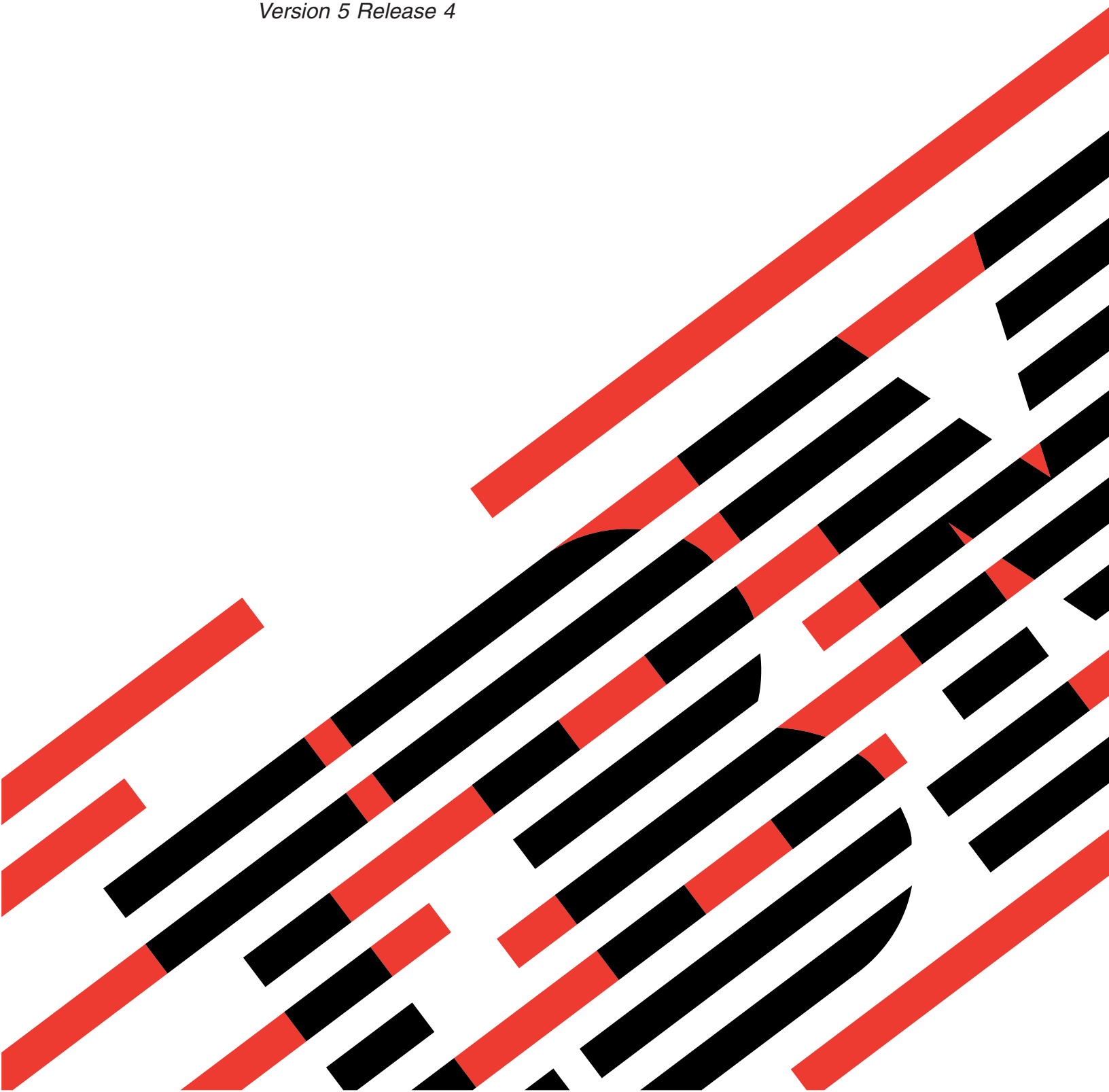
IBM Systems - iSeries

Security
Service tools user IDs and passwords

Version 5 Release 4



IBM Systems - iSeries

Security
Service tools user IDs and passwords

Version 5 Release 4

Note

Before using this information and the product it supports, read the information in "Notices," on page 29.

Fourth Edition (February 2006)

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

Contents

Service tools user IDs and passwords

Service tools are used to configure, manage, and service your IBM® @server iSeries™ model 270 or 8*xx* or logical partitions. If you want to manage logical partitions on servers other than model 8*xx*, you must use the Hardware Management Console (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 collection, the term service tools user IDs is used.

What's new for V5R4

For V5R4, you can use a new service tools user privilege called Take over console, which allows an Operations Console to take control from another console device.

For more information, see Take over or recover an Operations Console connection.

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.

Printable PDFs

Use this to view and print a PDF of this information.

To view or download the PDF version of this document, select Service tools user IDs and passwords (405 KB).

You can view or download the related topic Operations Console (1105 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 or topics:

- 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 the option that saves the PDF locally.
3. Navigate to the directory in which you want to save the PDF.
4. Click **Save**.

Downloading Adobe Reader

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

Concepts for service tools user IDs and passwords

These 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

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 cannot 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.

i5/OS™ user profiles
User profiles that are created with the Create User Profile (CRTUSRPRF) control language (CL) command or iSeries Navigator, and are used to sign on to the operating system.

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.

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 configuring your logical partitions, managing your disk units, and troubleshooting 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 user profiles.

system service tools (SST)
System service tools (SST) allow you to access service functions from operating system. 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 i5/OS has not been loaded. SST is available from the operating system.

Service tools are used to perform the following actions:

Note: This list is not all inclusive but gives you an overview of the functions provided by service tools.

- 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
- Take over console: A service tools user privilege that allows an Operations Console to take control from another console device.

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. i5/OS is not required to access DST.	Available when the operating system has been started. i5/OS is required to access SST.
How to authenticate	Requires service tools user ID and password.	Requires service tools user ID and password.

Related information

Take over or recover an Operations Console connection

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 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). Specific authorities are granted to the IBM-provided service tools user IDs. The IBM-supplied service tools user ID 11111111 is useful when upgrading Operations Console.

Note: When IBM ships a server, there is a QSECOFR i5/OS 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 user profile. Service tools user IDs have different password policies than i5/OS 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).

Attention: If you lose or forget the passwords for all i5/OS security officer profiles and all security service tools user IDs, you might need to install and initialize your system from distribution media to recover them. For this reason, it is recommended that you create multiple profiles and user IDs. Contact your service provider for assistance.

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 control which service functions can be accessed by any service tools user ID. Here are some examples of how you might 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.

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.

Related concepts

"Monitor service function use" on page 25
You can monitor the use of service functions through DST, and you can monitor service tools use through the security audit log. These logs can help you trace unusual access patterns or other potential security risks.

Related reference

"Password policies for service tools user IDs"
This topic describes the password policies for service tools user IDs and the process of changing Data Encryption Standard (DES) and Secure Hash Algorithm (SHA) encryption.

"Access service tools" on page 7
You can access service tools using DST, SST, and iSeries Navigator.

Related information

Tips and tools for securing your iSeries

Operations console

Secure your Operations Console configuration

Password policies for service tools user IDs

This topic describes the password policies for service tools user IDs and the process of changing Data Encryption Standard (DES) and Secure Hash Algorithm (SHA) encryption.

Note: Multiple incorrect password attempts to sign on will disable the service tools user ID. If that occurs, you can sign on with the disabled user ID from the console, and then reset the user ID.

Service tools user IDs are separate from i5/OS user profiles. Passwords for service tools user IDs are encrypted at different levels for security. The default password level uses 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 SHA encryption, which is mathematically impossible to reverse and provides stronger encryption and a higher level of security. If you change to SHA encryption, however, you cannot change back to DES encryption. Also, if you change to SHA encryption, you can no longer connect to the service tools server with pre-V5R1 clients, such as Operations Console. When you upgrade your password level to SHA, you need to upgrade any clients that use these functions.

DES encryption

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

- Use 10-digit, uppercase user IDs.
- Use 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:

- Use 10-digit, uppercase user IDs.
- Use 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.

Related concepts

"Access service tools using DST" on page 8
The service tools user ID you use to access service tools with DST needs to have the functional privilege to use the DST environment.

"Change service tools user IDs and passwords using STRSST or Change Service Tools User ID (QSYCHGDS) API" on page 18
You can change your service tools user ID password using STRSST or the Change Service Tools User ID (QSYCHGDS) API.

"Recover or reset QSECOFR passwords" on page 19
When IBM ships a server, both a QSECOFR i5/OS 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.

Related tasks

"Change service tools user IDs and passwords using DST" on page 17
You can change a service tools user ID password using DST.

"Change service tools user IDs and passwords using SST" on page 17
You can change a service tools user ID password using SST.

Related reference

"Service tools user IDs" on page 4
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 user profiles.

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, i5/OS, or both. After configuration, 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 i5/OS partitions.
3. If you use Operations Console (LAN), the service tools server is already configured.

Related concepts

"Access service tools using iSeries Navigator" on page 9
You can access service tools using iSeries Navigator when the server has been powered on to DST or when i5/OS is running.

Related reference

"Configure the service tools server" on page 23
You can configure the service tools server for DST, i5/OS, or both.

Related information

Partitioning with iSeries Navigator

Disk management

Manage service tools user IDs and passwords

You can develop an effective strategy for managing and maintaining service tools user IDs and passwords.

Access service tools

You can access service tools using DST, SST, and iSeries Navigator.

After 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.

Related reference

"Service tools user IDs" on page 4
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 user profiles.

"Manage service tools user IDs" on page 10
To develop an effective strategy for managing and maintaining service tools user IDs, you need to configure and change service tools user IDs, recover or reset QSECOFR passwords, and save or restore service tools security data.

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.

Access service tools using DST from the system control panel

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.

Access service tools using DST from a manual IPL

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 i5/OS, enter the Power Down System (PWRDWNSYS) command, PWRDWNSYS *IMMED RESTART(*YES), on an i5/OS 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.

Related reference

"Password policies for service tools user IDs" on page 5
This topic describes the password policies for service tools user IDs and the process of changing Data Encryption Standard (DES) and Secure Hash Algorithm (SHA) encryption.

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 i5/OS user profile needs to have the following authorizations:

- Authorization to the CL command Start SST (STRSST)
- Service special authority (*SERVICE)

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

1. Enter `STRSST (Start SST)` on an i5/OS 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.
   - **Password:** The password associated with this user ID.
3. Press Enter.

Related reference

"Configure service tools user IDs" on page 10
You can create, change, delete, and display service tools user IDs from dedicated service tools (DST) or system service tools (SST).

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 i5/OS is running.

Access service tools using iSeries Navigator when powered on to DST

Note: If you use Operations Console (LAN), the service tools server is already configured.

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. After you select the Taskpad item, you need to type the IP address of the server to which you want to connect.

Access service tools using iSeries Navigator when running i5/OS

To access service tools using iSeries Navigator when the server is running **i5/OS**, make sure the Service tools server is configured for i5/OS 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.

Related tasks

"Configure the service tools server for i5/OS" on page 24
You must add the service tools server to the service table in order to access service tools on i5/OS using TCP/IP and iSeries Navigator.

Related reference

"Service tools server" on page 7
The service tools server allows you to use your PC to perform service functions through TCP/IP.

"Configure the service tools server for DST" on page 23
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 because it is already available to you when the server has been powered on to DST.

Related information

iSeries Navigator

Manage service tools user IDs

To develop an effective strategy for managing and maintaining service tools user IDs, you need to configure and change service tools user IDs, recover or reset QSECOFR passwords, and save or restore service tools security data.

Related reference

"Access service tools" on page 7
You can access service tools using DST, SST, and iSeries Navigator.

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.

Related tasks

"Access service tools using SST" on page 9
The service tools user ID you use to access SST needs to have the functional privilege to use SST.

"Configure the service tools server using DST" on page 23
You can enable the service tools server with its own network interface card from DST.

"Configure the service tools server using SST" on page 24
You can enable the service tools server with its own network interface card from SST.

Related reference

"Change service tools user IDs and passwords" on page 16
This information explains how to change service tools user IDs and passwords.

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.

Related tasks

"Change service tools user IDs and passwords using DST" on page 17
You can change a service tools user ID password using DST.

Create a service tools user ID using DST:

You can create a service tools user ID from 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. After all information about the user ID has been entered, you can choose one of these 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 the service tools to which privileges might be granted. See "Change the functional privileges for a service tools user ID using DST" for more information about changing functional privileges.

Related tasks

"Change service tools user IDs and passwords using DST" on page 17
You can change a service tools user ID password using DST.

Change the functional privileges for a service tools user ID using DST:

You can change the functional privileges for a service tools user ID from 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.
   - Type 1 (Revoke) in the Option field next to the functional privileges you want to remove from the user ID.
   - 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:

You can change the description for a service tools user ID from 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 might include the user's name, department, and telephone number.

Display a service tools user ID using DST:

You can display a service tools user ID from 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 information:
   - 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:

You can enable a service tools user ID from 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:

You can disable a service tools user ID from 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 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 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.

Related tasks

"Change service tools user IDs and passwords using SST" on page 17
You can change a service tools user ID password using SST.

Create a service tools user ID using SST:

You can create a service tools user ID from 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. After all information about the user ID has been entered, you can choose one of these 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 the service tools to which privileges might be granted. See "Change the functional privileges for a service tools user ID using SST" for more information about changing functional privileges.

Related tasks

"Change service tools user IDs and passwords using SST" on page 17
You can change a service tools user ID password using SST.

Change the functional privileges for a service tools user ID using SST:

You can change the functional privileges for a service tools user ID from 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.
   - Type 1 (Revoke) in the Option field next to the functional privileges you want to remove from the user ID.
   - 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:

You can change the description for a service tools user ID from 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 might include the user's name, department, and telephone number.

Display a service tools user ID using SST:

You can display a service tools user ID from 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 information:
   - 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:

You can enable a service tools user ID from 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:

You can disable a service tools user ID from 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 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 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 service tools user IDs and you might 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 i5/OS security officer profiles and all security service tools user IDs, you might need to install and initialize your system from distribution media to recover them. For this reason, it is recommended that you create multiple profiles and user IDs. Contact your service provider for assistance.

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.

Related concepts

"Recover or reset QSECOFR passwords" on page 19
When IBM ships a server, both a QSECOFR i5/OS 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.

Related reference

"Configure service tools user IDs" on page 10
You can create, change, delete, and display service tools user IDs from dedicated service tools (DST) or system service tools (SST).

"Recommendations for managing service tools user IDs" on page 22
This information provides the recommendations for managing service tools user IDs.

Change service tools user IDs and passwords using DST:

You can change a service tools user ID password using DST.

To change a service tools user ID password using DST, complete the following steps:

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 is not accepted, you might 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.

Related tasks

"Create a service tools user ID using DST" on page 10
You can create a service tools user ID from DST.

Related reference

"Configure service tools user IDs using DST" on page 10
You can create, change, display, enable, disable, or delete service tools user IDs from DST.

"Password policies for service tools user IDs" on page 5
This topic describes the password policies for service tools user IDs and the process of changing Data Encryption Standard (DES) and Secure Hash Algorithm (SHA) encryption.

Change service tools user IDs and passwords using SST:

You can change a service tools user ID password using SST.

To change a service tools user ID password using SST, complete the following steps:

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 is not accepted, you might 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.

Related tasks

"Create a service tools user ID using SST" on page 13
You can create a service tools user ID from SST.

Related reference

"Configure service tools user IDs using SST" on page 13
You can create, change, display, enable, disable, or delete service tools user IDs from SST.

"Password policies for service tools user IDs" on page 5
This topic describes the password policies for service tools user IDs and the process of changing Data Encryption Standard (DES) and Secure Hash Algorithm (SHA) encryption.

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.

Related reference

"Password policies for service tools user IDs" on page 5
This topic describes the password policies for service tools user IDs and the process of changing Data Encryption Standard (DES) and Secure Hash Algorithm (SHA) encryption.

Change your service tools user ID password using STRSST:

You can 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 signon 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 are typed correctly and your new password is accepted, you will be able to sign on with your new password. If your new password is not accepted, you might 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:

This 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.

The Change Service Tools User ID (QSYCHGDS) 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.

Related information

Change Service Tools User ID (QSYCHGDS) API

Change default and expired passwords:

You can change default and expired service tools 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. Sign 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 i5/OS 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 i5/OS user profile. Service tools user IDs have different password policies than i5/OS user profiles.

If you lose or forget the passwords for both the QSECOFR i5/OS user profile and the QSECOFR service tools user ID, you might need to install your operating system again to recover them. For this reason, it is recommended that you create multiple profiles and user IDs. 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.

Related reference

“Change service tools user IDs and passwords” on page 16
This information explains how to change service tools user IDs and passwords.

“Recommendations for managing service tools user IDs” on page 22
This information provides the recommendations for managing service tools user IDs.

“Password policies for service tools user IDs” on page 5
This topic describes the password policies for service tools user IDs and the process of changing Data Encryption Standard (DES) and Secure Hash Algorithm (SHA) encryption.

Reset the QSECOFR i5/OS user profile password:

If you know the password for the QSECOFR service tools user ID, you can use it to reset the QSECOFR i5/OS 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 effect until after the IPL.

To reset the QSECOFR i5/OS user profile, 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. 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 i5/OS 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 included in every iSeries server and is commonly known.

Reset the QSECOFR service tools user ID and password:

If you know the password for the QSECOFR i5/OS 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.

Complete the following steps to reset the QSECOFR service tools user ID and password:

1. Ensure that the server is in normal operating mode, not DST.
2. Sign on at a workstation using the QSECOFR i5/OS user profile.

3. On a command line, enter CHGDSTPWD (Change IBM Service Tools Password). Then press F4 (Do not press Enter). You see the Change IBM Service Tools Password (CHGDSTPWD) display.
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.

```
                  Change IBM Service Tools Pwd (CHGDSTPWD)


Type choices, press Enter.


Password . . . . . . . . . . . .  *DEFAULT              *SAME, *DEFAULT
```

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 included in every iSeries server and is commonly known.

Save and restore service tools security data

The service tools security data is saved as part of a save system using the (SAVSYS) command or save Licensed Internal Code operation. 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:

You can save service tools security data using DST.

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 data. 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 data. 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:

You can restore service tools security data using DST.

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 data. 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 data. The Work with Optical Devices display appears.
  b. You might 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. Select the device from which you want to restore security data. The instructions for selecting the device 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

This information provides the recommendations for managing service tools user IDs.

Create your own version of the QSECOFR service tools user ID

Do not use the IBM-supplied service tools user ID QSECOFR. 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. Use this new user ID to manage your other service tools user IDs. This can help eliminate the security exposure that originates because QSECOFR is the value included in every server and is commonly known.

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 included in every iSeries 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. Because 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.

Related concepts

"Recover or reset QSECOFR passwords" on page 19
When IBM ships a server, both a QSECOFR i5/OS 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.

Related reference

"Change service tools user IDs and passwords" on page 16
This information explains how to change service tools user IDs and passwords.

Configure the service tools server

You can configure the service tools server for DST, i5/OS, or both.

Note: If your server is using Operations Console (LAN), the service tools server is already configured.

Related reference

"Service tools server" on page 7
The service tools server allows you to use your PC to perform service functions through TCP/IP.

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 because it is already available to you when the server has been powered on to DST.

The service tools server requires a dedicated LAN adapter unless Operations Console (LAN) is already in use or has previously been configured; for example, the LAN console is being used as a backup console. Verify that you have satisfied the hardware requirements using one of the following methods:

1. If your server is not running in a logical partitioning (LPAR) environment the service tools server resource is required to be installed in a specific location, based on your model. See Meet Operations Console hardware requirements to verify this location.
2. If your server is running in an LPAR environment, then the service tools server resource (I/O processor (IOP) that the LAN adapter reports to) must be tagged as the console and for electronic customer support (even if ECS is not being used).

You need to temporarily configure the server for Operations Console (LAN) in order to configure the LAN adapter and activate the resource. After you verify the resource is working properly, you can specify your original console.

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

Related concepts

"Access service tools using iSeries Navigator" on page 9
You can access service tools using iSeries Navigator when the server has been powered on to DST or when i5/OS is running.

Configure the service tools server using DST:

You can enable the service tools server with its own network interface card from 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 LAN adapter) and press Enter. The Configure Service Tools LAN Adapter display appears.

   Note: If you receive a message indicating no resource is available or it is the wrong type, you have not satisfied the hardware requirements for the service tools server. See Meet Operations Console hardware requirements.
4. From the Configure service tools LAN adapter display, 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.

Related reference

"Configure service tools user IDs" on page 10
You can create, change, delete, and display service tools user IDs from dedicated service tools (DST) or system service tools (SST).

Configure the service tools server using SST:

You can enable the service tools server with its own network interface card from 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 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.

Related reference

"Configure service tools user IDs" on page 10
You can create, change, delete, and display service tools user IDs from dedicated service tools (DST) or system service tools (SST).

Configure the service tools server for i5/OS

You must add the service tools server to the service table in order to access service tools on i5/OS 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 in 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. Enter ENDTCP (End TCP) to end TCP/IP if this is possible in your environment. TCP/IP must be ended and restarted for the service table entry to be used. If you cannot end TCP at this time, you will not be able to use the service tools server.

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 i5/OS partitions.

1. From an iSeries Navigator session, right-click the server name under **My Connections** (for your environment you might use your own name for the connections function instead of the default **My Connections**).
2. Click **Application Administration**.
3. Click **OK** until you see a window that has a **Host Applications** tab. Click the **Host Applications** tab, expand **i5/OS** → **Service**.
4. 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.
5. Click **OK**. These functions are now available to the iSeries Navigator user provided they have a service tools user ID.

After 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.

Related concepts

"Access service tools using iSeries Navigator" on page 9
You can access service tools using iSeries Navigator when the server has been powered on to DST or when i5/OS is running.

Related information

iSeries Navigator

Logical partition with HMC

Monitor service function use

You can monitor the use of service functions through DST, and you can monitor service tools use through the security audit log. These logs can help you trace unusual access patterns or other potential security risks.

Related reference

"Service tools user IDs" on page 4
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 user profiles.

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. You can use the DST security log to monitor service functions.

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 shows security-related activity by date and time.
6. Press F6 (Print) to print this log.
7. Type 5 (Display details) in the Option field of the activity you are interested in. The Display Service Tools Security Log Details display appears showing information for the activity you selected.

Monitor service tools use through i5/OS security audit log

You can use the i5/OS security audit log to record service tools actions.

To enable the i5/OS security audit log to record service tools actions, complete the following steps for each server on which you want to enable the i5/OS security audit log:

1. From an iSeries Navigator session, select the server name under **My Connections** (for your environment, you might 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. Click the **System** tab. Make sure the following items are checked (other items might also be checked):
   - Activate action auditing
   - Security tasks
   - Service tasks
4. Click **OK**. These security audit log functions are now available on the iSeries server.

After 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 Display Journal (DSPJRN) command, DSPJRN QSYS/QAUDJRN ENTTYP(ST), on an i5/OS command line.

After 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 iSeries Security Reference .

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 of too many incorrect password
| attempts. You know the password, but have typed incorrect characters or typed it in lowercase.

| 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).

Related information for Service tools user IDs and passwords

Listed here are the product manuals, 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

- Service tools user IDs and passwords (405 KB)
- Operations Console (1105 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 the option that saves the PDF locally.
3. Navigate to the directory in which you want to save the PDF.
4. Click **Save**.

Downloading Adobe Reader

You need Adobe Reader installed on your system to view or print these PDFs. You can download a free copy from the Adobe Web site (www.adobe.com/products/acrobat/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 grant you any license to these patents. You can send license inquiries, in writing, to:

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

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

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

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

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

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

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

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

IBM Corporation

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

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

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

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

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

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

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

COPYRIGHT LICENSE:

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

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

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

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

Programming Interface Information

This Service tools user IDs and passwords publication documents intended Programming Interfaces that allow the customer to write programs to obtain the services of IBM i5/OS.

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
IBM (logo)
iSeries

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

Terms and conditions

Permissions for the use of these publications is granted subject to the following terms and conditions.

Personal Use: You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of these publications, or any portion thereof, without the express consent of IBM.

Commercial Use: You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

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

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED ″AS-IS″ AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Printed in USA