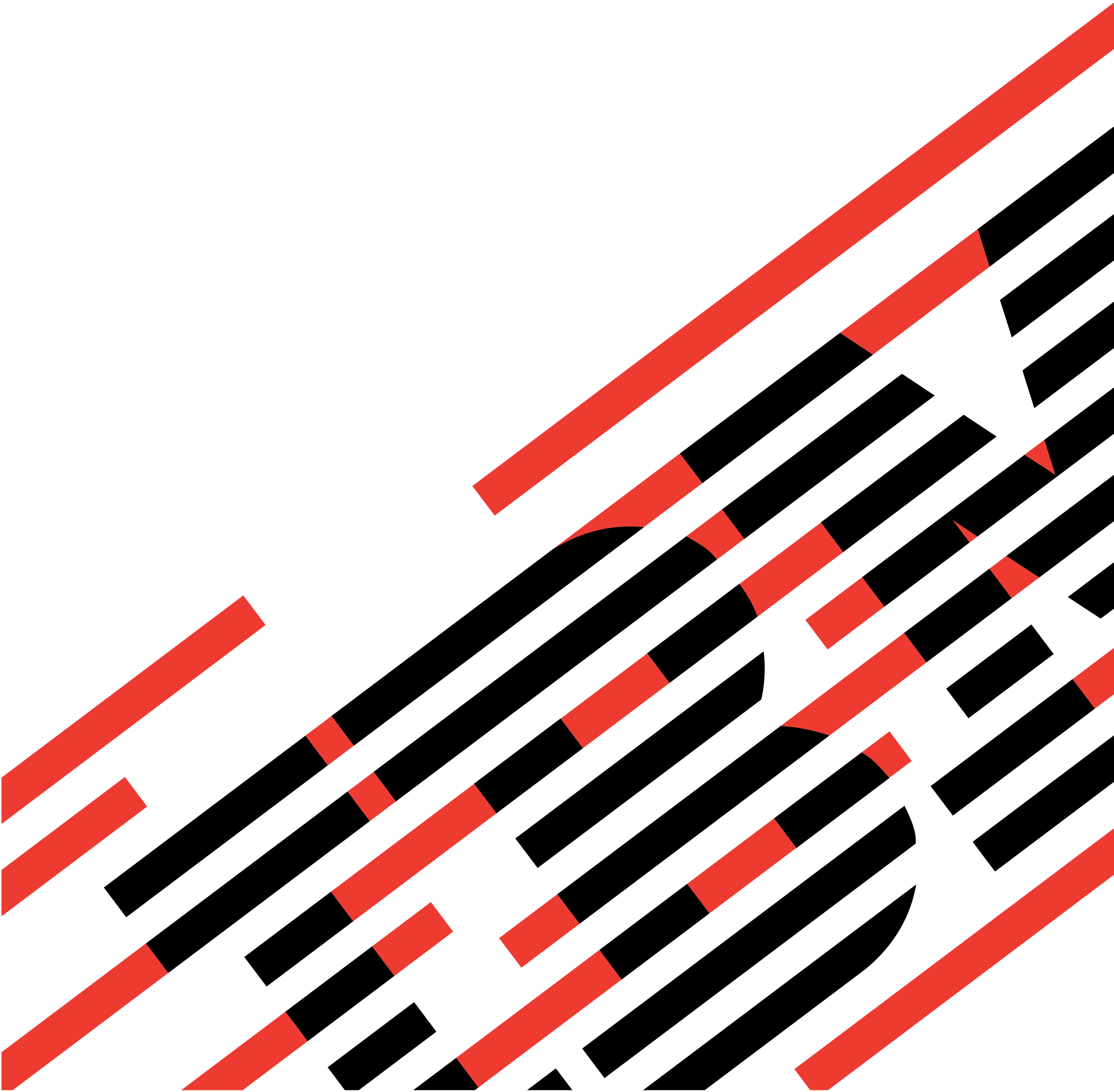
IBM

eserver

iSeries

Service tools



iSeries

Service tools

Contents

Service tools

Service tools are used to configure, manage, and service your server. 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.

Before beginning, review the following information:

What's new for V5R2
Find out what has changed for V5R2, as well as any late-breaking information.

Print this topic
Print a PDF of all the information included in the Service tools topic.

For more information about service tools, select any of the following topics:

Service tools concepts
This topic contains general information that needs to be understood before beginning to manage service tools, including definitions of the service tools terms used throughout this topic.

Manage service tools
Learn how to manage service tools on your server.

Troubleshoot
Troubleshoot common service tools problems.

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

What's new for V5R2

Service tools is a new topic in the Information Center for V5R2. Not only is this information new, but there are also significant enhancements to service tools for V5R2.

Manage service tools user IDs from SST

Service tools user IDs can now be managed and created from system service tools (SST). You no longer need to go into dedicated service tools (DST) to reset passwords, grant or revoke privileges, or create service tools user IDs. These functions can now be accessed from SST by selecting option 8 (Work with service tools user IDs) from the main SST display.

If you want to create a service tools user ID or use the Work with service tools user IDs option from SST, the password for the service tools user ID you use to sign on must not be the default password. If you sign on to SST using a service tools user ID that has a default password and try to create a new service tools user ID or use the Work with service tools user IDs option, an error results.

Limited ability to change default and expired passwords

The server is shipped with limited ability to change default and expired passwords. This means that service tools user IDs that have default and expired passwords cannot be changed through the Change

Service Tools User ID (QSYCHGDS) API, nor can their passwords be changed through SST. A service tools user ID with a default and expired password can only be changed through DST.

You can change the setting to allow default and expired passwords to be changed. Use SST or DST and select the Work with System Security option. From the Work with System Security display, change the **Allow a service tools user ID with a default and expired password to change its own password** field from No (the default) to Yes.

Terminology changed

The textual data and other documentation have been changed to reflect the new service tools terminology, specifically the use of the term service tools user IDs instead of previous uses such as DST user profiles, DST user IDs, service tools user profiles, or variations of these names.

Start service tools (STRSST) privilege added

A new Start service tools (STRSST) privilege has been added. This privilege allows a service tools user ID to be created that can access DST, but can be restricted from accessing SST.

Memorandum to Users

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

Print this topic

To view or download the PDF version, select Service tools (about 109 KB or 24 pages).

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...**
3. Navigate to the directory in which you would like to save the PDF.
4. Click **Save**.

Downloading Adobe Acrobat Reader

If 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) .

Service tools concepts

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

Service tools terminology
This information contains definitions of the service tools terms used throughout this topic.

DST and SST
This information describes what DST and SST are and the differences between them.

Service tools user IDs
This information describes service tools user IDs and functional privileges.

Password policies for service tools user IDs
This information describes the password policies for service tools user IDs.

Service tools server
This information describes the service tools server.

Service tools terminology

The following definitions will help you understand the service tools 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 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 determination and problem solving, often with the assistance of IBM support. Examples of service functions include licensed internal code (LIC) trace, licensed internal code (LIC) 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
User IDs that are 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 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

Dedicated service tools (DST) and 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 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 QSRV or the following authorizations: • Authorized to STRSST (Start SST) CL command. • Service special authority (*SERVICE) or All object special authority (*ALLOBJ). • 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
- 11111111
- 22222222

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.

IBM has also provided the ability to create additional service tools user IDs. This way, a security administrator can manage and audit the use of service tools without giving out the passwords to the IBM-supplied service tools user IDs. Creating additional service tools user IDs is done through the dedicated service tools (DST) or system service tools (SST).

Service tools user IDs have expiration dates, which allow you to minimize your server's security risk. For example, you can create a service tools user ID for a service technician that is valid for a short time, granting that technician access to only the service tools necessary. The user ID can also be disabled if the 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 by service tools users.

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.

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.

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 for DST, OS/400, or both. Once configured, authorized users can use functions such as LPAR or disk management in iSeries Navigator.

Note: You will be unable to access any iSeries Navigator service functions until you have configured and started the service tools server.

Manage service tools

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

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

Manage service tools user IDs
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
Configure the service tools server for DST, OS/400, or both.

Monitor service function use
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 from SST or DST.

The following sections provide the steps to access service tools using all of these methods.

Access service tools with 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 power down 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 with 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.
   - **Password:** The password associated with this user ID.
3. Press Enter.

Access service tools with 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 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 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
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
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
Save and restore critical service tools security data.

Recommendations for managing service tools user IDs
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). Once you have configured the service tools user IDs, you can change service tools user IDs and passwords.

Create a service tools user ID

To create a service tools user ID from DST or SST, complete the following steps:

1. Start DST or SST.
2. Sign on to DST or SST using your service tools user ID and password.
   - In DST, 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. Continue with step **3** below.
   - In SST, the System Service Tools (SST) main menu appears. Select option 8 (Work with Service Tools User IDs). The Work with Service Tools User IDs display appears. Continue with step **4** below.
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. 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.
5. 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.
6. 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 for more information about changing functional privileges.

Change the functional privileges for a service tools user ID

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

1. Start DST or SST.
2. Sign on to DST or SST using your service tools user ID and password.
   - In DST, 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. Continue with step **3** below.
   - In SST, the System Service Tools (SST) main menu appears. Select option 8 (Work with Service Tools User IDs). The Work with Service Tools User IDs display appears. Continue with step **4** below.
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 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

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

1. Start DST or SST.
2. Sign on to DST or SST using your service tools user ID and password.
   - In DST, 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. Continue with step **3** below.

   - In SST, the System Service Tools (SST) main menu appears. Select option 8 (Work with Service Tools User IDs). The Work with Service Tools User IDs display appears. Continue with step **4** below.
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

To display a service tools user ID from DST or SST, complete the following steps:

1. Start DST or SST.
2. Sign on to DST or SST using your service tools user ID and password.
   - In DST, 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. Continue with step **3** below.
   - In SST, the System Service Tools (SST) main menu appears. Select option 8 (Work with Service Tools User IDs). The Work with Service Tools User IDs display appears. Continue with step **4** below.
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 or disable a service tools user ID

To **enable** a service tools user ID from DST or SST, complete the following steps:

1. Start DST or SST.
2. Sign on to DST or SST using your service tools user ID and password.
   - In DST, 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. Continue with step **3** below.
   - In SST, the System Service Tools (SST) main menu appears. Select option 8 (Work with Service Tools User IDs). The Work with Service Tools User IDs display appears. Continue with step **4** below.
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.

To **disable** a service tools user ID from DST or SST, complete the following steps:

1. Start DST or SST.
2. Sign on to DST or SST using your service tools user ID and password.
   - In DST, 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. Continue with step **3** below.
   - In SST, the System Service Tools (SST) main menu appears. Select option 8 (Work with Service Tools User IDs). The Work with Service Tools User IDs display appears. Continue with step **4** below.
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

You can delete a service tools user ID from DST or SST. IBM-supplied service tools user IDs cannot be deleted. To delete a service tools user ID, complete the following steps:

1. Start DST or SST.
2. Sign on to DST or SST using your service tools user ID and password.
   - In DST, 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. Continue with step **3** below.
   - In SST, the System Service Tools (SST) main menu appears. Select option 8 (Work with Service Tools User IDs). The Work with Service Tools User IDs display appears. Continue with step **4** below.
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.

Change service tools user IDs and passwords

This information explains how to change service tools user IDs and passwords. You should have already configured your service tools user IDs and you may want to review the recommendations for managing service tools user IDs 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 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 using SST or DST

You can change service tools user IDs and passwords from SST or 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.
      - **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.

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). The Work with Service Tools User IDs display appears.
4. On the Work with Service Tools User ID display, find the user ID to change and type 2 (Change password) in the Option field.
5. 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.
   - **Set Password to expired:** Type 1 (Yes) or 2 (No) in this field. The default value is 1 (Yes).
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 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.

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 Starting and stopping the iSeries 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). 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 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 (LIC). 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 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

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 by dedicating a network interface card to the service tools server. 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 6 (Console mode) and press Enter. The Select Console Type display appears.
4. From the Select Console Type display, press F11 (Configure). The Configure Service Tools Adapter display appears.
5. From the Configure Service Tools Adapter display, enter the LAN Adapter and TCP/IP information. Press F1 (Help) for the type of information required in each field.
6. Press F7 (Store) to save your changes.
7. 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 prior to 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 quotes)
   - 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:

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 on **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 .

Troubleshoot service tools

Use this information to understand your options when you have problems with service tools. 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 reenable 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).

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 topic. You can view or print any of the PDFs.

Manuals

- **Tips and Tools for Securing Your iSeries** (about 1420 KB or 276 pages)
  A manual that provides a set of practical suggestions for using the security functions of iSeries servers and for establishing operating procedures that are security-conscious.

- **iSeries Service Functions** (about 1780 KB or 360 pages)
  A manual located on the *Supplemental Manuals* CD-ROM that provides basic information about iSeries service functions that are commonly used by hardware service representatives. The book is meant to assist the hardware service representative in gathering information about commonly encountered hardware problems. It does not cover all service functions available on the iSeries server.

- **iSeries Security Reference** (about 4260 KB or 688 pages)
  This manual provides information about planning, setting up, managing, and auditing security on your iSeries server. It describes all the features of security on the system and discusses how security features relate to other aspects of the system, such as work management, backup and recovery, and application design.

Other information

- Security
- Operations Console
- Logical partitions
- iSeries Navigator

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...**
3. Navigate to the directory in which you would like to save the PDF.
4. Click **Save**.

If 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) .

Printed in U.S.A.