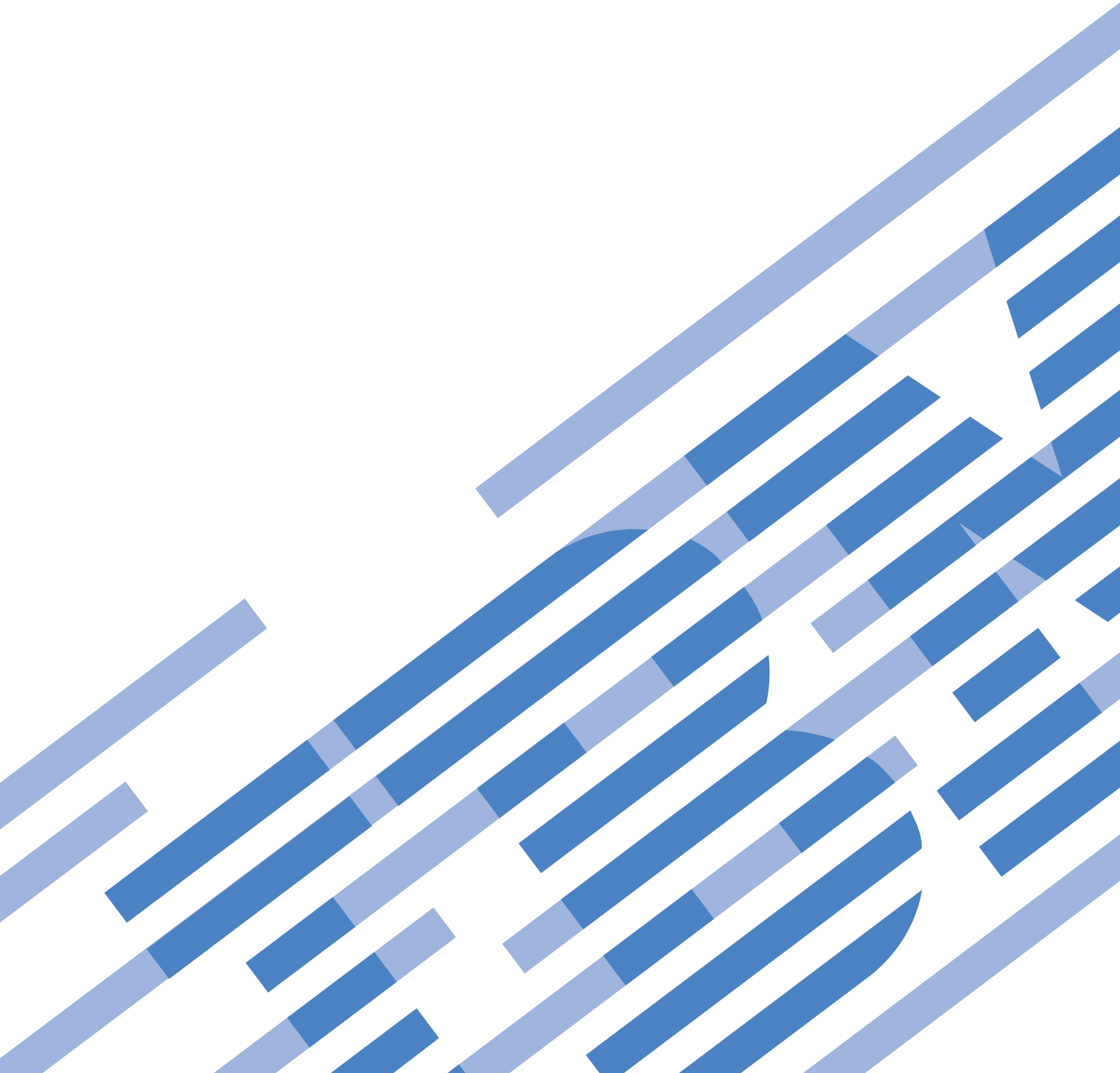




System i
Security
Service tools

Version 6 Release 1





System i
Security
Service tools

Version 6 Release 1

Note

Before using this information and the product it supports, read the information in "Notices," on page 39.

This edition applies to version 6, release 1, modification 0 of IBM i5/OS (product number 5761-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.

© **Copyright International Business Machines Corporation 2003, 2008.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Service tools	1	Resetting the QSECOFR service tools user ID and password	24
What's new for V6R1	1	Saving and restoring service tools security data	25
PDF file for Service tools	1	Saving service tools security data	25
Service tools concepts	2	Restoring service tools security data	25
Service tools functions	2	Enabling working with device IDs from SST	26
Service tools language versions	2	Managing service tools device IDs.	26
Service tools server	3	Managing service tools device IDs using DST and SST	26
Service tools user IDs	3	Managing service tools device IDs using DST	26
Password policies for service tools user IDs	5	Managing service tools device IDs using SST	28
Managing service tools	6	Resetting passwords for service tools device IDs	31
Accessing service tools	6	Resetting the passwords for service tools device IDs using DST	31
Accessing service tools using DST	6	Resetting service tools device IDs passwords using SST	31
Accessing service tools using SST	7	Resetting the QCONSOLE device profile password from the control panel	31
Accessing service tools using System i Navigator	8	Automatically creating device IDs	33
Configuring the service tools server	9	Changing service tools security policies	33
Configuring the service tools server for DST.	9	Changing to allow default and expired passwords to be used from SST.	33
Configuring the service tools server using DST	9	Changing the password expiration interval.	34
Configuring the service tools server using SST	10	Changing the maximum failed sign-on attempts	34
Configuring the service tools server for i5/OS	10	Changing the duplicate password control	34
Changing the service tools language of your system or logical partition	12	Troubleshooting service tools user IDs and passwords.	35
Managing service tools user IDs	13	Monitoring service function use	36
Linking service tools user IDs to user profiles	13	Monitoring service function use through DST	36
Managing service tools user IDs using DST and SST	13	Monitoring service tools use through security audit log	36
Recommendations for managing service tools user IDs.	14	Related information for Service tools	37
Managing service tools user IDs using DST	14	Appendix. Notices	39
Managing service tools user IDs using SST	18	Programming interface information	40
Changing passwords for service tools user IDs	21	Trademarks	41
Changing the passwords for service tools user IDs using DST.	21	Terms and conditions	41
Changing service tools user IDs and passwords using SST	22		
Changing service tools user IDs and passwords using the QSYCHGDS API	23		
Recovering or resetting QSECOFR passwords	23		
Resetting the QSECOFR user profile password	23		

Service tools

Service tools are used to configure, manage, and service models 5xx, models 8xx, and earlier, or the 8xx logical partitions (LPAR). To manage logical partitions on models other than 8xx, 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 if you want to access DST, SST, and to use the System i® Navigator functions for logical partition 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 V6R1

Read about new or significantly changed information for the Service tools topic collection.

- With the implementation of user ID integration, users can have a certain level of access to dedicated service tools (DST) using their i5/OS® user IDs and passwords. For more information, see [Linking service tools user IDs to user profiles](#).
- DST now supports automatic creation of device IDs through the service tools server. For more details, see [Automatically creating device IDs](#).

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.

In PDF files, you might see revision bars (|) in the left margin of new and changed information.

To find other information about what's new or changed this release, see the [Memo to users](#).

PDF file for Service tools

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


- | To view or download the PDF version of this document, select [Service tools \(about 420 KB\)](#).

Saving PDF files

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

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

Downloading Adobe Reader

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

Related reference

“Related information for Service tools” on page 37

Other information center topic collections contain information that relates to the Service tools topic collection. You can view or print any of the PDF files.

Service tools concepts

You need to understand some basic concepts that relate to service tools functions, service tools user IDs, and passwords.

Service tools provide various functions that you can perform through dedicated service tools (DST) or system service tools (SST), including diagnosing system problems, managing disk units, and managing system security. With the service tools server, you can also use your PC to perform service functions through TCP/IP.

To access these service tools functions through DST, SST, System i Navigator (for logical partitions and disk unit management), and Operations Console, service tools user IDs are required. To change or reset the passwords for the service tools user IDs, you must comply with certain password policies.

Related tasks

“Changing the password expiration interval” on page 34

To change the default password expiration interval from 180 days, follow these steps.

Service tools functions

You can use dedicated service tools (DST) or system service tools (SST) to access service tools functions. DST is available when the Licensed Internal Code is started even if the operating system has not been loaded. SST is available from the operating system.

Service tools are used to perform the following actions. This list is not all inclusive but gives you an overview of the functions provided by service tools:

- Add hardware resources to the system.
- Diagnose system problems.
- Manage disk units.
- Manage logical partition (LPAR) activities, including memory.
- Manage or view main storage dumps.
- Manage other service tools user IDs.
- Manage system security.
- Manage the Take over console function, which allows a second LAN console to take over an existing LAN console.
 1. You need to enable the Take over console before using it. To do so, use the Select console menu.
 2. When attempting to take over an existing LAN console with a second LAN console, the user must have the Take over privilege or the Service tool security privilege.
- Review the Licensed Internal Code and product activity logs.
- Trace Licensed Internal Code.

Related information

Takeover or recovery of an Operations Console connection

Service tools language versions

If you want to use a different language version as the service language, you can change it in the service environments of dedicated service tools (DST) and system service tools (SST). You can also change the service language back to a previously chosen language. By default, the primary language of the current operating system and the service language stay in synch unless you change the service language.

Related tasks

“Changing the service tools language of your system or logical partition” on page 12
You can change the service tools language to the language of your service representative. This procedure can guide you through installing a service tools language.

Service tools server

With the service tools server, you can use your PC to perform service functions through Transmission Control Protocol/Internet Protocol (TCP/IP).

To use the service tools server to perform GUI-based logical partitions or disk management activities, you need to make the service tools server available. You can configure the service tools server for DST, the operating system, or both. After configuration, authorized users can use functions such as logical partition or disk management in System i Navigator.

Notes:

1. You cannot access any System i Navigator service functions until you have configured and started the service tools server.
2. If your server model is not 8xx, you must use the Hardware Management Console (HMC) to manage i5/OS logical partitions.
3. If you use Operations Console (LAN), the service tools server is already configured.

Related concepts

“Accessing service tools using System i Navigator” on page 8

From System i Navigator, you can access service tools when your system is powered on to dedicated service tools (DST), or when the system is running i5/OS.

Related reference

“Configuring the service tools server” on page 9

You can configure the service tools server for dedicated service tools (DST), the operating system, or both.

Related information

Logical partitions

Disk management

Service tools user IDs

Service tools user IDs are user IDs that are required for accessing service functions through dedicated service tools (DST), system service tools (SST), System i 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 i5/OS 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: A QSECOFR user profile and a QSECOFR service tools user ID are provided with every system. The QSECOFR user profile and the QSECOFR service tools user ID 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 from 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 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 suggested that you create multiple profiles and user IDs. Contact your service provider for assistance.

The passwords for service tools user IDs can have expiration dates, which allow you to minimize the security risk to your system. When users sign on with an expired password, they must change the password. A service tools user ID can be disabled, in which case it cannot be used at all until someone with the appropriate authority level re-enables it.

Functional privileges for service tools user IDs

Functional privileges control which service functions can be accessed by any service tools user ID. You can set up functional privileges to grant or revoke the ability for a service tools user ID to access individual service functions. These examples show 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 prevents people from using the known QSECOFR user ID and helps protect your system from security risks.

You can manage the functional privileges through DST or SST. When set to revoked, the Start Service Tools privilege allows a service tools user ID to access service functions through DST, but restricts the user ID 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.

Related concepts

“Monitoring service function use” on page 36

You can monitor the use of service functions through the dedicated service tools (DST) security log or through the i5/OS security audit log. These logs help you trace unusual access patterns or potential security risks.

Related reference

“Password policies for service tools user IDs” on page 5

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

“Accessing service tools” on page 6

To access service tools, you can use dedicated service tools (DST), system service tools (SST), or System i Navigator.

Related information

Operations console

Password policies for service tools user IDs

Here are 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 attempts to sign on with incorrect password can disable the service tools user ID. If the user ID is QSECOFR, additional sign-on attempts are allowed until the correct password has been entered, and the user is signed on. You can now re-enable the QSECOFR user ID. To enable other user IDs, you must have the QSECOFR user ID or another user ID that has the service tool security privilege.

Service tools user IDs are separate from i5/OS user profiles. Passwords for service tools user IDs are encrypted at different levels of security. The default password level uses DES encryption. You should use DES encryption if you have pre-V5R1 clients that use System i 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.
- Even though passwords don't expire when using DES encryption, it still can be created expired.
- By default, passwords are initially set as expired (unless explicitly set on the display to No).

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.
- By default, passwords for user IDs expire after 180 days. The expiration interval can be changed through Option 8 (Password expiration interval in days) on the Work with Service Tools Security Data menu. The value can be 0 for *NOMAX or up to 999 days.
- By default, passwords are initially set as expired (unless explicitly set on the display to No).

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 is shown.
2. Select option 5 (Work with DST environment) and press Enter. The Work with DST Environment display is shown.
3. Select option 6 (Service tools security data) and press Enter.

- Select option 6 (Change password level) and press Enter. Press Enter again if you are ready to go to the new password level. The current status of PWLVL 2 is displayed.

Related concepts

“Accessing service tools using DST”

To access service tools, you can use dedicated service tools (DST) from the system control panel or from a manual initial program load (IPL).

Managing service tools

- To effectively work with your service tools, you need to know the different ways to access service tools, how to change the service tools language, how to configure the service tools server, and how to change your user IDs and passwords.

Accessing service tools

To access service tools, you can use dedicated service tools (DST), system service tools (SST), or System i Navigator.

The service functions available to you depend on the functional privileges you have. If you do not have the correct privileges, you cannot sign on to SST. If you have the appropriate functional privileges, you can manage service tools user IDs from SST or DST.

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 an interactive job with the ability to sign on with QSECOFR or the following authorizations: <ul style="list-style-type: none"> • Authorization to the Start SST (STRSST) CL command. • Service special authority (*SERVICE). • Functional privilege to use SST.
When available	Available even when the system has limited capabilities. The operating system is not required for accessing DST.	Available when the operating system is started. The operating system is required for accessing SST.
How to authenticate	Requires service tools user ID and password.	Requires a service tools user ID and password.

Accessing service tools using DST

To access service tools, you can use dedicated service tools (DST) from the system control panel or from a manual initial program load (IPL).

The service tools user ID that you use to access service tools with DST needs to have the functional privilege to use DST. You can start the DST by using function 21 from the system control panel or by using a manual initial program load (IPL).

Accessing service tools using DST from the system control panel

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

- Put the control panel in manual mode.
- Use the control panel to select function 21 and press Enter. The DST Sign On display appears on the console.
- 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.

Accessing service tools using DST from a manual IPL

To access service tools using DST from a manual initial program load (IPL), complete the following steps:

1. Put the control panel in manual mode.
2. Take either of the following actions:
 - If the system is powered off, turn the system on.
 - If the system is powered on, enter the Power Down System (PWRDWN SYS) command, PWRDWN SYS *IMMED RESTART(*YES), on a command line to turn off the system and restart it.
3. Sign on to DST using your service tools user ID and password. The Use dedicated service tools (DST) display is shown.
4. 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.

Accessing service tools using SST

If your user profile has the required authorizations, you can use system service tools (SST) to access service tools.

About this task

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 Start SST (STRSST) CL command.
- 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 is shown.
2. Enter the following information:
 - **Service Tools User ID:** The service tools user ID you sign on with.
 - **Password:** The password associated with this user ID.
3. Press Enter.

Results

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: <ul style="list-style-type: none">• Authorization to the Start SST (STRSST) CL command.• Service special authority (*SERVICE).• Functional privilege to use SST.
When available	Available even when the system has limited capabilities. The operating system is not required for accessing DST.	Available when the operating system is started. The operating system is required for accessing SST.
How to authenticate	Requires service tools user ID and password.	Requires service tools user ID and password.

Accessing service tools using System i Navigator

From System i Navigator, you can access service tools when your system is powered on to dedicated service tools (DST), or when the system is running i5/OS.

Accessing service tools using System i Navigator when the system is powered on to DST

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

To access service tools using System i Navigator when the system is powered on to DST, make sure that the service tools server is configured for DST and has been started, and then complete the following steps:

1. From System i Navigator, select **My Connections** or your active environment.
2. Select Open System i Navigator Service Tools Window in the Taskpad window. If the Taskpad window is not displayed, select **View** and select **Taskpad**.
3. After the Open Service Tools Window is displayed, type the name or IP address of the system to which you want to connect.

Accessing service tools using System i Navigator when the system is running i5/OS

To access service tools using System i Navigator when the system is running i5/OS, make sure that the service tools server is configured for the operating system and has been started, and then complete the following steps:

1. From System i Navigator, expand **My Connections** or your active environment.
2. Select the system 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. Sign on using your service tools user ID and password when prompted.

Related reference

“Service tools server” on page 3

With the service tools server, you can use your PC to perform service functions through Transmission Control Protocol/Internet Protocol (TCP/IP).

Related information

Connecting to System i: System i Navigator

Configuring the service tools server

You can configure the service tools server for dedicated service tools (DST), the operating system, or both.

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

Related reference

“Service tools server” on page 3

With the service tools server, you can use your PC to perform service functions through Transmission Control Protocol/Internet Protocol (TCP/IP).

Configuring the service tools server for DST

You can configure the service tools server to be available when your system is powered on to dedicated service tools (DST).

If you use only the Operations Console with LAN connectivity to perform DST activities, you do not need to reconfigure the service tools server because it is already available to you when the system is powered on to DST.

| The service tools server may require 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 system is not running in a logical partitioning environment, the service interface used for the
| service tools server is required to be installed in a specific location, based on your model. See
| Operations Console hardware requirements to verify this location.
- | 2. If your system is running in a logical partitioning environment, use one of the following options to
| specify the service tools server resource:
 - | • If your system is an 8xx model, then you need to tag the I/O processor (IOP) that the LAN adapter
| reports to as the console and for electronic customer support (even if electronic customer support is
| not being used.)
 - | • If your system is an i5/5xx model, then you need to tag the actual LAN adapter to be used for the
| service tools server as the console. You need to temporarily configure the system for Operations
| Console (LAN) to configure.

| To configure the LAN adapter and activate the resource, you need to temporarily configure the system
| for Operations Console (LAN). This might require a change in the console tag. After you verify that 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 as the
| service interface for use by the service tools server.

Related information

Operations Console hardware requirements

Configuring the service tools server using DST:

| To enable the service tools server with the service interface, complete these 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 Service Tools User IDs and Devices display, select option 4 (Configure service tools LAN adapter) and press Enter. You might get an error message that indicates that there is no valid hardware.

Note: If you receive a message that indicates no resource is available or it is the wrong type, you have not satisfied the hardware requirements for the service interface. This might indicate that you have not set the console tag yet.

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.

Results

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

Related reference

“Managing service tools user IDs using DST and SST” on page 13

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

Related information

Operations Console hardware requirements

Configuring the service tools server using SST:

To enable the service tools server with the service interface, complete these 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. You might get an error message that indicates that there is no valid hardware.

Note: If you receive a message that indicates no resource is available or it is the wrong type, you have not satisfied the hardware requirements for the service interface. This might indicate that you have not set the console tag yet.

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.

Results

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

Related reference

“Managing service tools user IDs using DST and SST” on page 13

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

Configuring the service tools server for i5/OS

To access service tools on the operating system using TCP/IP and System i Navigator, you must add the service tools server to the service table.

About this task

You can add the service tools server 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 before you can use the service table entry. If you cannot end TCP at this time, you cannot use the service tools server. Instead of using the ENDTCP or Start TCP (STRTCP) command, users can initial program load (IPL) at their convenience.
7. Enter STRTCP. 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.

Results

If you use System i Navigator to perform disk unit or logical partition configuration and management, you need to complete the following steps once per system:

Note: If your server model is not 8xx, you must use the Hardware Management Console (HMC) to manage i5/OS logical partitions.

1. From a System i Navigator session, right-click the system 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, and 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 System i Navigator users who have a service tools user ID.

After the service tools server is added to the service table, authorized users can access the logical partition (LPAR) and disk management service functions using System i 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 information

Logical partitions

Changing the service tools language of your system or logical partition

You can change the service tools language to the language of your service representative. This procedure can guide you through installing a service tools language.

About this task

Prerequisites

Before you begin to change the service tools language, obtain the media labeled as I_BASE_01. Ensure that the release and modification of your system are the same as that of your media. You need to be aware of the following things:

- You will need the CD image that contains the License Internal Code for the version, release, and modification level installed on the system.
- Image catalogs (virtual optical and tape devices) do not support the procedures in this topic.
- You can only change the service tools language one time before an initial program load (IPL) is required.

To change the service tools language on the system or logical partition, follow these steps:

1. Load the media labeled I_BASE_01 in the optical device.
2. Access service tools using DST.

Note: Use the service tools user ID QSECOFR to sign on to the DST.

3. Select option 5 (Work with DST environment).
4. Select option 7 (Change service tools language). The Select Service Tools Language display is shown including a list of service languages that you can choose from. The display also indicates the primary language of the current operating system.
5. Enter the language ID (29xx) of the service tools language that you want in the Selection field and press Enter. For example, if your service representatives understand English, you might want to choose 2924.
6. Select the optical device from step 1 and press Enter.
7. On the Confirm Select Service Tools Language display, press Enter.

Results

The next display depends on the method used to access service tools using DST.

- If you access the service tools using DST from the system control panel, the i5/OS Sign On display is shown.
- If you access the service tools using DST from a manual IPL, the IPL or Install the System display is shown.

Related reference

“Service tools language versions” on page 2

If you want to use a different language version as the service language, you can change it in the service environments of dedicated service tools (DST) and system service tools (SST). You can also change the service language back to a previously chosen language. By default, the primary language of the current operating system and the service language stay in synch unless you change the service language.

Managing service tools user IDs

Developing an effective strategy for managing service tools user IDs involves a series of tasks, such as configuring service tools user IDs, resetting QSECOFR passwords, and saving or restoring service tools security data.

Related reference

“Accessing service tools” on page 6

To access service tools, you can use dedicated service tools (DST), system service tools (SST), or System i Navigator.

Linking service tools user IDs to user profiles

If you link a service tools user ID to a user profile, you can have the privileges of the service tools user ID while using an i5/OS interface that requires those privileges.

Before you begin

You must have service (*SERVICE) special authority to use some APIs. To have the authority to call the advanced analysis commands, the current user profile must be linked to a service tools user ID that has the proper privileges.

About this task

To link a service tools user ID to user profiles, follow these steps:

1. Access service tools using DST.
2. From the DST Sign-On display, enter the QSECOFR service tools user ID and password.
3. Select option 5 (Work with DST environment) when the Use Dedicated Service Tools (DST) main menu is shown and press Enter. The Work with DST Environment display is shown.
4. From the Work with DST Environment display, select option 3 (Service tools user IDs) and press Enter.
5. From the Work with Service Tools User IDs display, type 9 (Link) on the line associated with the user you want to work with and press Enter. The Link Service Tools User ID display is shown.

Notes:

- If you choose option 9 for the QSECOFR service tools user ID, a message is shown at the bottom of the display: This Service Tools User ID cannot change the linked User Profile. The QSECOFR service tools user ID is always linked to the QSECOFR user profile. Users are not able to remove this link or link any other user profile to the QSECOFR service tools user ID.
 - Only one user profile is allowed to link to a service tools user ID and only one service tools user ID is allowed to link to a user profile. When a group profile is linked to a service tools user ID, then every member of that group profile can use the privileges of the service tools user ID.
6. Enter information about the tools user ID and the user profile it links to:
 - **Service tools user ID:** The name of the service tools user linked from.
 - **User profile:** The user profile to link to from the service tools user ID.
 7. Press Enter. The user profile is linked to from the service tools user ID.

Managing service tools user IDs using DST and SST

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

Related tasks

“Accessing service tools using SST” on page 7

If your user profile has the required authorizations, you can use system service tools (SST) to access service tools.

Related reference

“Changing passwords for service tools user IDs” on page 21

You have various ways to change the passwords for service tools user IDs. You can use dedicated service tools (DST), system service tools (SST), or the Change Service Tools User ID (QSYCHGDS) API.

Recommendations for managing service tools user IDs:

Here are the recommendations to ensure the security of your service tools user IDs.

Creating 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 system 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 system 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

“Recovering or resetting QSECOFR passwords” on page 23

Both a QSECOFR user profile and a QSECOFR service tools user ID are supplied with IBM systems. When you lose your QSECOFR user profile password or your QSECOFR service tools user ID, use one of the passwords to reset the other.

Related reference

“Changing passwords for service tools user IDs” on page 21

You have various ways to change the passwords for service tools user IDs. You can use dedicated service tools (DST), system service tools (SST), or the Change Service Tools User ID (QSYCHGDS) API.

Managing service tools user IDs using DST:

You can use dedicated service tools (DST) to create, change, display, enable, disable, and delete service tools user IDs.

Creating a service tools user ID using DST:

To create a service tools user ID using dedicated service tools (DST), follow these steps.

About this task

1. Access service tools using DST.
2. Sign on to DST using your service tools user ID and password.

3. When the Use dedicated service tools (DST) display is shown, select option 5 (Work with DST environment) and press Enter. The Work with DST Environment display is shown.
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 is shown.
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 is shown.

Note: User IDs can be 1-10 characters. They should be in uppercase and can include letters and numbers. User IDs cannot include spaces between characters.

6. Enter information about the new user ID:

- **Service tools user ID name:** The name of the new service tools user ID.
- **Password:** This password is used by the new user ID. The password must be at least 1 character in length. If you use DES (Data Encryption Standard) encryption or default password level, the maximum password allowed is 8 digits. If you use SHA (Secure Hash Algorithm) encryption or password level 2, then 128-digit case-sensitive passwords are allowed.
- **Set password to expire:** By default, the value for this field is set to 1 (Yes).
- **Description:** This is an optional field to specify more detailed information about the owner of the user ID, such as name, department, and telephone number.
- **Linked user profile name:** The name of the user profile that links from the current service tools user ID.

Note: The linked user profile name is not required for each service tools user ID. It does not even need to exist at the time it is added to a service tools user ID.

7. After entering all information about the user ID, 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 (Change privilege) to go to the Change Service Tools User ID Privileges display. This display lists all the service tools, to which privileges might be granted. For more details, see the information about changing functional privileges for a service tools user ID using DST.

Related tasks

“Changing the passwords for service tools user IDs using DST” on page 21

To change a service tools user ID password using dedicated service tools (DST), complete these steps.

“Changing the functional privileges for a service tools user ID using DST”

To change the functional privileges for a service tools user ID using dedicated service tools (DST), follow these steps.

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

To change the functional privileges for a service tools user ID using dedicated service tools (DST), follow these steps.

About this task

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

- 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 do not take effect. If you press F9 (Defaults), the functional privileges are reset to the default values.

Changing the description for a service tools user ID using DST:

To change the description for a service tools user ID from dedicated service tools (DST), complete these steps.

About this task

1. Access service tools using DST.
2. Sign on to DST using your service tools user ID and password. When the Use dedicated service tools (DST) display is shown, select option 5 (Work with DST environment) and press Enter. The Work with DST Environment display is shown.
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 is shown.
4. On the Work with 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 name, department, and telephone number of the user ID.

Displaying a service tools user ID using DST:

To display a service tools user ID from dedicated service tools (DST), complete these steps.

About this task

1. Access service tools using DST.
2. Sign on to DST using your service tools user ID and password. When the Use dedicated service tools (DST) display is shown, select option 5 (Work with DST environment) and press Enter. The Work with DST Environment display is shown.
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 is shown.
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 is shown.
5. Press F5 (Display privileges) to view the functional privileges associated with this user ID. The Display Service Tools User Privileges display is shown. This display lists all functional privileges and the status for each user ID. You cannot make changes to the user ID from this display.

| *Displaying service tools user IDs using the DSPSSTUSR command:*

| You can use the Display Service Tools User ID (DSPSSTUSR) command to show a list of service tools user
 | identifiers. By using this command, you can view the detailed information about a specific service tools
 | user ID, including the status and privileges of that user ID.

| **About this task**

| **Note:** To use this command, you must have either security administrator (*SECADM) or audit (*AUDIT)
 | special authorities.

- | 1. On the command line, enter DSPSSTUSR USRID (*ALL). The Display Service Tools User ID display is
 | shown.

2. Press F17 (Top) or F18 (Bottom) to scroll to either the top or bottom of the service tools user IDs information.
3. Type 5 (Display) in the Option field from this display to view the functional privileges associated with this user ID. The Display Service Tools User ID display is shown. This display lists all the service tools user IDs and some basic information. It also lists all the functional privileges and the status for each user ID.
4. To go to the Display linked user profile display, press F15 (Display linked user profile). This display lists all the service tools to which privileges might be granted. See “Linking service tools user IDs to user profiles” on page 13 for more information. You can only use the F15 function key when a linked user profile exists.

Example

The following example shows how to display the basic information of a service user tools ID. This command shows the status and privileges of the service tools user ID named 11111111:

```
DSPSSTUSR USRID(11111111)
```

The following example shows how to print all service tools user identities. This command is used to print the status and privileges of all service tools user IDs:

```
DSPSSTUSR USRID(*ALL) OUTPUT(*PRINT)
```

Related information

Display Service Tools User ID (DSPSSTUSR) command

Enabling a service tools user ID using DST:

To enable a service tools user ID from dedicated service tools (DST), complete these steps.

About this task

1. Access service tools using DST.
2. Sign on to DST using your service tools user ID and password. When the Use dedicated service tools (DST) display is shown, select option 5 (Work with DST environment) and press Enter. The Work with DST Environment display is shown.
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 is shown.
4. On the Work with 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 is shown.
5. Press Enter to confirm your choice and the service tools user ID you selected is enabled.

Disabling a service tools user ID using DST:

To disable a service tools user ID from dedicated service tools (DST), complete these steps.

1. Access service tools using DST.
2. Sign on to DST using your service tools user ID and password. When the Use dedicated service tools (DST) display is shown, select option 5 (Work with DST environment) and press Enter. The Work with DST Environment display is shown.
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 is shown.
4. On the Work with 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 is shown.
5. Press Enter to confirm your choice and the service tools user ID you selected is disabled.

Deleting a service tools user ID using DST:

To delete a service tools user ID from dedicated service tools (DST), complete these steps.

About this task

Note: IBM-supplied service tools user IDs cannot be deleted.

1. Access service tools using DST.
2. Sign on to DST using your service tools user ID and password. When the Use dedicated service tools (DST) display is shown, select option 5 (Work with DST environment) and press Enter. The Work with DST Environment display is shown.
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 is shown.
4. On the Work with 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 is shown.
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 IDs display.

Managing service tools user IDs using SST:

You can use system service tools (SST) to create, change, display, enable, disable, and delete service tools user IDs.

Related tasks

“Changing service tools user IDs and passwords using SST” on page 22

To change a service tools user ID password using system service tools (SST), complete these steps.

Creating a service tools user ID using SST:

To create a service tools user ID from system service tools (SST), complete these steps.

About this task

1. Accessing service tools using SST.
2. Sign on to SST using your service tools user ID and password.
3. When the System Service Tools (SST) main menu is shown, 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 service tools user ID in the field provided and press Enter. The Create Service Tools User ID display is shown.

Note: User IDs can be from 1-10 characters. They should be in uppercase and can include letters and numbers. User IDs cannot include spaces between characters.

6. Enter information about the new user ID:
 - **Service tools user ID name:** The name of the new service tools user ID.
 - **Password:** This password is used by the new user ID. The password must be at least 1 character in length. If you use DES encryption (or the default password level), the maximum password allowed is 8 digits. If you use SHA encryption (or password level 2), 128-digit case-sensitive passwords are allowed.
 - **Password is set expired:** Whether the password is set to expire on a particular date.
 - **Description:** This is an optional field where you specify 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 is 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.

Related tasks

“Changing service tools user IDs and passwords using SST” on page 22

To change a service tools user ID password using system service tools (SST), complete these steps.

“Changing the functional privileges for a service tools user ID using SST”

To change the functional privileges for a service tools user ID from system service tools (SST), complete these steps.

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

To change the functional privileges for a service tools user ID from system service tools (SST), complete these steps.

1. Access service tools using SST.
2. Sign on to SST using your service tools user ID and password. When the System Service Tools (SST) main menu is shown, 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 is shown.
 - 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 do not take effect. If you press F9 (Defaults), the functional privileges are reset to the default values.

Related tasks

“Creating a service tools user ID using SST” on page 18

To create a service tools user ID from system service tools (SST), complete these steps.

Changing the description for a service tools user ID using SST:

To change the description for a service tools user ID from system service tools (SST), complete these steps.

1. Accessing service tools using SST.
2. Sign on to SST using your service tools user ID and password. From the System Service Tools (SST) main menu, 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. From 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.

Displaying a service tools user ID using SST:

To display a service tools user ID from system service tools (SST), complete these steps.

About this task

1. Accessing service tools using SST.

2. Sign on to SST using your service tools user ID and password. When the System Service Tools (SST) main menu is shown, 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 is shown. 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
 - Date password expires, or none if password level 1 (Data Encryption Standard) is used
 - Password is 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 is shown. This display lists all functional privileges and the user's status for each. You cannot make changes to the user ID from this display.

Enabling a service tools user ID using SST:

To enable a service tools user ID from system service tools (SST), complete these steps.

About this task

1. Accessing service tools using 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.

Disabling a service tools user ID using SST:

To disable a service tools user ID from system service tools (SST), complete these steps.

About this task

1. Accessing service tools using 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.

Deleting a service tools user ID using SST:

To delete a service tools user ID from system service tools (SST), complete these steps.

About this task

Note: IBM-supplied service tools user IDs cannot be deleted.

1. Accessing service tools using 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.

Changing passwords for service tools user IDs

You have various ways to change the passwords for service tools user IDs. You can use dedicated service tools (DST), system service tools (SST), or the Change Service Tools User ID (QSYCHGDS) API.

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 security officer profiles and all security service tools user IDs, you might need to install and initialize your system from the distribution media to recover them. For this reason, it is suggested that you create multiple profiles and user IDs. Contact your service provider for assistance.

Related concepts

“Recovering or resetting QSECOFR passwords” on page 23

Both a QSECOFR user profile and a QSECOFR service tools user ID are supplied with IBM systems. When you lose your QSECOFR user profile password or your QSECOFR service tools user ID, use one of the passwords to reset the other.

Related reference

“Managing service tools user IDs using DST and SST” on page 13

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

“Recommendations for managing service tools user IDs” on page 14

Here are the recommendations to ensure the security of your service tools user IDs.

Changing the passwords for service tools user IDs using DST:

To change a service tools user ID password using dedicated service tools (DST), complete these steps.

About this task

1. Access service tools using 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 is shown. 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 is shown. 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. The default previous password remembered is 18. Option 10 (Duplicate password control) can be used to change the value from 0 to 32.
 - **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. Refer to the information about password policies for service tools user IDs and make sure that you comply with these password policies when choosing a service tools user ID password. The maximum length allowed for the password is 8 digits if you use Data Encryption Standard (DES) encryption and 128 digits if you use Secure Hash Algorithm (SHA) encryption.

Related tasks

“Creating a service tools user ID using DST” on page 14

To create a service tools user ID using dedicated service tools (DST), follow these steps.

Related reference

“Password policies for service tools user IDs” on page 5

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

Changing service tools user IDs and passwords using SST:

To change a service tools user ID password using system service tools (SST), complete these steps.

About this task

1. Accessing service tools using 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. The minimum required for the password is 1 digit (same as creating a password). The maximum length allowed for the password is 8 digits if you use Data Encryption Standard (DES) encryption and 128 digits if you use Secure Hash Algorithm (SHA) encryption.
 - **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

“Creating a service tools user ID using SST” on page 18

To create a service tools user ID from system service tools (SST), complete these steps.

Related reference

“Managing service tools user IDs using SST” on page 18

You can use system service tools (SST) to create, change, display, enable, disable, and delete service tools user IDs.

“Password policies for service tools user IDs” on page 5

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

Changing service tools user IDs and passwords using the QSYCHGDS API:

You can use the Change Service Tools User ID (QSYCHGDS) API to change your service tools user ID and password or to change the service tools user ID and password for another user if you have sufficient privileges.

The QSYCHGDS API can also be useful if you have several systems and you need to manage service tools user IDs across all of those systems.

Related information

Change Service Tools User ID (QSYCHGDS) API

Recovering or resetting QSECOFR passwords

Both a QSECOFR user profile and a QSECOFR service tools user ID are supplied with IBM systems.

When you lose your QSECOFR user profile password or your QSECOFR service tools user ID, use one of the passwords to reset the other.

Your QSECOFR service tools user ID can have a different password from your QSECOFR user profile. Service tools user IDs have different password policies from user profiles.

It is suggested 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

“Changing passwords for service tools user IDs” on page 21

You have various ways to change the passwords for service tools user IDs. You can use dedicated service tools (DST), system service tools (SST), or the Change Service Tools User ID (QSYCHGDS) API.

“Recommendations for managing service tools user IDs” on page 14

Here are the recommendations to ensure the security of your service tools user IDs.

“Password policies for service tools user IDs” on page 5

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

“Troubleshooting service tools user IDs and passwords” on page 35

When you have problems with service tools user IDs and passwords, refer to this information for solutions.

Resetting the QSECOFR user profile password:

If you know the password for the QSECOFR service tools user ID, use this password to reset the QSECOFR user profile to its initial value (QSECOFR).

About this task

This procedure requires you to perform an initial program load (IPL) on your system. The change does not take effect until after the IPL. To reset the QSECOFR user profile, complete the following steps:

1. Access service tools using 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. From the Work with DST Environment menu, select option 6 (Work with Service Tools Security Data). The Work with Service Tools Security Data menu is shown.
5. Select option 1 (Reset operating system default password). The Confirm Reset of System Default Password display is displayed.
6. Press Enter to confirm the reset. A confirmation message is displayed 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 is displayed.
9. Select option 1 (Perform an IPL). The system continues with a manual IPL.
10. When the IPL completes, return the keylock switch or electronic keystick to the Auto position, if applicable.
11. Sign on to the system as QSECOFR. Use the CHGPWD command to change the QSECOFR password to a new value. Store the new value in a safe place.

Results

Attention: Do not leave the QSECOFR password set to the default. This is a security exposure because this is the value included in every system and is commonly known.

Resetting the QSECOFR service tools user ID and password:

If you know the password for the QSECOFR user profile, use this password to reset the password for the IBM-supplied service tools user ID that has service tools security authority (QSECOFR) to the IBM-supplied default value.

About this task

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

1. Ensure that the system is in normal operating mode, not DST.
2. Sign on at a workstation using the QSECOFR 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.

Results

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 system and is commonly known.

Saving and restoring service tools security data

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

Saving service tools security data:

To save service tools security data using dedicated service tools (DST), complete these steps.

About this task

1. From the Work with DST Environment menu, select option 6 (Service tools security data).
2. From the Work with Service Tools Security Data menu, select option 5 (Save service tools security data). The Save Service Tools Security Data menu is shown.
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 menu is displayed.
 - b. You can select, deselect, or display details on any of the tape devices that are displayed. 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 are displayed. Enter the appropriate value in the Option field next to the optical device, to which you want to save the security data.

Restoring service tools security data:

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

About this task

1. From the Work with DST Environment display, select option 6 (Service tools security data).
2. From the Work with Service Tools Security Data menu, 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.

Enabling working with device IDs from SST

To enable working with device IDs from SST, follow these steps.

1. Access service tools using DST.
2. From the DST Sign-On display, enter the QSECOFR service tools user ID and password.
3. From the Use DST menu, select option 5 (Work with DST environment).
4. From the Work with DST Environment menu, select option 6 (Work with Service Tools Security Data).
5. From the Service Tools Security Data menu, select option 7 (Work with lock for device IDs from SST) and press Enter until the status says Enabled.

Note: This option enables or disables the ability of the service tool security user to change the device IDs from SST. The default is disabled, which means that the device IDs can only be changed from DST.

6. Continue pressing F3 (Exit) to return to the Exit DST menu.
7. Select option 1 (Exit DST).

Related tasks

“Resetting service tools device IDs passwords using SST” on page 31

To reset a service tools device ID password using system service tools (SST), complete these steps.

Managing service tools device IDs

Device IDs are only used for LAN console. Each connecting LAN console requires its own device ID. The IBM-supplied device ID is QCONSOLE and is supplied with a default password of QCONSOLE. You can create a maximum of 50 service tools device IDs (including the IBM-supplied device ID).

Related tasks

“Accessing service tools using SST” on page 7

If your user profile has the required authorizations, you can use system service tools (SST) to access service tools.

Managing service tools device IDs using DST and SST

You can create, display, change, and delete service tools device IDs from dedicated service tools (DST) or system service tools (SST).

Managing service tools device IDs using DST:

You can use dedicated service tools (DST) to create, display, and enable service tools device IDs. You can also use DST to change the attributes and description for a service tools device ID.

Creating a service tools device ID using DST:

To create a service tools device ID using dedicated device tools (DST), follow these steps.

1. Access service tools using DST.
2. Sign on to DST using your service tools user ID and password.
3. From the Use dedicated service tools (DST) display, select option 5 (Work with DST environment) and press Enter.
4. From the Work with DST Environment display, select option 5 (Service tools device IDs) to work with service tools device IDs.

5. From the Work with Service Tools device IDs display, type 1 (Create), type the new service tools device ID in the field provided, and press Enter.

Note: Device IDs can be 1-10 characters. They should be in uppercase and can include letters and numbers. Device IDs cannot include spaces.

6. Enter information about the new device ID, such as the service tools device ID and description.

7. After entering all information about the device ID, you can choose one of these options:

- To create the device ID with the default attributes, press Enter.
- To change the default attributes, press F5 (Change attributes) to go to the Change Service Tools device ID Attributes display. This display lists all the attributes that might be granted.

Related tasks

“Changing the attributes for a service tools device ID using DST”

To change the attributes for a service tools device ID using dedicated service tools (DST), follow these steps.

Changing the attributes for a service tools device ID using DST:

To change the attributes for a service tools device ID using dedicated service tools (DST), follow these steps.

1. Access service tools using DST.
2. Sign on to DST using your service tools user ID and password.
3. From the Use dedicated service tools (DST) display, select option 5 (Work with DST environment) and press Enter.
4. From the Work with DST Environment display, select option 5 (Service tools device IDs) to work with service tools device IDs.
5. From the Work with Service Tools device IDs display, select the device ID to change and type 7 (Change attributes) in the Option field. The Change Service Tools Device Attributes display is shown.
 - Type 1 (Revoke) in the Option field next to the attributes you want to remove from the device ID.
 - Type 2 (Grant) in the Option field next to the attributes you want to add to the device ID.

Note: Only the following two attributes are available for 5xx models and secondary partitions on 8xx models.

- **Operations Console (LAN):** This attribute allows the device ID to be used as the system console.
- **Partition remote panel:** This attribute allows the device ID to start a remote control panel for the system.

For the primary partition of 8xx models that have partitions, the remote control panel attribute can be granted or revoked for each partition, and the remote console for Linux[®] partitions can be granted or revoked.

6. Press Enter to enable these changes. If you press F3 (Exit) before pressing Enter, the changes do not take effect. If you press F9 (Defaults), the attributes are reset to the default values.

Changing the description for a service tools device ID using DST:

To change the description for a service tools device ID from dedicated service tools (DST), complete these steps.

About this task

1. Access service tools using DST.
2. Sign on to DST using your service tools user ID and password. From the Use dedicated service tools (DST) display, select option 5 (Work with DST environment) and press Enter.

3. From the Work with DST Environment display, select option 5 (Service tools device IDs) to work with service tools device IDs.
4. From the Work with Service Tools Device IDs display, select the device ID description to change and type 8 (Change description) in the Option field.
5. In the Description field, enter a new description for the device ID. This might include the name, department, and telephone number of the device ID.

Displaying a service tools device ID using DST:

To display a service tools device ID from dedicated service tools (DST), complete these steps.

1. Access service tools using DST.
2. Sign on to DST using your service tools user ID and password. From the Use dedicated service tools (DST) display, select option 5 (Work with DST environment) and press Enter.
3. From the Work with DST Environment display, select option 5 (Service tools device IDs) to work with service tools device IDs.
4. From the Work with Service Tools Device IDs display, select the device ID you want to display and type 4 (Display) in the Option field. The Display Service Tools Device ID display is shown. This display shows information that relates to the device ID.
5. Press F5 (Display attributes) to view the attributes that are associated with this device ID. The Display Service Tools Device Attributes display is shown. This display lists all the attributes and the status for each device ID. You cannot make changes to the device ID from this display.

Enabling a service tools device ID using DST:

To enable a service tools device ID from dedicated service tools (DST), complete these steps.

About this task

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

Managing service tools device IDs using SST:

You can use system service tools (SST) to create, change, display, enable, disable, and delete service tools device IDs.

Creating a service tools device ID using SST:

To create a service tools device ID from system service tools (SST), complete these steps.

1. Accessing service tools using SST.
2. Sign on to SST using your service tools user ID and password.
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 2 (Service tools device IDs).

5. From the Service Tools Device IDs display, type 1 (Create), type the service tools device ID in the field provided, and press Enter. The Create Service Tools Device ID display is shown.

Note: The device IDs can be 1-10 characters. They should be in uppercase and can include letters and numbers. Device IDs cannot include spaces.

6. Enter information about the new device ID, such as the service tools device ID name and description.

7. After all information about the device ID is entered, select one of these options:

- To create the device ID with the default attributes, press Enter.
- To change the default attributes, press F5 (Change attributes). The Change Service Tools Device ID Attributes display is shown, where all the attributes that might be granted are listed.

Changing the attributes for a service tools device ID using SST:

To change the attributes for a service tools device ID from system service tools (SST), complete these steps.

1. Accessing service tools using SST.

2. Sign on to SST using your service tools user ID and password. From the System Service Tools (SST) main menu, 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 2 (Service tools device IDs).

4. From the Service Tools Device IDs display, select the device ID to change and type 7 (Change attributes) in the Option field. The Change Service Tools Device Attribute display is shown.

- Type 1 (Revoke) in the Option field next to the attributes you want to remove from the device ID.
- Type 2 (Grant) in the Option field next to the attributes you want to add to the device ID.

Note: Only the following two attributes are available for 5xx models and secondary partitions on 8xx models.

– **Operations Console (LAN):** This attribute allows the device ID to be used as the system console.

– **Partition remote panel:** This attribute allows the device ID to start a remote control panel for the system.

For the primary partition of 8xx models that have partitions, the remote control panel attribute can be granted or revoked for each partition, and the remote console for Linux partitions can be granted or revoked.

5. Press Enter to enable these changes. If you press F3 (Exit) before pressing Enter, the changes do not take effect. If you press F9 (Defaults), the attributes are reset to the default values.

Changing the description for a service tools user ID using SST:

To change the description for a service tools user ID from system service tools (SST), complete these steps.

1. Accessing service tools using SST.

2. Sign on to SST using your service tools user ID and password. From the System Service Tools (SST) main menu, 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 2 (Service tools device IDs).

4. From the Service Tools Device IDs display, select the device ID description to change and type 8 (Change description) in the Option field.

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

| *Displaying a service tools device ID using SST:*

| To display a service tools device ID from system service tools (SST), complete these steps.

- | 1. Accessing service tools using SST.
- | 2. Sign on to SST using your service tools user ID and password. From the System Service Tools (SST) main menu, 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 2 (Service tools device IDs).
- | 4. From the Service Tools Device IDs display, select the device ID you want to display and type 4 (Display) in the Option field. The Display Service Tools Device ID display is shown. This display shows the information that relates to the device ID.
- | 5. Press F5 (Display attributes) to view the attributes that are associated with this device ID. The Display Service Tools Device Attributes display is shown. This display lists all the attributes and the status for each user. You cannot make changes to the device ID from this display.

| *Enabling a service tools device ID using SST:*

| To enable a service tools device ID from system service tools (SST), complete these steps.

- | 1. Accessing service tools using SST.
- | 2. Sign on to SST using your service tools user ID and password. From the System Service Tools (SST) main menu, 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 2 (Service tools device IDs).
- | 4. From the Service Tools Device IDs display, select the device ID you want to disable and type 5 (Enable) in the Option field. The Enable Service Tools Device ID display is shown.
- | 5. Press Enter to confirm your choice to enable the service tools device ID you selected.

| *Disabling a service tools device ID using SST:*

| To disable a service tools device ID from system service tools (SST), complete these steps.

- | 1. Accessing service tools using SST.
- | 2. Sign on to SST using your service tools user ID and password. From the System Service Tools (SST) main menu, 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 2 (Service tools device IDs).
- | 4. From the Service Tools Device IDs display, select the device ID you want to disable and type 6 (Disable) in the Option field. The Disable Service Tools Device ID display is shown.
- | 5. Press Enter to confirm your choice to disable the service tools device ID you selected.

| *Deleting a service tools device ID using SST:*

| To delete a service tools device ID from system service tools (SST), complete these steps.

| **About this task**

| **Note:** IBM-supplied service tools device IDs cannot be deleted.

- | 1. Accessing service tools using SST.
- | 2. Sign on to SST using your service tools user ID and password. From the System Service Tools (SST) main menu, 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 2 (Service tools device IDs).

4. From the Service Tools Device IDs display, select the device ID you want to delete and type 3 (Delete) in the Option field. The Delete Service Tools Device ID display is shown.
5. You are prompted for confirmation of your choice to delete the device ID.
 - Press Enter to delete the device ID.
 - Press F12 (Cancel) to cancel the action and return to the Work with Service Tools User ID and Devices display.

Resetting passwords for service tools device IDs

You can use dedicated service tools (DST) or system service tools (SST) to reset the passwords for service tools device IDs. You can reset the QCONSOLE device profile password from the control panel.

Resetting the passwords for service tools device IDs using DST:

To reset a service tools device ID password using dedicated service tools (DST), complete these steps.

1. Access service tools using DST.
2. Sign on to DST using your service tools user ID and password.
3. From the Use dedicated service tools (DST) display, select option 5 (Work with DST environment) and press Enter.
4. From the Work with DST Environment display, select option 5 (Service tools device IDs) to work with service tools device IDs.
5. From the Work with Service Tools Device ID display, select the device ID to change and type 2 (Reset password) in the Option field. The Reset Service Tools Device Password display is shown.
6. Press Enter to confirm the reset operation.

Resetting service tools device IDs passwords using SST:

To reset a service tools device ID password using system service tools (SST), complete these steps.

1. Accessing service tools using SST.
 2. Sign on to SST using a service tools user ID and password that has the service tool security privilege.
 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 2 (Service tools device IDs).
 5. From the Service Tools Device IDs display, select the device ID to change and type 2 (Reset password) in the Option field.
- Note:** If you get a message that says Work with device IDs from SST disabled, you need to enable working with device IDs from SST.
6. From the Reset Service Tools Device Password display, verify that this is the device ID name you want to reset.
 7. Press Enter to confirm the reset operation.

Related tasks

- “Enabling working with device IDs from SST” on page 26
- To enable working with device IDs from SST, follow these steps.

Resetting the QCONSOLE device profile password from the control panel:

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

| **About this task**

| To reset the service tools device ID password using the control panel or remote control panel, follow
| these steps:

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

| **Note:** If the system shows 65 FF, repeat steps 2 and 3 again.

- | 4. Using the Down button, decrement the data to display 65, and then press Enter. The system shows 65
| 00.

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

- | 5. Using the Down button, decrement the data to display 13, and then press Enter. The system shows
| ...0001 and continues to increment as you perform each function 65.
- | 6. Repeat steps 4 and 5 so that you have entered seven function 65s. You have five minutes to complete
| this task. When the seventh 65 is entered and if it is found that more than five minutes have elapsed,
| the reset operation is not processed and the count returns to zero. Use the following information to
| help determine your progress and success of the reset: The double-row display control panel presents
| data like this:

| xxxxxxxxxxxxxxxx
| xxxxxxxxxxxxxxxx

| Each word is 8 characters but four words are displayed at a time for words 12 through 19. For
| example, requesting word 12 (function 12) provides:

| word_12word_13
| word_14word_15

| Requesting word 13 (function 13) provides:

| word_16word_17
| word_18word_19

| The remote control panel presents data like this:

| xxxxxxxx

| Each word is 8 characters only and displayed individually. If you want word 17, you have to request
| function 17.

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

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

| **Note:** If you enter function 65 more than seven times, the count starts over.

- | 7. Highlight the connection name and then use one of these methods to start your connection:

- Right-click the connection name and select Connect.
- Click the connection icon in the toolbar.
- Click the connection drop-down menu and select Connect.

Related concepts

“Accessing service tools using DST” on page 6

To access service tools, you can use dedicated service tools (DST) from the system control panel or from a manual initial program load (IPL).

Automatically creating device IDs

The automatic creation of device IDs function is turned on by default with a limit of 10 new device IDs. You can control whether to turn on this function and specify the number of device IDs that can be automatically created. If you do not want to use this function, turn it off.

About this task

To disable or enable automatic creation of device IDs through the dedicated system service tools (DST), follow these steps:

1. Access service tools using DST.
2. Enter the QSECOFR service tools user ID and password on the DST Sign-On display.
3. From the Use DST menu, select option 5 (Work with DST environment).
4. From the Work with DST Environment menu, select option 6 (Work with Service Tools Security Data).
5. From the Work with Service Tools Security Data menu, enter a value of 0 to 49 in the **Autocreate service tools device IDs** field and press Enter.

Note: A value of 0 disables the automatic creation function. The maximum number of device IDs that can be automatically created is 49. The system can manage up to 50 IDs including the default device ID QCONSOLE.

6. Continue pressing F3 (Exit) to return to the Exit DST menu.
7. Select option 1 (Exit DST).

Changing service tools security policies

You can make necessary changes to allow more flexibility for some security policies or rules.

Changing to allow default and expired passwords to be used from SST

You can make changes to allow default and expired service tools passwords to be used from system service tools (SST).

About this task

To allow default and expired service tools passwords to be used from SST, follow these steps:

1. Access service tools using DST.
2. Enter the QSECOFR service tools user ID and password on the DST Sign-On display.
3. Select option 13 (Work with System Security).
4. 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.
5. Press F3 (Exit) to return to the Exit DST menu.
6. Select option 1 (Exit DST).

If the QSECOFR service tools user ID has a non-default password or another service tools user ID with service tools security privilege has a non-default password, then follow these steps:

1. Accessing service tools using SST.

2. Enter the service tools user ID and password on the SST Sign-On display.
3. Select option 7 (Work with system security).
4. 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.
5. Press F3 (Exit) to return to the SST menu.
6. Press F3 (Exit) and then press Enter to exit SST.

Changing the password expiration interval

To change the default password expiration interval from 180 days, follow these steps.

About this task

1. Access service tools using 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. The Work with Service Tools Security Data menu is shown.
5. Enter a number between 0 and 999 on the option 8 line.

Note: 0 means *NOMAX, which means that the password never expires. Be default, when using SHA encryption, the password expires in 180 days.

6. Select option 8 (Password expiration interval in days) and press Enter.
7. Press F3 (Exit) until you return to the Exit DST menu.
8. Select option 1 (Exit DST).

Changing the maximum failed sign-on attempts

To change the default maximum failed sign-on attempts before the user ID is disabled, follow these steps.

About this task

1. Access service tools using 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. The Work with Service Tools Security Data menu is shown.
5. Enter a number between 2 and 99 on the option 9 line.

Note: The default is 3 failed sign-on attempts, at which point the user ID is disabled.

6. Select option 9 (Maximum sign-on attempts allowed) and press Enter.
7. Continue pressing F3 (Exit) to return to the Exit DST menu.
8. Select option 1 (Exit DST).

Changing the duplicate password control

To change the default duplicate password control, complete these steps.

About this task

1. Access service tools using 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. The Work with Service Tools Security Data menu is shown.
5. Enter a number between 0 and 32 on the option 10 line.

Note: 0 means no passwords are remembered and can be reused at any time. The default is 18 passwords remembered before they can be reused.

6. Select option 10 (Duplicate password control) and press Enter.
7. Continue pressing F3 (Exit) to return to the Exit DST menu.
8. Select option 1 (Exit DST).

Troubleshooting service tools user IDs and passwords

When you have problems with service tools user IDs and passwords, refer to this information for solutions.

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 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 dedicated service tools (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. The password cannot be changed from system service tools (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 concepts

“Recovering or resetting QSECOFR passwords” on page 23

Both a QSECOFR user profile and a QSECOFR service tools user ID are supplied with IBM systems. When you lose your QSECOFR user profile password or your QSECOFR service tools user ID, use one of the passwords to reset the other.

“Accessing service tools using DST” on page 6

To access service tools, you can use dedicated service tools (DST) from the system control panel or from a manual initial program load (IPL).

Monitoring service function use

You can monitor the use of service functions through the dedicated service tools (DST) security log or through the i5/OS security audit log. These logs help you trace unusual access patterns or potential security risks.

Related tasks

“Changing the password expiration interval” on page 34

To change the default password expiration interval from 180 days, follow these steps.

Related reference

“Service tools user IDs” on page 3

Service tools user IDs are user IDs that are required for accessing service functions through dedicated service tools (DST), system service tools (SST), System i Navigator (for logical partitions and disk unit management), and Operations Console.

Monitoring service function use through DST

You can use the dedicated service tools (DST) security log to monitor service functions. Any time a user signs on to DST using a service tools user ID, the event is logged by the service tools security log.

About this task

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

1. Access service tools using 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. From the Work with DST Environment display, select option 6 (Work with Service Tools Security Data).
5. From the Work with Service Tools Security Data menu, select option 3 (Work with service tools security log) and press Enter. The Work with Service Tools Security Log display is shown. 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 is shown with the information for the activity you selected.

Monitoring service tools use through security audit log

The security audit log can be used to record the service tools actions by individual user IDs.

About this task

To enable the security audit log to record service tools actions, complete the following steps for each system on which you want to enable the security audit log.

1. From a System i 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 your system.

Results

After the security audit log functions have been enabled, the log information is displayed in the journal receiver. To access the current service tools action entry in the journal receiver, enter the Display Journal (DSPJRN) command on a command line: DSPJRN QSYS/QAUDJRN ENTTYP(ST).

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 Security reference.

Related information for Service tools

Other information center topic collections contain information that relates to the Service tools topic collection. You can view or print any of the PDF files.

Other information

- Disk management
- Licensed Internal Code logs
- Locking and unlocking security-related system values
- Operations Console
- Partitioning with System i
- Planning and setting up system security
- Problem logs
- Security
- Security reference (13400 KB)
- System i Navigator
- Using the Hardware Service Manager
- Working with systems with partitions

Related reference

“PDF file for Service tools” on page 1

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

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 document 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 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:

i5/OS
IBM
IBM(logo)
iSeries
System i

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

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

Terms and conditions

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

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

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

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

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

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

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



Printed in USA