropriate value in the Option field next to the optical device to which you want to save the security data.

Restore service tools security data

To restore service tools security data using DST, complete the following steps:

1. From the Work with DST Environment display, select option 6 (Service tools security data).
2. From the Work with Service Tools Security Data display, select option 4 (Restore service tools security data). The Select Media Type display appears.
3. Make sure the device is available and select one of the available options:
   - Tape
     a. Press Enter to restore. The Work with Tape Devices display appears.
     b. You can select, deselect, or display details on any of the tape devices that appear. If you choose to select, continue to step 4.
   - Optical
     a. Press Enter to restore. The Work with Optical Devices display appears.
     b. You may choose to select, deselect, or display details on any of the optical devices that appear. If you choose to select, continue to step 4.
4. The instructions for selecting the device from which you want to restore security data are the same for tape and optical devices.
   a. Type option 1 (Select) in the option field next to the resource you want to work with. The Restore Service Tools User ID display appears.
   b. Select one of these options:
      - To restore all service tools user IDs:
        1) Type 1 in the Option field.
        2) Press Enter. All service tools user IDs are restored.
      - To choose the service tools user IDs you want to restore:
        1) Type 2 in the Option field and press Enter. The Select Service Tools User ID to Restore display appears.
        2) Type 1 (Select) in the Option field next to the profile you want to restore. Press Enter. That service tools user ID is restored.

Recommendations for managing service tools user IDs

The following are recommendations for managing service tools user IDs.

Create your own version of the QSECOFR service tools user ID

Do not use the IBM-supplied QSECOFR service tools user ID. Instead, review what functional privileges are given to QSECOFR and create a duplicate user ID with a different name that has the same functional privileges. See the information in “Change service tools user IDs and passwords” on page 20 for detailed instructions. Use this new user ID to manage your other service tools user IDs. This will help eliminate the security exposure that originates because QSECOFR is the value shipped with every server and is commonly known.

Service tools security functional privilege

The **Service tools security** functional privilege is the privilege that allows a service tools user ID to create and manage other service tools user IDs. Since this is a powerful privilege, only your QSECOFR-equivalent service tools user ID should be given this privilege. Give careful consideration to whom you grant this functional privilege.

Configure the service tools server

You can configure the service tools server for DST, OS/400, or both.

- "Configure the service tools server for DST"
- "Configure the service tools server for OS/400" on page 27

Configure the service tools server for DST

The service tools server can be configured to be available when the server has been powered on to DST. If you use only the Operations Console with LAN connectivity to perform DST activities, the service tools server does not need to be reconfigured, as it is already available to you when the server has been powered on to DST.

You can enable the service tools server through DST or SST by dedicating a network interface card to the service tools server.

- "Configure the service tools server using DST"
- "Configure the service tools server using SST"

Configure the service tools server using DST

To enable the service tools server with its own network interface card, complete the following steps:

1. From the Use dedicated service tools (DST) display, select option 5 (Work with DST environment) and press Enter. The Work with DST Environment display appears.
2. From the Work with DST Environment display, select option 2 (System devices) and press Enter. The Work with System Devices display appears.
3. From the Work with System Devices display, select option 7 (Configure Service Tools Adapter) and press Enter. The Select Console Type display appears.
4. From the Configure Service Tools Adapter display, enter the LAN Adapter if is not already entered and enter the TCP/IP information. Press F1 (Help) for the type of information required in each field.
5. Press F7 (Store) to save your changes.
6. Press F14 (Activate) to activate the adapter.

The service tools server is ready to use with a valid service tools user ID.

Configure the service tools server using SST

To enable the service tools server with its own network interface card, complete the following steps:

1. From the System service tools (SST) display, select option 8 (Work with service tools user IDs and Devices) and press Enter.
2. From the Work With Service Tools User IDs and Devices display, select option 4 (Configure service tools LAN adapter) and press Enter.
3. From the Configure Service Tools LAN Adapter display, enter the LAN Adapter if is not already entered and enter the TCP/IP information. Press F1 (Help) for the type of information required in each field.

4. Press F7 (Store) to save your changes.
5. Press F14 (Activate) to activate the adapter.

The service tools server is ready to use with a valid service tools user ID.

Configure the service tools server for OS/400

You must add the service tools server to the service table in order to access service tools on OS/400 using TCP/IP and iSeries Navigator. The service tools server can be added before configuring your local area network (LAN). To add the service tools server to the service table, complete the following steps:

1. From any command line, type `ADDSRVTBLE` (Add Service Table Entry) and press Enter. The Add Service Table Entry display appears.
2. Enter the following information in the fields provided:
   - Service: `as-sts`
   - Port: `3000`
   - Protocol: `’tcp’` (this entry must appear lowercase and in single quotation marks)
   - Text description: `’Service Tools Server’`
     This field is optional, but you are strongly recommended to enter a description of the table entry.
3. Press F10 (Additional Parameters).
4. Enter `AS-STS` in the **Alias** field. The Alias must be capitalized because some table searches are case-sensitive.
5. Press Enter to add the table entry.
6. TCP/IP must be ended and restarted for the service table entry to be use. If you cannot end TCP at this time, you will not be able to use the service tools server. Enter `ENDTCP` (End TCP) to end TCP/IP if this is possible in your environment.
7. Enter `STRTCP` (Start TCP). Verify that the service tools server is listening to port 3000 by entering `NETSTAT OPTION(*CNN)` from a 5250 session. Look for `as-sts` under the heading Local Port with a State value of Listen.

If you will be using iSeries Navigator to perform disk unit or logical partition configuration and management, you need to complete the following steps once per server:

Note: If your server model is not 8*xx*, you must use the Hardware Management Console (HMC) to manage OS/400 partitions. For more information, see Partitioning with an HMC.

1. From an iSeries Navigator session, right-click the server name under **My Connections** (for your environment you may use your own name for the connections function instead of the default **My Connections**).
2. Select **Application Administration**. Press **OK** until you get to a window with a **Host Applications** tab. Select the **Host Applications** tab, expand **Operating System/400®**, and expand **Service**.
3. Select any of the service tools that you want to authorize: Disk Units, QIBM_QYTP_SERVICE_LPARMGMT, or Service Trace. You can select more than one.
4. Press **OK**. These functions are now available to the iSeries Navigator user provided they have a service tools user ID.

Once the service tools server has been added to the service table, authorized users can access the logical partition (LPAR) and disk management service functions using iSeries Navigator and TCP/IP. Note that, as with all service tools user IDs, you can selectively grant or restrict a user to specific service functions using functional privileges.

Monitor service function use

You can monitor service function use DST and service tools use through the OS/400 security audit log. These logs can help you trace unusual access patterns or other potential security risks.

Monitor service function use through DST

Any time a user signs on to DST using a service tools user ID, the event is logged by the Service Tools security log.

To work with the Service Tools security log, complete the following steps:

1. Start DST.
2. Enter the QSECOFR service tools user ID and password on the DST Sign-On display.
3. Select option 5 (Work with DST environment) from the Use DST menu.
4. Select option 6 (Work with Service Tools Security Data) from the Work with DST Environment menu. You will see the Work with Service Tools Security Data menu.

```
+--------------------------------------------------------------------------------+
|                     Work with Service Tools Security Data                      |
|                                                    System: _____________       |
|  Select one of the following:                                                  |
|           1. Reset operating system default password                           |
|           2. Change operating system install security                          |
|           3. Work with service tools security log                              |
|           4. Restore service tools security data                               |
|           5. Save service tools security data                                  |
|           6. Password level                                                    |
|  Selection                                                                     |
+--------------------------------------------------------------------------------+
```

5. From the Work with Service Tools Security Data display, select option 3 (Work with Service Tools Security Log) and press Enter. The Work with Service Tools Security Log display appears. This display displays security related activity by date and time.
6. (Optional) Press F6 (Print) to print this log.
7. (Optional) Type 5 (Display details) in the Option field of the activity you are interested in.
   - If the activity is related to a granted or revoked privilege, the Display Service Tools Security Log Details display appears showing the following information:
     - Time of activity
     - Activity description
     - User ID of the person who made the change
     - Affected user ID
     - Privilege description
   - If the activity is related to enabling or disabling a user ID, the Display Service Tools Security Log Details display appears showing the following information:
     - Time of activity

  - Activity description
  - User ID of the person who made the change
  - Affected user ID
- If the activity is related to any other type of event, the Display Service Tools Security Log Details display appears showing the following information:
  - Time of activity
  - Activity description
  - Affected user ID

Monitor service tools use through OS/400 security audit log

You can use the OS/400 security audit log to record service tools actions. To enable the OS/400 security audit log to record service tools actions, complete the following steps for each server on which you want to enable the OS/400 security audit log:

1. From an iSeries Navigator session, select the server name under **My Connections** (for your environment you may use your own name for the connections function instead of the default **My Connections**). Sign on using an ID that has both all object (*ALLOBJ) and all audit (*ALLAUDIT) special authorities.
2. Expand **Security**, select **Policies**, and double click **Auditing policy**.
3. Select the **System** tab. Make sure the following items are checked (other items may also be checked):
   - Activate action auditing
   - Security tasks
   - Service tasks
4. Press **OK**. These security audit log functions are now available on the iSeries server.

Once the security audit log functions have been enabled, the log information will be displayed in the journal receiver. To access the current service tools action entry in the journal receiver, enter the command DSPJRN QSYS/QAUDJRN ENTTYP(ST) on an OS/400 command line.

Once you have accessed the service tools action entry in the journal receiver, you can view service tools audit entries for individual service tools user IDs. These audit entries include actions such as logging on to SST or DST, changing a service tools user ID password, and accessing service tools. For a complete list of the audit entries and related information, see the iSeries Security Reference .

Chapter 6. Troubleshoot service tools user IDs and passwords

Use this information to understand your options when you have problems with service tools user IDs and passwords. It also gives you information about reporting problems to a support center.

Problem 1: You get an error that the password is not correct.

Be sure the password is entered in the correct case. The passwords shipped for the IBM-supplied service tools user IDs are uppercase. If you have changed your password, but sure to enter the password using the same case as when the password was changed.

Problem 2: You lost the password for the QSECOFR service tools user ID.

Reset the password for the QSECOFR service tools user ID using the CHGDSTPWD command.

Problem 3: Your QSECOFR service tools user ID has become disabled because you forgot the password was uppercase. You know the password, but have typed it incorrectly.

You can always sign on to DST with the QSECOFR service tools user ID, even if the password is disabled. You can sign on to DST and re-enable the password from there.

Problem 4: You get the error `Service tools user ID password cannot be changed` when attempting to change the password for your service tools user ID using the Change Password display from STRSST or when using the QSYCHGDS API.

Your service tools user ID is the default and has expired and the password cannot be changed from SST or by using the QSYCHGDS API. Use one of the following options:

- Use another service tools ID with appropriate functional privileges to change your password. Then sign on and change your password to a value only you know.
- Access DST to change your password.
- Use another service tools user ID with the appropriate functional privileges to access the Work with System Security option (from DST or SST) and change the setting of the *Allow a service tools user ID with a default and expired password to change its own password* setting to 1 (Yes). Change your password, and then have the setting changed back to option 2 (No).

Chapter 7. Related information for service tools

Listed below are the iSeries manuals and IBM Redbooks(TM) (in PDF format), Web sites, and Information Center topics that relate to the Service tools user IDs and passwords topic. You can view or print any of the PDFs.

Manuals

- Tips and Tools for Securing Your iSeries (1420 KB)
- iSeries Service Functions (1780 KB)
- iSeries Security Reference (4260 KB)

Other information

- Security
- Operations Console
- Partitioning with iSeries Navigator
- iSeries Navigator

Saving PDF files

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

1. Right-click the PDF in your browser (right-click the link above).
2. Click **Save Target As...** if you are using Internet Explorer. Click **Save Link As...** if you are using Netscape Communicator.
3. Navigate to the directory in which you would like to save the PDF.
4. Click **Save**.

Downloading Adobe Acrobat Reader

You need Adobe Acrobat Reader to view or print these PDFs. You can download a copy from the Adobe Web site (www.adobe.com/products/acrobat/readstep.html) .

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 give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594-1785
U.S.A.

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

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

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

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

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

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

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

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

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

The drawings and specifications contained herein shall not be reproduced in whole or in part without the written permission of IBM.

IBM has prepared this publication for use with the specific machines indicated. IBM makes no representations that it is suitable for any other purpose.

IBM'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 IBM's support Web sites 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:

e(logo)server
eServer
i5/OS
IBM
iSeries
Operating System/400
OS/400

Communications statements

The following Class A statements apply to the IBM eServer i5 and eServer p5 servers, and to the IBM eServer OpenPower servers, with the exception of those that are specifically identified as Class B.

The following Class B statements apply to model 9111–520 (stand-alone version).

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.

Responsible Party:

International Business Machines Corporation
New Orchard Road
Armonk, NY 10504

Telephone: 1-919-543-2193

Industry Canada Compliance Statement

This Class A digital apparatus meets the requirements of the Canadian Interference-Causing Equipment Regulations.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

European Community Compliance Statement

This product is in conformity with the protection requirements of EU Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

Australia and New Zealand Class A statement

Attention: 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、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。

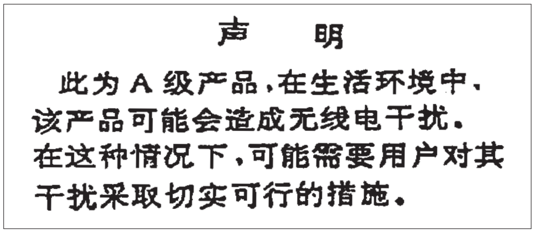
ＶＣＣＩ－Ａ

The following is a summary of the VCCI Japanese statement in the box above.

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

Electromagnetic Interference (EMI) Statement - People's Republic of China

Per GB 9254–1998, the user manual for a Class A product must carry the following warning message (English translation from the Chinese standard) about use in a residential environment in Chinese (*Simplified Chinese*):

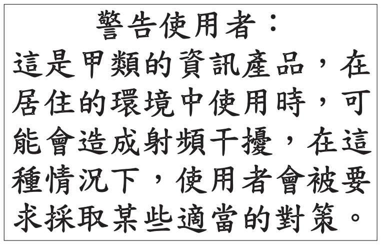


声　明

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.

Radio Protection for Germany

Dieses Gerät ist berechtigt in Übereinstimmung mit Dem deutschen EMVG vom 9.Nov.92 das EG–Konformitätszeichen zu führen.

Der Aussteller der Konformitätserklärung ist die IBM Germany.

Dieses Gerät erfüllt die Bedingungen der EN 55022 Klasse A. Für diese von Geräten gilt folgende Bestimmung nach dem EMVG:

Geräte dürfen an Orten, für die sie nicht ausreichend entstört sind, nur mit besonderer Genehmigung des Bundesministers für Post und Telekommunikation oder des Bundesamtes für Post und Telekommunikation betrieben werden. Die Genehmigung wird erteilt, wenn keine elektromagnetischen Störungen zu erwarten sind.

(Auszug aus dem EMVG vom 9.Nov.92, Para.3, Abs.4)

Hinweis

Dieses Genehmigungsverfahren ist von der Deutschen Bundespost noch nicht veröffentlicht worden.

The following Statement applies to this IBM product. The statement for other IBM products intended for use with this product will appear in their accompanying manuals.

Federal Communications Commission (FCC) statement

Note: This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult an IBM authorized dealer or service representative for help.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. Proper cables and connectors are available from IBM authorized dealers. IBM is not responsible for any radio or television interference caused by using other than recommended cables or 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 interferences, and (2) this device must accept any interferences received, including interference that may cause undesired operation.

Responsible Party:

International Business Machines Corporation
New Orchard Road
Armonk, NY 10504

Telephone: 1-919-543-2193

Industry Canada Compliance Statement

This Class B digital apparatus meets the requirements of the Canadian Interference-Causing Equipment Regulations.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe B respecte toutes les exigences du Réglement sur le matériel brouilleur du Canada.

European Community Compliance Statement

This product is in conformity with the protection requirements of EC Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

This product has been tested and found to comply with the limits for Class B Information Technology Equipment according to CISPR 22 / European Standard EN 55022. The limits for Class B equipment were derived for typical residential environments to provide reasonable protection against interference with licensed communication devices.

Properly shielded and grounded cables and connectors (IBM part number 75G5958 or its equivalent) must be used in order to reduce the potential for causing interference to radio and TV communications and to other electrical or electronic equipment. Such cables and connectors are available from IBM authorized dealers. IBM cannot accept responsibility for an interference caused by using other than recommended cables and connectors.

Terms and conditions for downloading and printing publications

Permissions for the use of the publications you have selected for download are granted subject to the following terms and conditions and your indication of acceptance thereof.

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 AND FITNESS FOR A PARTICULAR PURPOSE

All material copyrighted by IBM Corporation.

By downloading or printing a publication from this site, you have indicated your agreement with these terms and conditions.

Product recycling and disposal

This unit contains materials such as circuit boards, cables, electromagnetic compatibility gaskets and connectors which may contain lead and copper/beryllium alloys that require special handling and disposal at end of life. Before this unit is disposed of, these materials must be removed and recycled or discarded according to applicable regulations. IBM offers product-return programs in several countries. Information on product recycling offerings can be found on IBM’s Internet site at http://www.ibm.com/ibm/environment/products/prp.shtml.

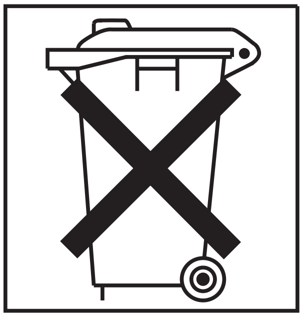
IBM encourages owners of information technology (IT) equipment to responsibly recycle their equipment when it is no longer needed. IBM offers a variety of programs and services to assist equipment owners in recycling their IT products. Information on product recycling offerings can be found on IBM’s Internet site at http://www.ibm.com/ibm/environment/products/prp.shtml.

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.

In the Netherlands, the following applies:



In Taiwan, the following applies. Please recycle batteries.

IBM Cryptographic Coprocessor Card Return Program

This machine may contain an optional feature, the cryptographic coprocessor card, which includes a polyurethane material that contains mercury. 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

Printed in USA