# IBM

@server

iSeries

Basic system security and planning

Version 5 Release 3

IBM

@server

iSeries

Basic system security and planning

Version 5 Release 3

> **Note**
>
> Before using this information and the product it supports, be sure to read the information in "Notices," on page 129.

Contents

      iii

Basic system security and planning

Basic system security and planning provides you with detailed information about planning and setting up your iSeries™ security. This topic emphasizes planning and provides forms which you can use to plan and record your security decisions. It also provides step-by-step set up instructions for your basic system security. Because of the workbook nature of this topic, you may want to print to review the material more thoroughly.

Setting up the best security for your iSeries consists of two major sets of activities: planning tasks and configuration tasks. To ensure that you set up security that meets your business needs, you should review these planning topics:

- Getting started with basic system security provides an overview of general security concepts and answers questions about basic system security.
- Planning user security provides information on how to plan security that affects users on your system. This includes physical security, application security, your overall strategy for security, and user profiles on your system.
- Planning resource security provides information on how to plan the security of objects on your system, including libraries and the objects in them, printers, printer output, and workstations.

After you complete the planning activities, you can review these topics to help you set up security for your system:

- Setting up user security provides details on setting up user and group security.
- Setting up resource security provides information on how to set up ownership to objects, public and specific authority to objects, and security for printers and workstations.
- Testing security provides information on testing your security.
- Changing security information provides information on updating and modifying user and group profiles and resource security.
- Saving security information provides information on backing up security information.
- Monitoring security provides checklists for keeping track of security and information on auditing your security.

In addition to these topics, use the planning forms to document your planning strategies and security decisions.

Print this topic

You can view or download a PDF version of this document for viewing or printing. You must have Adobe® Acrobat® Reader installed to view PDF files. You can download a copy from Adobe home page

To view or download the PDF version, select Basic system security and planning (950 KB or 164 pages).

To save a PDF on your workstation for viewing or printing:
1. Open the PDF in your browser (click the link above).
2. In the menu of your browser, click **File**.
3. Click **Save As...**
4. Navigate to the directory in which you would like to save the PDF.
5. Click **Save**.

Getting started with basic system security

Everyone from system administrators to users should be concerned with security. System security protects the iSeries and your sensitive business information from both intentional and unintentional security breaches.

You can customize your system security, basing it on your security environment and needs.

Think of security as a doorway to your system. You use security features to **lock up** or protect your information from unauthorized use.

You also use security features to **unlock** the flexibility of the system and customize it for each user.

A good security plan can protect your system, but it cannot guarantee the safety of your equipment or your information. You should divide system responsibilities among multiple employees to ensure that no one person has exclusive control over your system.

Basic system security and planning provides you with a step-by-step approach to planning and setting up your basic system security. This topic stresses the importance of planning system security and provides planning forms that you use to record your security decisions. To help you make decisions about security, throughout this topic you will find an example of a business that is planning its security.

To ensure that you accomplish system security successfully, good and thorough planning is essential. Review these topics to learn about basic security needs and the importance of security planning:
* Frequently asked questions about basic system security
* An overview of basic system security
* A method of planning basic system security

You should also have a good plan for backup and recovery of all the information on your system. In addition, you should also plan for replacing your equipment in the event of a disaster. For more information about designing a good backup plan, see the Backup and Recovery topic in the Information Center.

Detailed planning information on user security

The following topics provide techniques for planning user security:
* Planning security for your applications
* Planning your security strategy
* Planning user groups
* Planning individual user profiles

Detailed planning information on resource security

The following topics provide a systematic approach to planning your resource security for your users.
* Understanding types of authority
* Planning security for application libraries
* Determining ownership of libraries and objects
* Grouping objects
* Protecting printer output
* Protecting workstations
* Planning your application installation

Printable planning forms

Basic system security and planning provides printable planning forms which allow you to record all of your security decisions. You can print the entire topic as a PDF, or the individual planning forms by using your browser's print button.

Step-by-step set up instructions for your basic system security

After you complete your security planning, this topic provides steps to put your security plan into affect. The following topics will help you to set up your system security.
- Setting up user security
- Setting up resource security

Frequently asked questions about basic system security

Reviewing the answer to these frequently asked questions about security can help you better understand the importance of security for your system.

Why is security important?

The information stored on your system is one of your most important business assets. Keep three important objectives in mind when you think about how to protect your information assets:
- **Confidentiality:** Good security measures can prevent people from seeing and disclosing confidential information.
- **Integrity:** To some extent, a well-designed security system can ensure the accuracy of the information on your computer. With the right security, you can prevent unauthorized changes or deletions of data.
- **Availability:** If someone accidentally or intentionally damages data on your system, you cannot access those resources until you recover them. A good security system can prevent this kind of damage.

When people think about system security, they usually think about protecting their system from people outside the company, such as business rivals. Actually, protection against curiosity or system accidents by proper users is often the greatest benefit of a well-designed security system. In a system without good security features, a user might unintentionally delete an important file. A well-designed security system helps prevent this type of accident.

Ask yourself these questions as you decide how much security you need on your system:
- How important is your computer (and the data that you store on it) to your business?
- Do you have a company policy that require certain levels of security?
- Do your auditors require a level of security for the information stored on your computer?
- Will you need some degree of security in the foreseeable future?

Why customize your system?

The iSeries covers a wide range of users. A small system might have three to five users that run a few applications. A large system might have thousands of users on a large communications network running many applications.

iSeries design provides lots of flexibility to accommodate a wide range of users and situations. You have the opportunity to change many things about how the system looks to your users and how it performs.

When your system first arrives, you probably will not need or want to do very much customizing. IBM® ships your system with initial settings, called **defaults**, for many options. These defaults are the choices that usually work best for new installations.

Note: All new systems ship with a default security level of **40**. This security level ensures that only users who you have defined can use the system. It also prevents potential integrity or security risks from programs that can circumvent security.

However, if you do some customizing, you can make your system a simpler and more effective tool for your users. For example, you can make sure that a user always gets the correct menu when signing on. You can make sure that every user's reports go to the right printer. Your users will feel that more confident about the system if you do some initial customizing to make it look and feel like their own system.

Who should be responsible?

Different companies take different approaches to security. Sometimes programmers have responsibility for all aspects of security. In other cases, the person who manages the system is also in charge of security. If you are not sure how to assign the responsibility in your company, here is a suggested approach:

- You method of planning resource security depends on whether your company purchases or develops applications. If you develop your own applications, communicate your resource security needs during the development process. If you purchase applications, understand and work with the application designer. In both cases, the people who design applications should consider security as part of the design.
- Setting up security should be the responsibility of a security officer. The security officer defines system users and their access to the system. The security officer is often responsible for other things on your system, such as backup and recovery of information.
- The security officer should also customize your system, since many security elements play an important role in system customization.

No matter what method you use to assign responsibility for security, **communicate a security policy**. An executive in your company should tell everyone, preferably in writing, that the information in your computer is an important asset. You should protect that information, just as you would any other company asset. See "Example: JKL Toy Company's security policy" for an example of a security policy.

Now that you understand the need for security on your system, you may want to review an overview of system security considerations.

An overview of basic system security

To plan effectively, you need to understand how your view of what you want to accomplish relates to the tools the system provides. You need to know how the user and system features work together to help you achieve your objectives.

The following topics introduce the important pieces of security and customizing and show you how they fit together. These topics are intended to give you an overview before you begin planning. All the concepts introduced here are explained in more detail as they are needed in the planning process.

- Built-in system security
- Basic terminology
- The user's view of security
- System tools for security and customizing

Built-in system security

All the pieces of the system side of security are built into the system. They are not a separate product you buy. This integrated approach has several benefits:

- Security is consistent with the rest of the operating system. It uses the same displays, commands, and terminology.
- Users cannot bypass security, because it is not a separate piece of software.
- Properly designed security has minimal affect on performance.
- Security always keeps up with new software developments. When new functions become available, the security for those functions becomes available.

The iSeries ships with a security level of 40, which prevents unauthorized users from signing on to the system. It also prevents potential integrity or security risks from programs that can circumvent security. However, you may customize certain security settings or change security levels. Security levels are described in the topic, "Choosing your security level."

Now that you have a better understanding of how built-in security operates, you may want to familiarize yourself with common iSeries terminology.

Basic terminology

This set of general terminolgy are very important for understanding and understanding iSeries security:

Object
> An object is a named space on the system that can be manipulated. The most common examples of objects are files and programs. Other types of objects include commands, queues, libraries, and folders. Objects on the system are identified by object name, object type, and the library in which the object resides. Each object on the system can be secured.

Library
> A library is a special type of object that is used to group other objects. Many objects on the system reside in a library.

Directory
> A directory is another way to group objects on the system. Objects can reside in a directory. A directory can reside in another directory, forming a hierarchical structure.

Now that you have a better understanding of the general iSeries security terminolgy, you may want to review how a user views security.

The user's view of security

From a user's point of view, security affects how they use and complete tasks on the system. It also includes how they interact with the system to complete those tasks. It is important to consider how a user will view security. For example, setting passwords to expire every five days would frustrate and interfere with a user's ability to complete his or her job. On the other hand, too lax a password policy could cause security problems.

In order to provide the right security for your system, you need to divide security into specific parts that you can plan, manage, and monitor. From a user's point of view, you can divide your system security into several parts:

Physical access to the system

Physical security protects the system unit, all system devices, and backup storage media, such as diskettes, tapes, or CDs from accidental or intentional loss or damage.

Most measures you take to ensure the physical security of your system are external to the system. However, the system ships with a keylock or electronic keystick that prevents unauthorized use of functions at the system unit.

The topic, "Planning physical security," provides detailed information to help you plan the physical security of your system.

How users sign-on

Sign-on security prevents a person who is not identified on the system from signing on. In order to sign on, an individual must enter a valid combination of user ID and password.

You can use both system values and individual user profiles to make sure that your sign-on security is not violated. For example, you can require that passwords be changed on a regular basis. You can also prevent the use of passwords that are easy to guess.

What users are allowed to do

An important role of security, and of system customization, is to define what users can do. From a security perspective, this is often a **limiting** function, such as preventing people from seeing certain information. From a system customizing perspective, this is an **empowering** function. A properly customized system makes it possible for people to do their jobs well by eliminating unnecessary tasks and information.

Some methods for defining what users can do are appropriate for the security officer, while others are the responsibility of programmers. This information focuses primarily on those things that a security officer usually does. You can find descriptions for all system values in Chapter 3, "Security System Values," of

Security-Reference (SC41-5302).

Parameters are available in individual user profiles, job descriptions, and classes to control what the user can do on the system. The list below briefly describes the techniques available:

Limiting users to a few functions
> You can limit users to a specific program, menu or set of menus, and a few system commands based on their user profile. Usually, the security officer creates and controls user profiles.

Restricting system functions
> System functions allow you to save and restore information, manage printer output, and set up new system users. Each user profile specifies which of the most common system functions that the user can perform.
>
> On the iSeries, you perform system functions by using control language (CL) commands and application programming interfaces (APIs). Because every command and API is an object, you can use object authorities to control who can use them and complete system functions.

Determining who can use files and programs
> Resource security provides the capability to control the use of every object on the system. For any object, you can specify who can use it and how they can use it. For example, you can specify that one user can only look at the information in a file; another user can change data in the file; a third user can change the file or delete the entire file.

Preventing abuse of system resources
> The processing power on your system can become just as important to your business as the data that you store on it. The security officer helps to ensure that users do not misuse system resources by running their jobs at a high priority, printing their reports first, or using too much disk storage.

How your system communicates with other computers

Additional security measures may be necessary if your system communicates with other computers or with programmable workstations. If you do not have proper security controls, someone on another computer in your network can start a job or access information on your computer without going through the sign-on process.

You can use both system values and network attributes to control whether you allow remote jobs, remote access of data, or remote PC access on your system. If you allow remote access, you can specify what security to enforce. You can find descriptions for all system values in Chapter 3, "Security System Values,"

of *Security-Reference* (SC41-5302).

How to save your security information

You need to regularly back up the information on your system. In addition to saving the data on your system, you need to save security information. If a disaster occurs, you need to be able to recover information about system users, authorization information, and the information itself.

The topic "Saving security information" explains how to save security information. The Backup and Recovery topic in the Information Center provides more detailed information about backing up and recovering security data.

How to monitor your security plan

The system provides several tools for monitoring security effectiveness:
- Messages are sent to the system operator when certain security violations occur.
- Various security-related transactions can be recorded in a special audit journal.

The topic, "Monitoring security" discusses the use of these tools in general terms. You can find more details on security auditing, in Chapter 9, "Auditing Security on the System," of *Security-Reference*

(SC41-5302).

To better understand how to customize your system, you should understand customization from a user's view.

The user's view of customizing the system: You can customize your system to help your users accomplish their day-to-day work. To best customize your system for your users, think of what they need to accomplish their work successfully. You can customize the system to show menus and applications in the several ways:

Showing users what they want to see

Most of us arrange our desks and our offices so we can easily reach the things that we need most. Think of your users' access to the system in the same way. After signing on the system, a user should first see the menu or display that person uses the most. You can easily design user profiles to make this happen.

Eliminating the unnecessary

Most systems have many different applications on them. Most users only want to see the things they need to do their jobs. Limiting them to a few functions on the system makes their jobs easier. With user profiles, job descriptions, and appropriate menus, you can give each user a specific view of the system.

Sending something to the right place

Users should not have to worry about how to get their reports to the correct printer or how their batch jobs should run. System values, user profiles, and job descriptions do these things.

Providing assistance

No matter how well you succeed in customizing the system, users may still wonder "Where is my report?" or "Has my job run yet?" **Operational Assistant** displays provide a simple interface to system functions, which help users answer these questions. Different versions of system displays, called **assistance levels**, provide help for users with different levels of technical experience. When your system arrives, Operational Assistant displays are automatically available for all users. However, the design of your applications may require you to change the way users get access to the Operational Assistant menu.

The iSeries provides system tools which allow you to customize your system security to protect your resources while allowing users to access those resources.

System tools for security and customizing

To plan effectively, you need to understand how your view of your security goals relates to the tools the system provides. You can use these system tools to customize security on your system.

Security level

IBM ships all new iSeries with a security level of 40. Security level 40 provides password and resource security and system integrity. If you want to change the active level of security on your system, you can change the QSECURITY system value. However, IBM strongly recommends that you leave the security level set to 40. In order to change the security level, a user needs a *SECOFR user class or *ALLOBJ and * SECADM special authorities.

The system offers four levels of security as shown in this table:

Table 1. Security levels available on the system

Security level	Description
Security Level 20	Provides password security only.
Security Level 30	Provides password and resource security.
Security Level 40	Provides password and resource security; integrity security.
Security Level 50	Provides password and resource security; enhanced integrity protection.

The topic "Choosing your security level" provides details on how to determine which security level would best meet your needs.

System values

You can set system values to control how certain features of the operarating system work on your iSeries. Think of system values as company policy. System values apply to everyone using the system, unless something more specific, such as a user profile, overrides the system value.

System values determine such things as the main printer, how the system displays the date, and how often you need to change your password.

Network attributes

Network attributes define some characteristics of how your system communicates with other computers, including personal computers. Network attributes apply to your entire system.

Group profiles

A group profile defines a group of users. Think of group profiles as department policy. You can use group profiles as a pattern for creating individual user profiles. You can also use group profiles to define how the members of the group are allowed to access objects on the system. For more information on group profiles, see the topic "Planning user groups."

User profiles

The user profile is one of the most powerful and versatile objects on the system. It contains things such as the user's password and what menu the user sees after signing on. The user profile defines what a

person can and cannot do on the system. It determines a user's unique view of the system. The topic "Planning user security" discusses tips for planning user profiles.

Job descriptions

A job description works with system values and user profiles to determine the way the system processes a user's jobs. The job description sets up a user's initial library list, which determines the libraries that a user gains access to automatically after signing on.

Resource security

The security officer protects the resources (objects) on the system by determining who has the authority to use them and how user can access these objects. The security officer can set object authorities for individual objects or for groups of objects (authorization lists). Files, programs, and libraries are the most common objects requiring protection, but system security allows you to set object authorities for any object on the system.

You can manage resource security simply and effectively, if you plan a general, straightforward approach in advance. A resource security scheme created without prior planning can become complicated and ineffective. The topic, "Planning resource security" describes ways to plan your resource security.

The system provides several tools to assist you in designing a straightforward resource security scheme:
- **Group profiles:** You can group similar users under a single group profile. Then the user group can all share the same authority to objects.
- **Authorization lists:** You can group objects with similar security needs in one list. Then you can grant authority to the list rather than to the individual objects.
- **Object ownership:** Every object on the system has an owner. Group profiles or individual users can own objects. Proper assignment of object ownership helps you (1) manage applications, and (2) delegate responsibility for the security of your information.
- **Primary group:** You can specify primary group authority for an object. The system stores the primary group authority with the object. The use of primary group authority may simplify your authority management and improve authority checking performance.
- **Library authority:** You can put files and programs that require protection into a library and restrict access to that library. This is often simpler than restricting access to each individual object. To protect critical objects, you may want to secure both the object and the library.
- **Object authority:** In cases where the access to a library is not restrict access to a library is not specific enough, you can restrict authority on individual objects, such as files.
- **Public authority:** For each object, you can define what kind of access is available for any system user who does not have any other authority to the object. Public authority is an effective means for securing objects that are not confidential and provides good system performance.
- **Directory authority:** You can use directory authority in the same way that you use library authority. You can group objects in a directory and secure the directory rather than the individual objects.
- **Authority holder:** When you delete an object, you also delete the authority information for that object. Authority holders maintain the authority information for program-defined files that are deleted and created again by an application. You can use authority holders to assist with migration from the System/36™.

Security tools

You can use security tools to help you manage and monitor the security environment on your iSeries. You can also use user profile tools to help you:
- Find out what user profiles have default passwords.
- Schedule user profiles to be unavailable at certain times of the day or week.

- Schedule a user profile to be removed when the employee leaves.
- Find out which user profiles have special authorities.
- Find out who adopts authority to objects on the system.

You can the object security tools to track the public and private authorities that are associated with confidential objects. You can print these reports regularly (monthly, for example) to help you focus your security efforts on current issues. You can run reports to display only the changes since the last time you ran the report.

Other tools provide the ability to monitor:

- Trigger programs
- Security-relevant values in communications entries, subsystem descriptions, output queues, job queues, and job descriptions.
- Altered or tampered programs

Now that you understand the importance of system security, you may to review a description of the planning method that this topic uses as an example.

A method of planning basic system security

These planning topics in this topic approach planning by moving from the outside to the inside and from the general to the specific. For example, to plan user profiles, you need to first think about what the user should see (the outside) and then decide how to make that happen (the inside). You plan system values and group profiles first (the general), and then decide on exceptions for individual users (the specific).The planning steps in the topic Planning user security are designed to be completed in order. They provide a logical progression for describing how you plan to use your system and for deciding how to secure and customize it.

When planning and designing system security, you build from the ground up, beginning with the most basic forms of security and then building to more complex security issues. Begin with the physical security of your system, moving to describing your applications and system values. Finally, you need to consider the security for the users and the objects on your system.

Throughout these planning topics, we have provided examples of this approach using a scenario company, JKL Toys. The topic, "JKL Toy Company: Introducing the example company" describes the sample company that is used throughout the planning topics.

See the topic, "Steps in the planning process" for brief descriptions of each step and how each step relates to one another.

Example: Introducing the JKL Toy Company

Examples make things easier to explain and easier to understand. With that in mind, this topics uses the JKL Toy Company as an example. The JKL Toy Company, a small, but rapidly growing, toy manufacturer, wants to set up security on an iSeries system. The company president, John Smith, wants his new iSeries system to ease the burden JKL Toy Company's explosive growth.

John gave Sharon Jones, the accounting manager, the responsibility of system administrator and security officer. She needs to make sure the entire installation, including security, goes smoothly. Sharon believes in the importance of planning. Today the company is small, and most of its employees have access to most information. But Sharon knows that this will change as the company grows. She is anxious to do things correctly the first time.

Initially, JKL Toy Company plans to run the following applications on its system: Customer Orders, Inventory Control, Contracts and Pricing, and Accounts Receivable. As you read the planning topics, you will learn more about how the JKL Toy Company handles security.

The topic "Steps in the planning process" explains each of the steps that you need to follow when you plan your system security.

Steps in the security planning process

The following chart describes each step in the planning process and how that step relates to the rest of the process.

Table 2. Steps in the security planning process

Step	What you do in this step	How this step relates to each other
Planning physical security	Describe how you plan to protect the system unit, devices, and backup media.	Most of this information is independent of the rest of the process. You do not enter physical security planning information into the system; however, you need some of this information to plan system values and resource security.
Planning your application	Describe the purpose, main menus, and libraries of all your applications.	Provides the basis for the rest of the planning process and your other security decisions. You do not enter this information into the system.
Planning your overall approach	Decide what your overall approach will be to security. Choose system values that support that approach.	Use your application planning information to help determine your overall approach. The system values that you choose affect how you plan user and group profiles.
Planning user groups	Decide how to divide your users into groups. Decide what characteristics each group has and how to define them on the system.	Use your application description to determine groups on the system. The user groups you define affect how you plan individual users on your system.
Planning individual user profiles	Assign each system user to a group. Define each user, including characteristics that differ from the rest of the group. For example, the users needs different access to an application or library than the rest of the group.	Use application planning and user group planning information to help define individual users.
Planning resource security	Decide which applications should be available to everyone on your system. If you need to restrict certain applications, decide which users or groups should be allowed to use them.	Use application planning and group profile planning information to help plan resource security.
Planning your application installation	Decide how to establish ownership and public authority to your application libraries.	Use resource security planning information to plan your application installation.

You should begin the security planning process by planning user security.

Planning user security

Planning user security includes planning all areas where security affects the users on your system. It is essential that you describe the following areas:

Physical security

Physical security includes the protection of your iSeries from accidental (or intentional) damage

and theft. In addition it includes all of your workstations, printers, and storage media. "Planning physical security" contains more information on planning physical security, risks, and IBM recommendations.

Application security

Application security deals with what applications you store on your system and how you will protect those applications while simultaneously allowing users access to them. "Planning security for your applications" provides details on describing your applications and their naming conventions.

Overall security strategy

Planning your overall security includes developing a security plan which considers both your present situation and future plans for your business. "Planning your overall security strategy" provides more information on determining your security policies, security level, password considerations, and system values.

User group security

A user group is a group of users who need to use the same applications in the same way. Planning user group security involves determining the work groups who plan to use the system and the application needs of those groups. "Planning user groups" provides detailed information about identifying user groups, planning group profiles, choosing system values, and determining the user's environment.

Individual user security

After you have determined what user groups you need, you can plan the individual user profiles that you need. "Planning individual user profiles" provides more information on naming users on the system, determining responsibilities of individual users, and choosing system values.

You will find links throughout these planning topics to planning forms that you can use to record your planning decisions.

Planning physical security

When you prepare to install your iSeries, you should create a physical security plan by asking these questions:

- Where will you put the system unit?
- Where will you locate each display station?
- Where will you locate printers?
- What additional equipment do you need, such as wiring, telephone lines, furniture, or storage areas?
- What measures will you take to protect your system from emergencies such as fire or power interruptions?

Physical security should be part of your overall security planning. You may need special measures to protect them depending on where you put the system and its devices.

You can use the Physical Security Planning form to record your decisions about the physical security of your system. To ensure that you cover all aspects of physical security, review these topics:

- Physical security for the system unit provides details about securing the system itself.
- Physical security for system documentation and storage media contains information on securing system documents and your storage media.
- Physical security for workstations discusses ways to secure workstations.
- Physical security for printers and printer output provides details on physically protecting printers and their output.
- Planning your security policy explains how to prepare a user guidelines and a security policy.

Each system unit has a control panel for servicing the machine and performing special system operations, such as powering the system on and off. To prevent unauthorized use of these system operations, each system unit has either a keylock switch or an electronic keystick. They provide some protection of your system unit, but the keylock switch or the electronic keystick are not replacements for adequate physical security.

Physical security for the system unit

The iSeries does not require a computer room with special environmental controls. Often you will find the system unit in the middle of an office area where many people have access to it. Customers like the small size and easy maintenance of the iSeries; however, these features could also pose security risks. For example, one person could easily steal the system unit or remove valuable components from it.

You should take measures to make sure that your system unit is in a safe place. The best location is in a private, locked room. At the very least, the system unit should be in a place that can be locked outside of regular business hours.

Risks to the system unit

In addition to theft of the system unit or its components, here are some other risks posed by inadequate physical security of your system unit:

Unintentional disruption of system operations
> Many security problems come from authorized system users. Suppose that one of the display stations on your system gets locked up. The system operator is away at a meeting. The frustrated display station user walks over to the system unit, thinking that, "Maybe if I press this button, it will correct things." That button may turn off or reload the system while many jobs are running. You may need several hours to recover partially updated files. You can use the system unit keylock switch to prevent this.

The use of dedicated service tools (DST) function to circumvent security
> Security does not control service functions the system performs, because your system software may not be operating properly when you need to perform these functions. A knowledgeable person who knows or guesses the Service Tools user ID and password could cause considerable damage to your system. To learn more about Sevice Tools, see the Service Tools topic in the Information Center.

Recommendations
- Ideally, keep your system unit in a locked room. If can not do this, place your unit where outsiders cannot access it. In addition choose a location where responsible employees can monitor it. The following physical security features can help you protect your system from accidental or intentional tampering:
- Use the electronic keystick or the keylock:
  - Set the operating mode to Normal if you want to be able to start your system without using the key.
  - Set the operating mode to Auto if you plan to use the Automatic Power On/Off function to start and stop your system.
  - Remove the key and put it in a safe place.
- Change the Service Tools (DST) user ID and password immediately after you install your system and after service personnel use it. The topic Service Tools in the Information Center explains how to do this in more detail.

You may want to see an example of JKL Toy Company's plan for unit security before you plan physical security for system documentation and storage media.

Example: JKL Toy Company's physical security planning form—system unit portion: Below is an example of the system unit portion of the Physical Security Planning form that Sharon Jones used for her system:

Table 3. JKL Toy Company's Physical Security Planning Form: System unit example

Physical Security Planning Form	
Prepared by: Sharon Jones	Date: 9/2/99
System Unit:	
Describe your security measures to protect the system unit (such as a locked room):	The system unit is in the accounting area. During the day, accounting people are always in the area and can watch the system unit. The accounting people are also responsible for petty cash and important records. Outside of regular business hours, the area is locked.
What keylock position is normally used?	Normal
Where is the key kept?	Small safe in Sharon's office.
Other comments relating to the system unit:	System unit will be easily accessible. Mention to the people in the accounting area that they should make sure people do not tamper with it.

After you plan your system unit's physical security, you can plan physical security for system documentation and storage media.

Physical security for system documentation and storage media

Another aspect of your physical security plan deals with the storage of important system documentation and storage media. System documentation includes information that IBM sends with the system, password information, your planning forms, and any reports that the system generates.

Depending on your system, backup media can include tapes, CD-ROMs, diskettes, or DVD storage. You should store both system documentation and backup media at your business location as well as at another remote location. In case of a disaster, you will need this information to recover your system. The following information suggests ways to store your system documentation and storage media. After you have decided on your method, record your choices on the Backup Media and Documentation section of the Physical Security Planning form.

Storing system documentation securely

Service tools and security officer passwords are critical to the operation of your system. You should write these passwords down and store them in a safe, confidential location. In addition, keep a copy of these passwords at an offsite location to help you recover from a disaster.

Consider storing other important system documentation, such configuration settings and your main application libraries, away from your business location to help you recover from a disaster.

Storing your storage media securely

When you install your system, make plans for regularly saving all the information on the system to tape or other storage media. These backups allow you to recover your system if necessary. You should keep these backups in a secure location offsite as well.

Risks

- Damage to backup media: If a disaster or vandals destroyed your system backup media, you could not recover the information that was on your system, except from printed reports.
- Theft of backup media or passwords: You may have confidential business information saved on your backup media. A knowledgeable person might be able to restore this information to another computer and print or process it.

Recommendations

- Store all passwords and backup media in a locked, fireproof cabinet.
- Take copies of your backup media to a secure, off-site location on a regular basis, for example at least weekly.

You may want to review an example of JKL Toy Company's plan for storage of system documentation before you plan physical security for your workstations.

Example: JKL Toy Company's physical security planning form—backup media and documentation portion: Sharon Jones of the JKL Toy Company completed the Backup Media and Documentation section of the Physical Security Planning form as shown in the table below:

Table 4. JKL Toy Company's Physical Security Planning Form: Backup media and documentation example

Physical Security Planning Form	
Prepared by: Sharon Jones	Date: 9/2/99
Backup media and documentation:	
Where are backup tapes stored at your business location?	In a large, fireproof safe.
Where are backup tapes stored away from your business location?	In a fireproof safe at the office of the company's accountant.
Where are the security officer, service, and DST passwords kept?	With the safe combination in John Smith's office.
Where is important system documentation, such as the serial number and the configuration, kept?	In a large safe off site, and at our accountant's office.

After you plan your storage and documentation security, you can plan physical security for your workstations.

Planning physical security for workstations

In most cases, you want all users to be able to sign on at any available workstation and perform all authorized functions. However, if you have workstations that are either very public or very private, you may want to take special precautions. For example, display stations that can store keystrokes and personal computers require special consideration. Use this to help you complete Part 2 (Physical Security of Workstations and Printers) of the Physical Security Planning form.

Risks associated with workstations

Using a workstation in a public location for unauthorized purposes
> If people outside your company can easily access locations, they could potentially see confidential information. If a system user leaves a workstation signed on, someone from outside the company might be able to walk up and access confidential information.

Using a workstation in a private location for unauthorized purposes
> A workstation located in a very private location gives an intruder the opportunity to spend long hours trying to circumvent your security without being observed.

Using the playback function or a PC sign-on program on a display station to circumvent security measures
> Many display stations have a record and playback function, that allows users to store frequently used keystrokes and repeat them by pressing a single key. When you use a personal computer as a workstation on the iSeries system, you can write a program to automate the sign-on process. Because users frequently use the sign-on process , they might decide to store their user IDs and passwords, rather than typing them every time they sign on.

Recommendations

Consider these recommendations when setting up physical security for workstations:

- If possible, avoid placing workstations in very public or very private locations.
- Emphasize to system users the importance of signing off before leaving a workstation. You should cover sign-off procedures in your security policy.
- Emphasize that recording a password in a display station or in a PC program violates system security. You should cover recording password information in your security policy.
- Take measures, using the inactive timer system values (QINACTITV and QINACTMSGQ), to prevent user from leaving workstations in public locations without signing off the system.
- Limit which functions users can perform at public workstations by authorizing only users with limited authority to those workstations.
- Prevent users with security or service authority from signing on at private workstations. Use the QLMTSECOFR system value to control where a user signs on with these authorities .
- Restrict users from signing on at more than one workstation at the same time. You can use the system value which limits device sessions (QLMTDEVSSN) to control where users sign on.

To put these recommendations into effect, see the topics "Choosing system values that affect sign on" and "Planning resource security for workstations" for details.

For the Physical Security Planning form, you need to identify which workstations might pose a risk because of their physical location. You may want to review the example of how Sharon Jones planned JKL Toy Company's workstation physical security.

After you plan workstation security, you can plan physical security for printers and printer output.

Physical security for printers and printer output

Once information starts printing, system security cannot control who sees it. To minimize the threat of someone seeing sensitive business information, you should secure printers and printer output. You should also create a policy that deals with printing confidential business information.

Risks associated with printers and printer output

The following risks may apply to your business situation. These are the most common security risks that are associated with printer and printer output. However, you should investigate other risks that may apply to your specific business situation.

- A printer located in a public place might give unauthorized people access to confidential information.
- Printer output left lying on a desk might reveal information.
- Your system may have only one or two printers. You may need to print valuable or confidential information, such as paychecks, that employees at your company should see.

Recommendations

The following recommendations can help you diminish security risks that are associated with printers and their output.

- Emphasize to system users the importance of protecting confidential printer output. Include your physical security decisions regarding printers in your security policy.
- Avoid locating printers in public places.
- Schedule the printing of highly confidential output and have an authorized person stay at the printer while it prints.

"Planning security for printers and printer output" discusses suggestions for handling confidential printer output.

You may want to see an example of JKL Toy Company's plan for printer security before you begin to plan your security policy.

Example: JKL Toy Company's physical security planning form—workstation and printer portion:
Below is an example of Part 2 of the Physical Security Plan that Sharon Jones used for JKL Toy Company:

Table 5. JKL Toy Company's Physical Security Planning Form: Workstation and printer example

Physical Security Planning form			Part 2 of 2
Physical security of workstations and printers			
Workstation or printer name	Its location or description	Security exposure	Protective measures to be taken
DSP06	Loading docks	Too public	Automatic sign-off. Limit functions that can be completed at the workstation.
DSP09	Customer service desk	Too public	Automatic sign-off. Limit functions that can be completed at the workstation.
RMT12	Remote sale office	Too private	Do not let security officer sign on there.
PRT02	Accounting, near system unit	Sensitive information, such as price lists, could be seen	Appoint someone to monitor printer output

After you complete the Physical Security Planning Form, continue to the topic,"Planning your security policy".

Planning your security policy

You may find it useful to send security guidelines to all of your employees to emphasize your security policies regarding physical and system security. You can give the same guidelines to new users who are added to your system later.

In these guidelines, you should include some general instructions about how to protect system security, such as signing off workstations and not sharing passwords. The guidelines also should include information about the specific security decisions you made.

As you read through this planning information, make notes about what your own security guidelines should include. You also may want to make notes for your security policy.

For example, Sharon Jones of JKL Toy Company made these notes for her security guideline as she planned physical security for the system:

```
Make sure to emphasize signing off for loading dock, customer service,
and remote sales office. Accounting people will watch system unit.
```

After you complete the Physical Security Planning Form, you are ready to plan security for your applications.

Planning your application security

To plan the right security for your applications, you need to know:
- What information do you plan to store on the system?
- Who needs access to that information?
- What kind of access do people need? Do they need to change information or only view it?

As you go through these application planning topics, you answer the first question about what information you plan to store on your system. In subsequent topics, you decide who needs that information and what kind of access people need. You do not enter the application planning information into the system; however, you will need it when you set up users and resource security.

What is an application?

In the first planning step for application security, you need to describe the applications you plan to run on your system. An application is a group of functions that logically belong together. For example, at JKL Toy Company, entering orders, shipping orders, and printing invoices are all part of an application called Order Processing.

Usually, two different types of applications can run on your iSeries:
- **Business applications**: Applications you buy or develop to perform specific business functions, such as order processing or inventory management.
- **Special applications**: Applications you provide that are used throughout your company to perform a variety of activities that are not specific to a business process.

What forms do you need?

Use the following forms to help plan your application security:
- Application Description Form
- Library Description Form
- Naming Conventions Form

To print these forms, click the link, select the right frame and then click the **Print** icon in your browser.

Read the following information to help you complete these planning forms.
- Describing your applications
- Describing naming conventions
- Describing library information
- Drawing an application diagram

Describing your applications

At this point, you need to gather some general information about each of your business applications. Add information about your application to the appropriate fields on the Application Description form as described below. Later you can use this information to help you plan user groups and application security:

Application name and abbreviation
> Give the application a short name and an abbreviation that you can use as shorthand on forms and for naming objects that the application uses.

Descriptive information
> Briefly describe what the application does.

Primary menu and library
> Identify which menu is the primary menu for accessing the application. Indicate the library in which the menu is. Usually the primary menu leads to other menus with specific application functions. Users like to see the primary menu for their main application immediately after signing on the system.

Initial program and library
> Sometimes applications run an initial program that sets up background information for the user or does security checking. If an application has an initial program or setup program, list it on the form.

Application libraries

Each application usually has a main library for its files. Include all libraries that the application uses, including program libraries and libraries that other applications own. For example, the JKL Toy Company's customer order application uses the inventory library to get item balances and descriptions.

You can use the relationship between libraries and applications to determine who needs access to each library.

Finding information about your applications

If you do not already know the information you need about your applications, you may need to contact your programmer or application provider.

Following are methods for gathering the information yourself, if you do not have access to this information about an application that runs on your system.
- Users of the application can probably tell you the name of the primary menu and library, or you can watch them sign on the system.
- If users see the application immediately after signing on, look at the **Initial program** field in their user profiles. This field contains the initial program to the application. You can use the DSPUSRPRF command to view the initial program.
- You can list the names and descriptions of all the libraries on your system. Use the DSPOBJD *ALL *LIB. This displays all libraries on your system.
- You can observe active jobs while users are running the application. Use the Work with Active Jobs (WRKACTJOB) command with intermediate assistance level to get detailed information about interactive jobs. Display jobs and look at both library lists and their object locks to find out which libraries are being used.
- You can display batch jobs in an application using the Work with User Jobs (WRKUSRJOB) command.

To ensure that you gather all the information you need to plan your application security, you should complete these tasks before continuing:
- Complete an Application Description form for each of your business applications. Fill out the entire form, except the security requirements section. You will use that section to plan resource security for the application as described in the topic "Planning resource security".
- Prepare an Application Description form for each special application, if applicable. Using the form helps you determine how to provide access to the application.

Note: Preparing Application Description forms for special applications from IBM, such as IBM Query for iSeries is optional. Access to the libraries used by these applications does not require any special planning. However, you may find it useful to gather the information and prepare the forms.

You may want to see an example of JKL Toy Company's Application Description form before you move on to describing naming conventions.

Example: JKL Toy Company's application description form: Sharon Jones listed all the company's applications with their abbreviations on her Application description form. She also briefly described how users work with these applications.

Customer Orders (CO)

Enter, track, and ship orders. Print invoices.

Inventory Control (IC)

Manage levels of inventory for both finished products and materials. Process all inventory transition.

Contract and Pricing (CP)
>   Manage special pricing and contracts with customers.

Accounts Receivable (AC)
>   Keep track of current balances. Print monthly statements.

The table below contains Sharon Jones' description of the Customer Order application. She prepared her forms systematically, beginning with one application and then describing the rest.

Table 6. JKL Toy Company's Application Description Form: example

Application Description form	
Prepared by: Sharon Jones	Date: 9/3/99
Application Name: Customer Orders	Abbreviation: CO
Brief description of the application:	Enter customer orders, track them prior to shipment, ship the order, and print invoices and shipping papers.
Primary menu name: COMAIN	Library: COPGMLIB
Initial program name: NA	Library: NA
List the libraries used by the application for both files and programs: • CUSTLIB • ITEMLIB • CONTRACTS • COPGMLIB	
Define the security objectives for the application, such as whether any information is confidential:	

In addition to the Customer Order application, Sharon Jones also prepared Application Description forms for these applications on JKL Toy Company system:

- Inventory Control
- Contracts and Pricing
- Accounts Receivable.

Next, you can describe naming conventions for objects on your system.

Describing naming conventions

When you know how the system names objects, you can plan and monitor security, solve problems, and plan backup and recovery. Most applications have rules for assigning names to objects, such as libraries, files, and programs. If your applications come from different sources, they probably each have their own unique naming system.

Be sure to record all the naming conventions of applications and objects on the Naming Conventions form. On the Naming Conventions form, list the rules your applications use for naming libraries and files. You may want to use the blank lines for other naming conventions, such as programs and menus. If your applications come from different sources, they probably each have unique naming conventions. Describe the naming conventions for each application. You may need to prepare more than one Naming Conventions form.

You may want to see an example of how Sharon used naming conventions for objects on JKL Toy Company's system before you move on to describing library information.

Example: JKL Toy Company's naming conventions form: The table below shows the naming conventions for the libraries and files only. You will also need to describe naming conventions for other

types of objects on your system. The Naming Conventions form contains several common objects; however, you may have others you will need to prepare.

Table 7. JKL Toy Company's Naming Conventions form: example

Naming Conventions form	
Prepared by: Sharon Jones	Date: 9/3/99
Type of Object	**Naming Convention**
Libraries	Libraries containing files have meaningful names, like CONTRACTS or ITEMLIB. Program libraries use the application abbreviation followed by PGMLIB, such as ICPGMLIB.
Files	Major files have meaningful names, such as CUSTMAST for the Customer Master file or ITEMMAST for the Item Master file. Other application files (used for reasons only programmers understand) are named with the application abbreviation followed by FILE and a number, such as ICFILE14.

After you have completed the Naming Conventions form, you can begin describing library information.

Describing library information

After you have described your naming conventions, you should describe the libraries on your system. Libraries identify and organize objects on your system. Placing similar files together in one library allows users easy access to critical applications and files. You can also customize your users' authorities, so that they can access some libraries, but not others. Describe all libraries that are on your system for each application. You may need to prepare more than one Library Description form

Note: Fill out only the descriptive information about the library. When you plan resource security for the library you will fill out the rest of the Library Description Form. You will need to add information about authorities to the libraries later. See "Planning security for application libraries" for details on completing the remainder on the Library Description Form.

Before you continue, be sure to complete the following:
- Fill in the library and file parts of the Naming Conventions Form.
- Fill in the descriptive information on the Library Description form for each application library.

You may want to see an example of how Sharon Jones of JKL Toy Company described libraries before you draw an application diagram.

Example: JKL Toy Company's library description form: The two tables below describe two libraries that the Customer Orders Application uses at the JKL Toy Company. The first table describes a library containing files, and the second describes a library containing programs.

Table 8. JKL Toy Company's Library Description Form: Library containing files example

Library Description form	
Prepared by: Sharon Jones	Date: 9/3/99
Library name: CUSTLIB	Descriptive name (text): Customer Records Library
Briefly describe the function of this library:	Holds all customer files, including orders and accounts receivable.

Table 9. JKL Toy Company's Library Description Form: Library containing programs example

Library Description form	
Prepared by: Sharon Jones	Date: 9/3/99

Table 9. JKL Toy Company's Library Description Form: Library containing programs example (continued)

Library name: COPGMLIB	Descriptive name (text): `Customer Order Program Library`
Briefly describe the function of this library:	`Holds all programs for the customer order application.`

After you describe your libraries, you should draw an application diagram for your system.

Drawing an application diagram

As you prepare your Application Description and Library Description forms, you may find it useful to draw a diagram showing the relationship between applications and libraries. A diagram will help you to plan both user groups and resource security.

The figure below shows the diagram Sharon Jones drew of the JKL Toy Company's applications and libraries:

JKL Toy Company's applications and libraries diagram

RV2L229-2
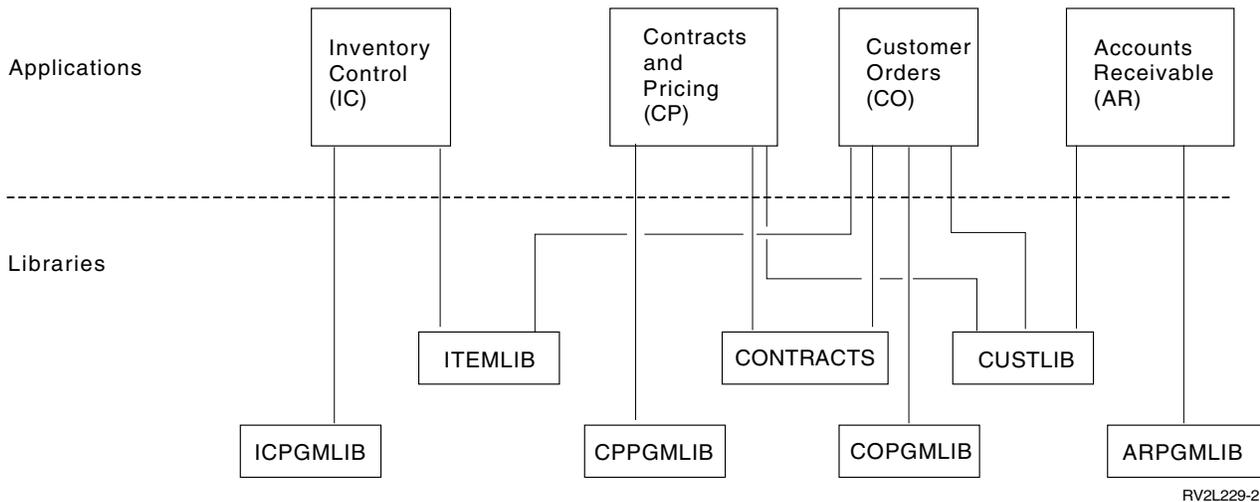
Collecting some information about your applications and libraries now will help you with many security decisions you need to make. Look at this as a chance to become more knowledgeable about your system and applications.

To ensure that you have gathered the application information that you need, you should:
- Complete an Application Description form for each business application on your system.
- Optionally, prepare an Application Description form for each special application on your system.
- Fill in the library and file sections of the Naming Conventions form.
- Prepare a Library Description form for each application library.
- Draw a diagram of the relationship between your applications and libraries.

When you have completed these forms, you can begin planning your overall security strategy.

Planning your overall security strategy

After you plan security for your applications, you are ready to start your overall security strategy. First, you need to make decisions about the overall approach to security on your system. As you make these decisions, balance the needs of your company today with the needs of the future.

Use this information to help you through the planning process to determine your security policy and objectives. You can also use this information to help you choose basic system values, which affect all of the users on your system.

What forms do you need?

To complete planning for your applications, use the System Values Selection Form.

You should use your completed Physical Security Plan form and Application Description forms as you review these topics to make your decisions about system values.

Review these topics to plan your security strategy:
- Writing a security policy
- Choosing your security level
- Choosing system values that affect sign on
- Choosing system values that affect passwords
- Using system values to customize your system

Writing your security policy

Before you begin planning, prepare a statement of your company policy regarding security on your system. This statement is an agreement between you and the top officials in your company. It helps you make decisions and determine what is important. Your security policy should state what your overall approach is and what information assets require protection.

Every system should have security. You can adopt one of these approaches to your security:
- **Strict**: Some people call this a need-to-know security scheme. In a strict security environment, you give users access only to the information and functions they need to do their jobs. All others are excluded. Many auditors recommend the strict approach.
- **Average**: An average security approach give users access to objects, based on the authorities you have assigned them.
- **Relaxed**: In a relaxed security environment, you allow authorized users access to most objects on the system. You restrict access in cases of specific critical or confidential resources single department or small company usually uses the relaxed approach on their systems.

Your overall approach helps you in making decisions about your specific security needs. The security approach for your system should match the philosophy for access to information throughout your company. If you are not sure of what approach to use, try this:
- Use your completed Application Description form to determine who should or should not have access to those applications.
- Examine the technologies that you use in your company. For example, if you plan to connect your system or network to the Internet, you will want a more restrictive security environment to protect your system from outside Internet users.
- Talk with other members of your organization, such as security auditors, to better determine your security needs.

Remember that you can always change your policy. Most companies find they need more strict security as they grow. This information helps you set up a security scheme that allows you to add more security later without having to make lots of changes or to test all your applications again.

What to secure

In addition to stating your overall approach to security in your security policy, you need to identify the critical information assets of your company. Your security system should be designed to protect this information. You can use several requirements to determine critical assets:

- **Confidentiality**: Information that is not generally available to people in your company. Payroll is an example of confidential information.
- **Competitiveness**: Information that gives you an advantage over your competition, such as product specifications and formulas.
- **Operations**: Information on your computer that is essential for the daily operations of your business, such as customer records and inventory balances.

Sharon Jones, the security officer, and John Smith, the company president, worked together to prepare a statement of their security policy. John Smith used these notes to draft their security policy for JKL Toy Company. You may like to review the security policy that JKL Toy Company sent to all of their employees after they completed planning and setting up their security. Remember as you work through these planning topics, take notes on what you would like to add to your security policy.

Table 10. JKL Toy Company's security policy: example

```
Overall Approach
        Relaxed: Most people need access to most information.
Critical Information
        • Contracts and special pricing
        • Payroll
        • Customer and inventory records are available to only company employees.
General Rules
        • Every system user will have a user profile. User can not share profiles or passwords.
        • User must change their passwords every 60 days.
```

After you have made notes regarding your security policy, you can choose your security level.

Choosing your security level

The QSECURITY system value lets you control how much security you want on your system. To understand how the security levels work, think of your system as a building, where people are trying to enter.

Level 20: Password security

> If you select level 20, you have some security protection. The guard at the door to the building asks for identification and a secret password. Only people who have both are admitted to the building. But once people are inside, they can go anywhere and do anything they want.
>
> If someone overhears a secret password and uses it to get past the guard at the door, you have no protection.

Level 30: Password and resource security

> Level 30 gives you everything you had at level 20, plus you can control who goes to certain parts of your building and what they do when they get there. You can designate some parts of your building as public, while others are restricted with guards at the doors.
>
> You can allow people who have access to restricted sections to do anything they want, or you can require that they make their requests for information to authorized information clerks (programs). An intruder who gets in using someone else's password might still have to get past the inside guards to get to protected sections.

Level 40: Integrity protection

> At level 40, you get all the protection of level 30, but the system verifies a user's access. The guards at the doors inside the building checks the passwords and logs all users entering the room.

Level 50: Advanced integrity protection

> At level 50, the guards enforce an even stricter set of rules to prevent a person with special knowledge from getting past the restricted doors by validating the identity of anyone who signs the log.

Recommendations

iSeries ship with a security level of 40. Security level 40 is the best choice for most installations, whether your security policy is strict, average, or relaxed. If you choose a relaxed approach, you can set up public access to most of the resources on your system. By using security level 40 from the very beginning, you have the flexibility to make your system more secure in the future without making many changes.

If you are buying application programs, check with your application provider to make sure the programs have been tested at level 40. Some applications use operations that cause errors at security level 40. If your applications have not been tested at level 40 or 50, start with level 30. Use the audit journal function to see if your applications log authority failures. If not, you can change to level 40 or 50.

Security level 50 prevents events that do not normally occur on most systems. The system does additional checking whenever programs are run on your system. This additional checking may have a negative effect on performance.

After you enter your choice for security level on the System Values Selection Form, you can choose system values that affect sign on.

Choosing system values that affect sign on

After you choose your security level, you can customize what users see on displays and how they interact with the system by using system values. You will need to plan these system values and use the System Values Selection form to record your choices.

The table below describes the system values used in this topic.

Table 11. iSeries system values and their descriptions

System value	Description
QMAXSIGN	Limits the number of consecutive sign-on attempts.
QMAXSGNACN	Specifies the action that the system takes if the consecutive sign-on attempts are reached.
QLMTDEVSSN	Determines whether a user can sign-on at more than one workstation with the same user profile.
QINACTITV	Determines when the system takes an action on inactive jobs.
QINACTMSGQ	Determines the action the system takes when an interactive job has been inactive for the length of time specified by the QINACTITV system value.
QDSCJOBITV	Controls if and when the system ends a job that has been temporarily disconnected.
QLMTSECOFR	Restricts the security officer, who has authority over all objects on the system to specific devices.

Limiting the number of sign-on attempts (QMAXSIGN and QMAXSGNACN): Two system values determine the number of times someone can attempt to sign on your system and the action the system takes once the limit has been reached.

The maximum sign on attempts (QMAXSIGN) system value limits the number of consecutive incorrect sign-on attempts that the system allows before taking some action. An incorrect sign-on attempt means that someone tries to use a particular user profile with either an invalid password or the improper authorization to a workstation.

The maximum sign on action (QMAXSGNACN) system value specifies what the system does if someone tries to sign on too many times in a row. The possible values are:

1   Prevent any more sign-on tries for the device. This is called disabling the device. No one can sign on at the device until an authorized person varies the device on using the WRKCFGSTS command. This option is usually not sufficient protection, especially when attempts are made to sign on to your system from a personal computer or a remote system.

       A system operator or anyone with *USE authority to the device can make the device available again.

2   Prevent any more sign-on tries for the user profile. This is called disabling the user profile. No one can sign on with that profile until an authorized person enables it by using the Change User Profile (CHGUSRPRF) command.

       To enable a user profile (change the status), you must be a security administrator with authority to use the profile.

3   Disable both the user profile and the device.

Risks and Recommendations

Some mischief makers enjoy the challenge of guessing passwords and breaking into systems. By limiting the number of sign-on attempts you allow, you limit their guesses.

The maximum not valid sign on (QMAXSIGN) system value determines how many sign-on tries you allow. Set it high enough to avoid frustrating users. Set it low enough to discourage careless typing and to prevent giving a potential intruder too many guesses. You should set the value for your maximum number of sign on attempts between 3 and 5.

The recommended maximum sign on action (QMAXSGNACN) is 3, even though disabling the device as well as the user profile might inconvenience system users. A workstation located in a private place might give an intruder the opportunity to try many different user profile and password combinations. If your system has no workstations which pose a risk because of their location, then disabling only the user profile is probably sufficient protection.

Check your completed Physical security form. If you have workstations in remote locations or have remote users (users who access your system through phone lines or VPN connections), then you may want to limit sign on more strictly. Be sure to add your choices for QMAXSIGN and QMAXSGNACN to Part 2 of the System Values Selection form.

You may find it useful to review an example that illustrates how these system values work together to limit sign-on attempts before you choose system values that limit users to one workstation at a time.

Example: Limiting sign-on attempts: Sharon Jones limited the sign-on attempts to 3 (QMAXSIGN is 3) and chose to disable both the profile and the device if the limit is exceeded (QMAXSGNACN is 3). Here is what might happen when these values were reached:
1. Roger types his password incorrectly twice.
2. After the second attempt he receives a message warning him that another incorrect sign-on attempt will disable the user profile.

3. He makes another mistake.
4. The system disables his profile and the workstation no longer has a Sign On display. If Roger tries to sign on at another workstation, he receives an error message.
5. Now he needs to ask Sharon to enable his profile for him to try again. Sharon or the system operator also needs to make Roger's workstation available. If Roger does not remember his password, Sharon can give him a temporary password, which he must change when he signs on again.

Next you can review the system value that limits users to one workstation at a time.

Limiting users to one workstation at a time: The limit device sessions (QLMTDEVSSN) system value determines whether the same user can be signed on at more than one workstation at the same time. The possible values are:

0   The system allows an unlimited number of users to be signed on at the same time with the same user profile.

1   A user profile may only be used at one device at a time. The user may have more than one session at the same device.

Risks and Recommendations

Allowing users to sign on to only one workstation at a time promotes good security habits. Lazy security habits pose a security risk:

- If you limit users to one device, you discourage sharing user IDs and passwords. If people share user IDs, you lose both control and accountability. You can no longer tell who really does what functions on the system.
- Users must remember to sign off one workstation before moving to another one. Workstations left signed on, but not in use, pose a security risk.

The recommended setting for the system value QLMTDEVSSN is 1, which limits users to a single device. Give every system user a unique user ID and password with the appropriate authorities, then restrict them to using one workstation at a time. Be sure to add your choice for QLMTDEVSSN to Part 2 of the System Values Selection form.

You can begin to plan system values for inactive jobs next.

Planning system values for inactive jobs: Three system values work together to determine what action the system takes when a user forgets to sign off a workstation.

The inactive job time-out interval (QINACTITV)
The QINACTITV system value determines whether the system takes action if a display has been signed on but inactive for a specified time period.

> **Note: Inactive** means that the user has not pressed the Enter key or a function key during the specified interval.

The inactive job message queue (QINACTMSGQ)
Your setting for the QINACTMSGQ system value determines what the system does when the time limit you specify in the system value QINACTITV expires. If you select ENDJOB, the system ends any job that has been inactive longer than the time-out interval you chose for QINACTITV. If you select DSCJOB, the system disconnects an inactive job. If you specify the name of a message queue, the system sends a warning message to that queue when a job has been inactive too long.

When the system **disconnects** a job at a workstation, it suspends the job temporarily. The workstation returns to the sign-on display. The disconnected job resumes when the same user signs on again at the same workstation.

The disconnected job time-out interval (QDSCJOBITV)

> The QDSCJOBITV system value controls if and when the system ends a job that has been temporarily disconnected. Jobs can be disconnected automatically by the system, as a result of the QINACTITV and QINACTMSGQ system values. Users can also request that their jobs be temporarily signed off (disconnected) using an option on the Operational Assistant menu or the Disconnect Job (DSCJOB) command.

Risks and Recommendations

If Sharon forgets to sign off her workstation before leaving, John can walk up to the workstation and perform any function that she is allowed to do on the system.

You should regulate inactive displays particularly for two reasons:
- You have a strict security environment with confidential information stored on your system.
- You have workstations located in places where people outside your company can access them easily.

Normal job duties often interrupt users at their workstations. Take advantage of the way these three system values work together to allow for normal interruptions and still protect your system security.

To eliminate these risks, IBM recommends using the QINACTITV, QINACTMSGQ, and QDSCJOBITV system values together to allow for normal work interruptions and still protect your system security.

The inactive job time-out interval (QINACTITV): Make the interval short enough to discourage leaving workstations unattended, but not so short as to inconvenience users. The recommended setting is 30 minutes. When a job has been inactive for 30 minutes, the system takes the action specified in the inactive job message queue.

The inactive job message queue (QINACTMSGQ): Choose disconnect job. The system disconnects any job that has been inactive for the period of time specified in the inactive job time-out interval. The system suspends the job and signs off the display. When the same user signs on again, the job will continue where it left off.

This is more convenient for users, because the system suspends rather that ends their jobs. Disconnecting an inactive job provides as much protection for your system as ending the job.

Note: The system cannot disconnect some jobs. If the system cannot disconnect an inactive job, it ends the job instead. This may cause the loss of information. Consider setting the QINACTMSGQ to send messages to the system operator message queue.

The disconnected job time-out interval (QDSCJOBITV): Encourage system users to temporarily sign off the system when they need to be away from their workstations for short periods and to finish their work and sign off for longer interruptions.

Use the QDSCJOBITV to end disconnected jobs before your system starts night processing, such as Automatic Cleanup. Set it long enough to give a user most of the business day to return to the workstation but short enough to end jobs before night processing starts. Choose 300 minutes (five hours) which gives night processing enough time to complete without interfering with a user's job.

Note: To prevent two users from trying to change the same information at the same time, the system **locks** a record before updating it. Any locks on resources remain in effect when a the system disconnects a user's job. Depending on your application design and the number of users on the system, locks may cause performance problems on your system. Check with your programmer or application provider to determine if locking may impact your performance.

You may want to review an example of how these system values work together to handle inactive jobs on the system.

After you record your decisions for inactive jobs on the System Value Selection form, you can decide how to limit where the security officer can sign on.

Example: Handling inactive jobs with the QINACTITV, QINACTMSGQ, and QDSCJOBITV system values: Assume you have set the inactive job time-out interval (QINACTITV) to 30 minutes. The system disconnects inactive jobs (QINACTMSGQ is DSCJOB). The disconnected job time-out interval (QDSCJOBITV) is 300 minutes (5 hours). For example, if Sharon forgets to signoff at 9:30 a.m., the system disconnects her job at 10:00 a.m. and will end the job at 3:00 p.m.

Add your choices for QINACTITV, QINACTMSGQ, and QDSCJOBITV system values on Part 2 of the System Values Selection form.

After you record your decisions for inactive jobs on the System Value Selection form, you can decide how to limit where the security officer can sign on.

Limiting where the security officer can sign on: You may want to restrict users with authority to change security and control objects to certain workstations. This prevents these users from signing on to workstations in remote locations without your knowledge. The system value QLMTSECOFR (limit security officer) allows you to do this. If you set QLMTSECOFR to 1, users with all-object (*ALLOBJ) or service (*SERVICE) special authority can sign on only at the console or other workstations you designate.

QLMTSECOFR restricts the security officer, users with authority over all the objects on the system, and service personnel to the console. You can use the Grant Object Authority (GRTOBJAUT) command to give these users access to other devices.

Note: In order for the QLMTSECOFR system value to work, your system security level needs to be 30 or higher.

Risks and recommendations

You should set the QLMTSECOFR system value to 1. If someone overhears or guesses the password for someone with the security officer profile, they must also get access to a device that allows them to sign on

After you have filled in your choices for QLMTSECOFR on Part 2 of the System Values Selection form, you can choose system values that affect passwords.

Choosing system values that affect passwords

You should allow users to assign their own passwords rather than the security officer assigning their passwords. When users create their own passwords, they usually do not need to write them down. Passwords that are written down tend to be stored in obvious places and pose a security risk.

A tip for creating passwords

Your users might have trouble thinking of good passwords. Suggest this technique: Use a sentence that is easy to remember to help you create a password that is difficult to guess. For example, after vacation you might use the sentence "July 4th fishing was poor" to create the password J4FWP.

Several system values regulate passwords. You can control how often users are required to change passwords. You can also establish many rules to prevent the use of passwords that are easy to guess. Many of these system values are important for large organizations. A few are important for everyone.

Using an option on the ASSIST menu or the Change Password (CHGPWD) command, users can assign their own passwords. When users change their own passwords, the system checks the new password against the password system values. If a user changes a password using the CHGUSRPRF command, the system does not check the new password against the security system values.

Note: If you have set any of the password system values, the system does not allow a new password to be the same as the user profile name, unless you use the CHGUSRPRF command to set the password.

The table below shows system values that affect passwords and their definitions:

Table 12. iSeries password-related system values

System value	Description
QPWDEXPITV	Requires users to change their passwords after a specified duration.
QPWDMAXLEN	Allows you to specify the maximum character length for passwords.
QPWDMINLEN	Allows you to specify the minimum character length for passwords.
QPWDRQDDIF	Prevents users from alternating between two different passwords.

These topics provide more details about these password-related system values:
- Determining password duration
- Determining the length of passwords
- Restricting duplicate passwords

Type `WRKSYSVAL *SEC` at the CL command line and view the on-line information for system values beginning with the characters QPWD.

Determining password duration: The QPWDEXPITV system value determines how often users are required to change their passwords.

The system warns users when their passwords are close to the expiration date. If a password expires, the system prompts the user to change their password at the next sign-on.

Recommendations

User should change their passwords periodically. This discourages sharing passwords with other system users. Also, if an unauthorized user learns someone's password, that password will only work for a short period of time. Set the password interval long enough to avoid irritating users, but short enough to provide good security. To avoid these problems set the interval between 45 to 60 days.

After you enter your choice for the QPWDEXPITV system value on Part 2 of your System Values Selection form, you can determine the length of passwords.

Determining the length of passwords: Some users do not like to type. If you let them, they will choose a one-letter password or their initials. Unfortunately, short passwords make it easier for an intruder to make a lucky guess. The QPWDMINLEN system value lets you set a minimum length for all passwords on your system.

If your system communicates with other systems, users may exchange passwords between the two computers. Some communications methods restrict the password to a maximum of 8 characters. The QPWDMAXLEN system value allows you to specify a maximum length for passwords.

Recommendations

Set your minimum password length at 6. This eliminates the use of initials and encourages users to be a little more creative in choosing passwords. Set your maximum password length at 8 if your system communicates with other systems.

After you enter your choices for the QPWDMINLEN and QPWDMAXLEN system values on Part 2 of your System Values Selection form, you can decide how much to restrict duplicate passwords.

Restricting duplicate passwords: The Change Password (CHGPWD) command requires that the new password be different from the old password. However, users can alternate back and forth between two different passwords unless you use the QPWDRQDDIF system value to prevent it. The table below shows the choices for the QPWDRQDDIF system value:

Table 13. Values for the QPDRQDDIF system value

Value	Number of passwords checked for duplicates
0	0 Duplicate passwords are allowed.
1	32
2	24
3	18
4	12
5	10
6	8
7	6
8	4

Recommendations

Use the password expiration interval and the duplicate password values to require that passwords be unique for a year. For example, if passwords expire in 60 days, select 7 for the QPWDRQDDIF system value.

After you enter your choice for the QPWDRQDDIF system value on Part 2 of your System Values Selection form, you can decide how to use system values to customize your system.

Using system values to customize your system

The iSeries uses system values and network attributes to control many things other than security. The system and application programmers use most of these system values and attributes. The security officer should set a few system values and network attributes to customize your system.

Giving your system a name

You use the SYSNAME network attribute to assign a name to your system. The system name appears in the upper-right corner of your sign-on display and on system reports. It is also used when your system communicates with another system or with personal computers using the iSeries Access for Windows®.

When your system communicates with other systems or personal computers, the system name identifies and distinguishes your system from others on the network. Computers exchange system names whenever they communicate. Once you assign a system name, you should not change it, because changing it affects other systems in your network.

Recommendations

Choose a meaningful and unique name for your system. Even if you are not communicating with other computers today, you may in the future. If your system is part of a network, the network manager will probably tell you what system name to use.

For example, Sharon Jones at the JKL Toy Company decided to name the system JKLTOY.

Displaying the time and date on your system

You can set the sequence in which year, month, and day appear when your system prints or displays the date. You can also specify what character the system should use between the year (Y), month (M), and day (D).

The system value QDATFMT determines the date format. The following chart shows how the system prints the date, 16 June 2000, for each possible choice:

Table 14. QDATFMT (System Date formats)

Your choice	Description	Result
YMD	Year, Month, Day	00/06/16
MDY	Month, Day, Year	06/16/00
DMY	Day, Month, Year	16/06/00
JUL	Julian Date	00/168

Note: These examples use the slash (/) date separator.

The system value QDATSEP determines what character the system uses between year, month, and day. The table below shows your choices. You use a number to specify your choice:

Table 15. QDATSEP (System Date Separator)

Separator character	QDATSEP value	Result
/ (slash)	1	16/06/00
- (hyphen)	2	16-06-00
. (period)	3	16.06.00
, (comma)	4	16,06,00
(blank)	5	16 06 00

Note: The above examples use the DMY format.

The QTIMSEP system value determines what character the system uses to separate hours, minutes, and seconds when it shows the time. You use a number to specify your choice. The table below shows how the time of 10:30 in the morning would be formatted using each value:

Table 16. QTIMSEP (System Time Separator)

Separator character	QTIMSEP	Result
: (colon)	1	10:30:00
. (period)	2	10.30.00
, (comma)	3	10,30,00
(blank)	4	10 30 00

Deciding how to name your system devices

Your system automatically configures any new display stations and printers you attach to it. The system gives a name to each new device. The QDEVNAMING system value determines how the names are assigned. The chart below shows how the system names the third display station and the second printer attached to your system:

Table 17. System Device Naming

Your choice	Naming format	Display station name	Printer name
1	iSeries	DSP03	PRT02
2	S/36	W3	P2
3	Address of the device	DSP010003	PRT010002

Note: In the above example, the display station and printer are attached to the first cable.

Recommendations

Use iSeries naming conventions, unless you are running software which requires S/36 naming. iSeries names for display stations and printers are less cumbersome than names which use the address of the device. Display station and printer names appear on several Operational Assistant displays. Printer names are also used to manage printer output.

After the system has configured a new device, use the Change Display Device (CHGDEVDSP) command or the Change Printer Device (CHGDEVPRT) command to enter a meaningful description of the device. Include in the description both the physical address of the device and its location, such as *John Smith's office, line 1 address 6*.

Choosing your system printer

Use the QPRTDEV system value to assign your system printer. This system value, the user profile, and the job description determine which printer a job uses. The job uses the system printer unless the user profile or the job description specifies a different one.

Recommendations

Normally, your system printer should be the fastest printer on your system. Use the system printer for long reports and system output.

Note: You will not know the names of your printers until you install and configure your system. Make a note about the location of your system printer now. Fill in the name of the printer later.

Allowing display of completed printer output

The system provides users the ability to find their printer output. The Work with Printer Output display shows all the output that is currently printing or waiting to print. You can also allow users to look at a list of completed printer output. This display shows when the output printed and on what printer it printed. This can be useful in locating lost reports.

The job accounting function and the QACGLVL system value allows you to display completed printer output. The *PRINT option for the QACGLVL system value allows information about completed printer output to be saved.

Recommendations

Storing information about completed printer output takes space on your system. Unless you think your users will print many reports, you probably do not need to provide this function. Enter NO on the System Values Selection form. This value sets the job accounting level to *NONE.

- Make sure you have written a security policy statement for your own company similar to the JKL Toy Company example that Sharon Jones and John Smith prepared.
- Make sure you have entered your choices for the system values on the System Values Selection form.
- Make notes about what you would like to include in your security memo.

After you have entered all your system options on the System Values Selection form and written a security policy, you can plan user groups.

Example: JKL Toy Company's security policy: The memo below illustrates the security policy that John Smith, president of JKL Toy Company, sent to his employees. He used the notes that he and Sharon created to develop this security memo.

Table 18. Example: JKL Toy Company's security memo

From: John Smith, President

Table 18. Example: JKL Toy Company's security memo (continued)

JKL Toy Company

To: All JKL Toy Company Employees

Subject: Security of the new system

You have all attended an information meeting about our new system. Those who will use the system have started training and will begin processing customer orders next week. We anticipate that this system will quickly become critical to the success of our business.

I want to review our security decisions and policies and emphasize their importance. These policies have been designed to protect information that is critical to our business.

- Sharon Jones has responsibility for security on the new system. Ken Harrison will assist her. Contact them if you have any questions or suspect any security problems.
- Our decisions about who can do functions on the system are based on our current policies regarding information. For example:
  - Contract and special pricing information is considered confidential. It should never be revealed to anyone outside the company.
  - Only Accounting can set and change credit limits for our customers.
- Everyone who needs to use the system will receive a user ID and a password. You will be required to change your password the first time you sign on the system and every 60 days after that. Choose a password that you can remember, but one that is not obvious. The form you receive with your user ID has some suggestions for creating passwords.
- *Do not share your password with anyone*. We intend for you to be able to do anything on the system that is necessary for your job. If you need access to information, contact Sharon or Ken. If you forget your password, Sharon or Ken can set up a new one for you immediately. There should be no reason for anyone to sign on with someone else's user ID and password.
- You may have learned how to use a record and playback function in your workstation to save typing. *Do not* use this to store your password.
- Do not leave your workstation signed on when you are away from your desk. In your training you learned how to sign off your workstation temporarily. Use this function if you need to leave your desk for a short time. If you will be away for a long period, finish your work and use the regular sign-off.

  Signing off when you leave your workstation is particularly important in locations that are accessible to the general public, such as the loading dock, the customer service area, and the remote sales offices.
- Although the system unit is very sturdy, please avoid bumping it or placing things on top of it. The control panels on the unit will normally be deactivated, but please do not touch them. Members of the Accounting department are responsible for making sure no one tampers with the system unit.

Remember, our new system is intended to make all our jobs easier and to improve our business performance. Our security policies should help you, not hinder you. If you have any questions or concerns, do not hesitate to contact Sharon, Ken, or me.

After you create a draft of your security policy, you can begin planning user groups.

Planning user groups

The first step in the planning process, deciding your security strategy, is like setting company policy. Now you are ready to plan for groups of users, which is like deciding department policy.

What is a user group?

A user group is exactly what its name implies: a group of people who need to use the same applications in the same way. Typically, a user group consists of people who work in the same department and have similar job responsibilities. You define a user group by creating a group profile.

What does a group profile do?

A group profile serves two purposes on the system:

- **Security tool**: A group profile provides a simple way to organize who can use certain objects on your system (object authorities). You can define object authorities for an entire group rather than for each individual member of the group.
- **Customizing tool**: You can use a group profile as a pattern for creating individual user profiles. Most people who are part of the same group have the same customizing needs, such as the initial menu and the default printer. You can define these in the group profile and copy them to the individual user profiles.

Group profiles make it easier for you to maintain a simple, consistent scheme for both security and customizing.

What forms do you need?

To plan for your user groups, you need these forms:
- User Group Identification form
- User Group Description form

> **Note:** You will need one User Group Description form for each user group that will be on your system.

Review these topics to help you complete these forms:
- Identifying user groups.
- Planning group profiles.
- Choosing values that affect sign on.
- Choosing values that limit what a user can do.
- Choosing values that set up the user's environment.

Identifying user groups

When you plan your user groups, you must first identify groups of users on your system. This allows you to plan accesses to resources that these groups need. Try using a simple method to identify your user groups. Think about the departments or work groups who plan to use the system. Look at the application diagram you drew earlier of your applications. See if a natural relationship exists between work groups and applications:

- Can you identify a primary application for each work group?
- Do you know which applications each group needs? Which applications they do not need?
- Do you know which group should own the information in each application library?

If you can answer "Yes" to those questions, then you can begin to plan your user groups. However, if you answered "sometimes" or "maybe", then you might find it helpful to use a systematic approach to identify your user groups.

You may want to review an example of using this approach to identify user groups.

> **Note:** Making users a member of only one group profile simplifies your security management. However, some situations can benefit from having users belong to more than one group profile.
>
> Having users belong to more than one group profile is usually easier to manage than giving many private authorities to individual user profiles.

Example: Identifying user groups: If the relationship between work groups and applications seems complicated or vague, using a matrix technique like the User Group Identification form might make things clearer. When you plot system users and their application needs on a matrix, you should see similar patterns emerge. In addition to filling in the User Group Identification form, Sharon Jones used her application diagram to identify which user groups needed access to the applications.

The illustration below shows JKL Toy Company application diagram.

RV2L228-3
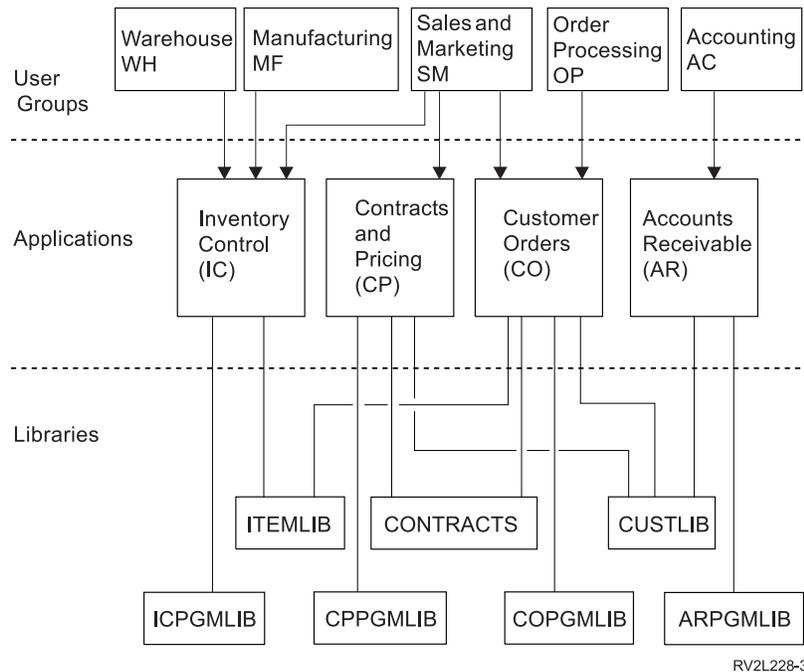
If your approach to security is relaxed, use an X to indicate that a user needs an application. If your approach to security is restrictive, you need to consider how people use applications. Rather than putting an X on the matrix, use a V (view) if someone only needs to look at the information in an application. Use a C (change) if someone needs to make changes to the information. Use an O (owner) if someone has primary responsibility for the information.

For example, at the JKL Toy Company, different groups need the Pricing and Contract application:
- The Sales and Marketing department sets prices and creating customer contracts. They *own* the pricing and contract information.
- The customer order department changes contract information indirectly. When they process orders, the quantities on the contract change. They need to *change* pricing and contract information.
- The order processing people need to look at the credit limit information to plan their work, but they are not allowed to change it. They need to *view* the credit limit file.

Table 19. JKL Toy Company's User Group Identification form: example

User Group Identification form					
Prepared by: Sharon Jones		Date: 9/2/99			
		Access Needed for Applications			
User Name	Department	APP: CO	APP: IC	APP: PC	APP: AR
Ken H.	Order Processing (OP)	O	C	C	C
Karen R.	Order Processing (OP)	O	C	C	C
Kris T.	Accounting (AC)	V		V	O

Table 19. JKL Toy Company's User Group Identification form: example (continued)

Sandy J.	Accounting (AC)	V	C	V	O
Peter D.	Accounting (AC)	C		V	O
Ray W.	Warehouse (WH)	V	O	V	
Rose Q.	Warehouse (WH)	V	O	V	
Roger T.	Sales and Marketing (SM)	C	C	O	C
Sharon J.	Managers (MG)	C	C	C	C
Note:					
• If your security environment is *Relaxed*, use an X to mark which applications users need.					
• If your security environment is *Average*, use A to mark which users will have authority to which applications.					
• If your security environment is *Strict*, you may need to use C (change), V (view), and O to specify *how* the applications are used.					

Sharon Jones made some notes about her decisions as she prepared the matrix:

- Order processing and accounting provide backup for each other. Today, they require similar applications. However, they should be separate groups because they will become more specialized in the future, as they add more people.

- Although we do not allow order processing to change inventory or contracts directly, item and contract balances change automatically when they create and fill orders. Will that become a security issue later?

- Sales and marketing people are involved in all parts of the business and every application. They set prices and descriptions for items. They set up new customers, although accounting sets the credit limits. They are responsible for setting all contract terms and prices.

Decide what your user groups should be. Fill in the User Group Identification form, if you need it to help you decide.

After you add your users to the User Group Identification form, you can plan a group profile.

Planning a group profile

Once you identify your user groups, you are ready to plan a profile for each group. Many of the decisions you make affect both security and customizing. For example, when you specify an initial menu, you may be restricting a user to only that menu. But you are also ensuring that the user sees the correct menu after signing on.

Prepare a User Group Description Form for one user group as an example. After you have finished the first form, go back and complete forms for the other groups that you need.

Security and customization on the iSeries are designed to be very flexible. The planning method in this topic provides a good way to design group profiles and job descriptions, but your programmer or application provider might recommend a different method.

Naming group profiles

Because a group profile acts as a special type of user profile, you may want to identify group profiles easily on lists and displays. You need to assign them special names. To appear together on lists, your group profiles should begin with the same characters, such as GRP (for group) or DPT (for department). Use these guidelines when naming user groups:

- User group names can be up to 10 characters long.
- The name may include letters, numbers, and the special characters: pound (#), dollar ($), underline (_), and the at sign (@).

- The name cannot begin with a number.

Note: For each group profile, the system assigns a group identification number (*gid*). Normally, you can let the system generate a *gid*. If you use your system in a network, you may need to assign specific gids to group profiles. Check with your network administrator to verify whether you need to assign gids.

You should add your naming system for group profiles in the appropriate field on the Naming Conventions Form. For example, Sharon Jones chose DPT as the naming convention for group profiles. She filled in the appropriate section of the Naming Conventions Form.

Table 20. JKL Toy Company's Naming Conventions Form: Group profile example

Type of object	Naming convention
Group Profiles	Use characters DPT followed by the abbreviation for the department. Text description of the group profile should be the department name.

Determining what applications and libraries a user group needs

If you have not already done so, add your user groups to the application diagram and libraries you drew earlier. This visual image will help you decide the resource and application needs of each group.

On Part 1 of the User Group Description Form indicate the group's primary application, which is the application they use most often. List the other applications the group needs.

Look at your Application Description Forms and your application diagram to see the libraries each group needs. Check with your programmer or application provider to find out the best method for providing access to these libraries. Most applications use one of these techniques:
- The application includes the libraries on a user's initial library list.
- The application runs a setup program which places the libraries in the user's library list.
- Libraries do not need to be in the library list. The application programs always specify the library.

The system uses a library list to find the files and programs you need when you run applications. The **library list** is a list of libraries the system searches for objects needed by the user. It has two parts:
1. **System portion**: Specified in the QSYSLIBL system value, the system portion is used for OS/400® libraries. The default for this system value does not need to be changed.
2. **User portion**: The QUSRLIBL system value provides the user portion of the library list.The user's job description specifies the initial library list, or commands after the user is signed on. If you have an initial library list, it overrides the QUSRLIBL system value. Application libraries should be included in the user portion of the library list.

Using a job description

When a user signs on the system, the user's job description defines many characteristics of the job, including how the job prints, how batch jobs are run, and the initial library list. Your system comes with a job description, called QDFTJOBD, which you can use when creating group profiles. However, QDFTJOBD specifies the QUSRLIBL system value as the initial library list. If you want different groups of users to have access to different libraries when signing on, you should create unique job descriptions for each group.

List each library needed by the group on the User Group Description Form. If the library should be included on the initial library list in the group's job description, mark each library name on the form.

You may want to review an example of how Sharon Jones described her user groups at JKL Toy Company, before you begin choosing values that affect sign on.

Example: JKL Toy Company's user group description form: The first table shows Part 1 of the User Group Description form that Sharon Jones prepared for the Sales and Marketing department. Notice that she did not include the libraries CONTRACTS and CPPGMLIB in the group's initial library list. The application automatically adds them to the library list rather than including them on the DPTSM initial library list. When a user exits the application, the system removes these libraries from the library list. This provides additional security for those libraries, because you can access them only through the application programs.

Table 21. JKL Toy Company's User Group Description form: Descriptive information example

User Group Description form	Part 1 of 2
Prepared by: Sharon Jones	Date: 9/5/99
Group profile name: DPTSM Description of the group: Sales and Marketing Department	
Primary application for the group: Contracts and Pricing List other applications needed by the group: Inventory (to enter item descriptions and prices), Customer Orders	
List each library the group needs. Mark (✔) each library that should be in the initial library list for the group: • ✔CUSTLIB • ✔ITEMLIB • ✔COPGMLIB • ✔ICPGMLIB • CPPGMLIB • CONTRACTS	

Additionally, Sharon also started a User Group Description form for the Warehouse Department.

Table 22. User Group Description form: Descriptive information

User Group Description form	Part 1 of 2
Prepared by: Sharon Jones	Date: 9/5/99
Group profile name: DPTWH Description of the group: Warehouse Department	
Primary application for the group: Inventory control	
List other applications needed by the group: none	
List each library the group needs. Place a check mark (✔) in front of each library that should be in the initial library list for the group: • ✔ITEMLIB • ✔ICPGMLIB	

After you have completed Part 1 of the User Group Description form, you can begin choosing values that affect sign on.

Choosing values that affect sign on

After you plan group profiles on your system, you need to choose system values that affect a sign on. Enter your choices on Part 2 of the User Group Description form. Remember, you choose values that will be copied to create individual profiles for the members of the group. Begin by entering the group profile name you have selected and a brief description (Text) for the group.

If you customize your system properly, users have to enter only their user IDs and passwords on the Sign On display. Their user profiles provide the other sign-on values.

Password

Set the password for a group profile to *NONE. This prevents anyone from signing on using the group profile. Later, when you copy the group profile to create individual user profiles, you set a password for each user.

Initial Program and Initial Procedure

A user's initial program, also called the **sign on program**, runs before the system displays the first menu. Put both the name of the program and its library in the group profile, even if the library is part of the initial library list. By specifying both, you make sure the system runs the correct program, and you do not have to worry about library list changes.

An initial program or procedure is used for one of the these reasons:
- Some applications use an initial program to set up the application environment.
- You want a user to run only one program and never see a menu. For example, at the JKL Toy Company, the people who use the workstation on the loading dock can only run the program for receiving inventory. This prevents security exposures at a workstation in a public location.

Setting the **Limit capabilities** field for a user to *YES or *PARTIAL prevents the user from changing the initial program on the Sign On display.

Check with your programmer to see if your applications require an initial program or procedure.

Initial Menu and Initial Menu Library

The initial menu, also called the **first menu**, is the first menu the user sees after signing on. The initial program runs before the initial menu is shown. If the initial program shows any displays, the user sees those displays before the system shows the initial menu.

Normally, the initial menu for a group should be the primary menu of the group's main application. Specify both the menu name and its library.

If you set the **Limit capabilities** field for a user to *YES, the user is not allowed to change the initial menu on the Sign On display. If you set the *limit capabilities* field for a user to *PARTIAL, you allow the user to change the initial menu on the Sign On display.

Current® library

The current library is also called the **default library**. Several things happen when you specify a current library for a user:
- If the user creates any objects, such as query programs, the system places those objects into the current library, unless the user specifies a different library.
- The system automatically adds the current library to the user portion of the library list. It can be included on the initial library list in the job description, but it does not have to be.
- The current library becomes the first library in the user portion of the library list. The system searches the current library for files and programs before searching the libraries in the user library list.
- If you do not assign a current library for a user, the system assigns the QGPL (general purpose) library.

Recommendations

The current library is particularly important if you plan to use the IBM Query for iSeries licensed program or another similar program. Use one of these approaches:

* Create a library for everyone in the group to share. Put all query programs and files for the group in that library. Give it the same name as the group profile and make it the current library for the group.
* Give each user who plans to use Query a personal library. Give the library the same name as the user profile. Specify that library as the current library on the individual profiles of group members, not on the group profile.

On Part 2 of the User Description form, fill in your choices for the fields that affect signing on.

After you choose the values that affect sign on, you can choose values that limit what a user can do.

Choosing values that limit what a user can do

After you enter your choices for the values that affect sign on on Part 2 of the User Group Description Form, you should consider limiting what a user can do on the system. You might want to limit what users can do for several reasons:

* To prevent people from using CL commands. They might be tempted to experiment and inadvertently damage things.
* To restrict users to specific applications and functions.
* To provide a simple environment where users are not confused by unnecessary choices.

Many factors determine how much your users can do:

* Application design
* System values
* Resource security
* Group profiles
* User profiles
* Job descriptions

Two fields in the group or user profile, **Limit capabilities** and **User class**, determine how much a user can override the decisions that you make.

Limit Capabilities

The **Limit capabilities** field is called **Restricted command line use**. You can limit whether users can change values on the Sign On display, enter commands, and change their Attention-key-handling program. Your can choose strict limits (*YES), average limits (*PARTIAL), or no limits (*NO). The following table shows what each of these values allow:

Table 23. Functions allowed for limit capabilities values

Limit capabilities value	Change initial program	Change initial menu	Change current library	Change attention program	Enter commands
*YES	No	No	No	No	A few[1]
*PARTIAL	No	Yes	No	No	Yes
*NO	Yes	Yes	Yes	Yes	Yes
1	These commands are allowed: SIGNOFF, SNDMSG, DSPMSG, DSPJOB, DSPJOBLOG, and STRPCO. The user cannot use F9 to display a command line from any Operational Assistant menu or display.				

User class

The user class, also called **type of user**, determines what options the user sees on Operational Assistant and system menus. It also determines what system functions a user is allowed to do, unless you list authorities in the **Special authority** field.

Recommendations for limited capabilities and user class

Most users do not need or want access to CL commands or system functions. The Operational Assistant displays give users enough information about and control over their own work. These recommendations allow users to access only those system resources they need to complete their tasks:

- In each group profile, set the **Limit capabilities** field to *YES. Set the *User class* field to *USER.
- Override these specifications for individual users who need system functions.
- Make sure that your menus provide a means to move between applications, if users need to do that.

After you enter your choices for user class and limit capabilities on Part 2 of the User Group Description form, you can choose values that set up the user's environment.

Choosing values that set up the user's environment

After you enter your choices for limiting what users can do on the system on Part 2 of the User Group Description form, you can choose values to determine the user's operating environment. Many fields in the user profile determine a user's operating environment: what printer to use, where to send messages, at what priority jobs should run. For many of these fields, the default setting is recommended. A few fields are described in the following paragraphs.

- **Job description and the job description library**: These fields in the profile tell the system what job description to use when the user signs on. The job description contains the initial library list. Each user group should have a job description with the same name as the group profile. Job descriptions are usually put in the QGPL library.
- **Printer device and output queue**: Any printer output created by the user goes to the printer device listed in the profile, unless the specific print job sends it to another printer. Members of a user group are usually located together and share the same printer. You can specify that printer in the group profile and copy it into each individual user profile. The user's printer device is also called the **default printer**.

  An output queue contains printer output before it is printed. Usually, each printer device has its own output queue with the same name. You can specify *DEV for the output queue to tell the system to use the printer device's output queue.

  Fill in the name of the job description and its library and the default printer and output queue fields on the User Group Description form.
- **Setting up the Operational Assistant interface**: When your system is shipped, the Operational Assistant menu is the Attention-key-handling program for every user. When users press the Attention key, they see the Operational Assistant (ASSIST) menu. If your application programs already use a different Attention-key-handling program, you should provide a different method for your users to reach the Operational Assistant menu:
  - Add the Operational Assistant menu as an option from your main application menus, either by using GO ASSIST or CALL QEZAST.
  - Have users type GO ASSIST from a command line.

If the **Limit capabilities** field is set to *YES in the user profile, the user cannot use the GO command to display a menu. You need to provide a method for Operational Assistant users to access the ASSIST menu.

You may want to review an example of what values Sharon Jones chose for the User Group Description form for JKL Toy Company.

To complete these planning steps, you should:

- Complete a User Group Description form for each user group in your company.
- Describe how you name user groups on the Naming Conventions form.
- Add user groups to your diagram of applications and libraries.

After you have completed these tasks, you can begin planning individual user profiles.

Example: JKL Toy Company's user group description form—part 2: Sharon Jones made a few notes about the Sales and Marketing and the Warehouse departments as she prepared the User Group Description form for the Sales and Marketing personnel.

- Sales and marketing personnel will be heavy users of IBM Query for iSeries. Each user should have a private library. Warehousing can have one group library.
- The warehouse people who work on the receiving dock will need an initial program instead of an initial menu.

Sharon prepared Part 2 of the User Group Description form for the two departments.

Table 24. JKL Toy Company's User Group Description form: Sales and Marketing department example

Field name	Recommended value	Your choice
Group profile name (User)		DSTSM
Password	*NONE	*NONE
User class (Type of user)	*USER	*USER
Current library (Default library)	*same as group profile name*	(leave blank in group; fill in for individual profiles)
Initial program to call (Sign on program)		
Initial program library		
Initial menu (First menu)		CPMAIN
Initial menu library		CPMAINLIB
Limit capabilities (Restrict command line use)	*YES	*PARTIAL
Text (User description)		Sales and marketing
Job description	*same as group profile name*	DPTSM
Job description library		QGPL
Group profile name (User group)	*NONE[1]	*NONE
Print device (Default printer)		PRT03
Output queue	*DEV	*DEV

Table 25. JKL Toy Company's User Group Description form: Warehouse department example

Field name	Recommended value	Your choice
Group profile name (User)		DPTWH
Password	*NONE	*NONE
User class (Type of user)	*USER	*USER
Special Environment		
Current library (Default library)	*same as group profile name*	DPTWH
Initial program to call (Sign on program)		
Initial program library		

Table 25. JKL Toy Company's User Group Description form: Warehouse department example (continued)

Field name	Recommended value	Your choice
Initial menu (First menu)		`ICMAIN`
Initial menu library		`ICPGMLIB`
Limit capabilities (Restrict command line use)	`*YES`	`*YES`
Text (User description)		`Warehouse Department`
Job description	*same as the group profile name*	`DPTWH`
Job description library		`QGPL`
Group profile name (User group)	`*NONE`[1]	`*NONE`
Print device (Default printer)		`PRT04`
Output queue	`*DEV`	`*DEV`

1	The group profile name must be *NONE for a group profile. A group profile cannot be a member of another group.

Now you can begin planning individual user profiles.

Planning individual user profiles

Now that you have decided on your overall security strategy and have planned user groups, you are ready to plan individual user profiles.

What forms do you need?

Use these forms to plan individual user profiles:
- Individual User Profile form
- System Responsibilities form

You will also need to use the information on these completed forms:
- User Group Definition form
- Naming Conventions form
- Your Application Diagram

Naming user profiles

Your user profile name is how you are identified to the system. You enter your user profile name in the **User ID** field of the Sign On display. Any work you do and printer output you create is associated with your user profile name.

Consider these things when deciding how to name user profiles:
- A user profile name can be up to 10 characters long. Some communications methods limit the user ID to 8 characters.
- A user profile name may include letters, numbers, and the special characters: pound (#), dollar ($), underline (_), and the at sign (@). It may not begin with a number or underline (_).
- The system does not distinguish between uppercase and lowercase letters in a user profile name. If you enter lowercase alphabetic characters, the system translates them to uppercase characters.
- The displays and lists you use to manage user profiles show them in alphabetical order by user profile name.

- All IBM-supplied profiles begin with the letter Q. To keep your profiles separate from IBM-supplied profiles, avoid assigning user profile names that begin with the character Q.

Recommendations

One technique for assigning user profile names is to use the first 7 characters of the last name followed by the first character of the first name. Below is the naming conventions Sharon used for user profiles at the JKL Toy Company:

Table 26. JKL Toy Company's Naming Convention form: User profile example

User name	User profile name
Anderson, George	ANDERSOG
Anderson, Roger	ANDERSOR
Jones, Sharon	JONESS

This method makes user profile names easy to remember. Also, your lists and displays are sequenced alphabetically by last name.

For example, Sharon Jones of the JKL Toy Company plans to use this naming technique. She filled in the appropriate section of the Naming conventions form.

Table 27. JKL Toy Company's Naming Convention form: User profile example

Type of object	Naming convention
User Profiles	Use the first 7 characters of the user's last name, followed by the first character of the user's first name. Descriptions of the user profile will be last name, first name.

Describe how you plan to name user profiles on Naming Conventions form, then you can determine who should be responsible for system functions and choose values for each user.

Determining who should be responsible for system functions

When planning individual user profiles, you must first determine responsibilities of individuals on the system. To keep your system operating efficiently, you need people to perform various management and maintenance functions regularly. The people who do these tasks need the authority to run commands and perform system functions.

Choosing values that limit what a user can do discussed how the **User class** and **Limit capabilities** fields control the system functions a user can access. Normally, you should not allow most users to perform system functions (set the user class to *USER and limit capabilities to *PARTIAL or *YES). However, some users need additional authority to keep your system operating efficiently.

The table below lists some of the important system management tasks. It also indicates the user class and special authorities that you can assign for people with those responsibilities. This list helps you to determine which users on your system need special authorities. However, it is not intended as a complete planning tool for operating and maintaining your system. This table provides the user class and special authorities that work with most systems. You may need to assign different authorities depending on your system

When you assign a user class other than *USER in the profile, the user automatically receives a certain set of special authorities to perform system functions. You can assign a user special authorities that are different from those you specify in the user class field, but it may not be necessary.

Table 28. System Responsibility, User Class, and Special Authority

System function[1]	Description	User class required [2]	Special authority required [3]
System Operations	Manage printer output, respond to system messages, monitor regular operations, perform initial program load (IPL).	*SYSOPR	*JOBCTL
System housekeeping	Perform system housekeeping functions, such as establishing an automatic cleanup schedule and monitoring disk usage.	*SYSOPR	*JOBCTL
System backup	Regularly save application libraries, system libraries, and security information. See the Backup and Recovery topic of the Information Center for details about these functions.	*SYSOPR	*SAVSYS
Profile administration	Add new user profiles, maintain existing profiles.	*SECADM	*SECADM
Resource security administration	Maintain authorities to objects on the system.	*SECOFR	*ALLOBJ
Program maintenance	Apply periodic program changes (PTFs) to IBM-supplied libraries. Makes changes to your application libraries.	*SECOFR	*ALLOBJ
Security auditing	Set up the security auditing function. Determine which events, users, and objects should be audited.		*AUDIT [4]
System configuration	Add, change, and remove devices from your system.		*IOSYSCFG[5]

1	Set the Limit capabilities field to *NO for users who have these responsibilities.
2	This is the minimum user class needed. The user class provides the authority to use the commands and menu options that are necessary to do the function. Depending on your resource security, additional object authority may also be required.
3	This particular special authority is required for the job responsibilities. The user class may give additional special authorities.
4	The *AUDIT special authority does not have a corresponding user class. The *SECOFR user class includes *AUDIT special authority. However, your auditor probably does not need the other capabilities of the *SECOFR user class. You should specify *AUDIT special authority for each individual user who needs to control auditing on your system.
5	The *IOSYSCFG special authority does not have a corresponding user class. The *SECOFR user class includes *IOSYSCFG special authority. You should specify *IOSYSCFG special authority only for individuals who need to configure your system. The individuals could create lines, controllers and devices, or configure TCP/IP. However, the user configuring your system may not need the other capabilities of the *SECOFR user class.

Recommendations

Use the table above to plan who should perform system functions. At a minimum, you should assign two people to manage system security, and two others to manage operations and backup.

Use the System Responsibilities form as a tool for managing and auditing your system. Keep track of everyone who has special authority on your system and why they need that special authority.

You may want to review an example of how Sharon Jones determined user responsibility before you choose values for each user.

Example: JKL Toy Company's system responsibility form: Below is an example of the System Responsibility Form that Sharon Jones completed:

Table 29. JKL Toy Company's System Responsibilities Form: example

Who is your primary security officer? Sharon Jones			
Who is your backup security officer?Ken Harrison			
Profile Name	User Name	Class	Comments
JONESS	Sharon Jones	*SECOFR	Sharon is the primary security officer and system manager.
HARRISOK	Ken Harrison	*SECOFR	Ken is Sharon's backup as overall system manager.
JOHNSONS	Sandy Johnson	*SYSOPR	Sandy has the primary responsibility for system operations and backup.
ROGERSK	Karen Rogers	*SYSOPR	Karen will help Sandy with operations and system backup.
WILLISR	Rose Willis	*SYSOPR	Rose will operate the system during second shift.

After you have completed the System Responsibility form, you can begin choosing values for each user.

Choosing values for each user

After you have determined the responsibilities of users on your system, you can begin choosing values for each user. By planning group profiles as patterns for individual user profiles, you have done most of the work. Use the Individual User Profile form to assign each user to the correct group and define how the user is different from others in the group. You should complete an Individual User Profile form for one user group as an example, then go back and prepare Individual User Profile forms for any additional user groups.

Fill in the group profile name and other descriptive information on the top of the Individual User Profile form.

Example: JKL Toy Company's Individual User Profile form's descriptive information

Here is how Sharon Jones filled in the top portion of the Individual User Profile form.

Table 30. JKL Toy Company's Individual User Profile form: Descriptive information example

Individual User Profile form	
Prepared by: Sharon Jones	Date: 9/5/99
Group profile names: DPTOP	
Owner of objects created:	Group authority to objects created:
Group authority type:	

Determining values for group members

On your Individual User Profile form write the profile name and the description (user's name) of each member of the group. The paragraphs below describe how to determine other values for each group member.

Remember, the group profile is a pattern for the individual user profiles. On the Individual User Profile form you need to specify only the things that are different from the group.

- **Assigning passwords**: The easiest way to assign initial passwords to users is to make the password the same as the profile name. You can then require that the password be changed the first time the user signs on by setting the password to expire. In the topic Setting the password to expire you learn how to do this automatically when you copy the group profile. If you plan to do this, you do not need to need to list passwords on the Individual User Profile form.
- **User class and limit capabilities**: Look at your System Responsibility form to see which members of each group need a different value for the **User class** and **Limit capabilities** fields. Fill in the appropriate information on the Individual User Profile form for anyone who needs different values than the group profile.
- **Specifying other values**: Check to see if a particular user needs values that are different from those specified on the User Group Description form for the group. On the User Group Description form, the **User class** and **Limit capabilities** fields are listed at the top, because their values may often differ for some members of the group. List any other fields that vary for members of the group with which you are working.

To finish this planning step, be sure that you:
- Complete your System Values Selection form.
- Describe how you plan to name user profiles on your Naming Conventions form.
- Prepare an Individual User Profile form for each user group in your company.

You may want to review an example of the information Sharon used for individual users before you plan resource security

Example: JKL Toy Company's individual user profile form: At the JKL Toy Company, people who work on the loading dock can run only one program. Sharon limited these users to a few functions because they work in an area in which the public can easily access their workstations. These members of the Warehouse department have an initial program and no initial menu. The Order Processing department has two local printers and one printer in a remote sales office. Therefore, Sharon assigned some users a different printer than the group.

Below is the Individual User Profile form that Sharon Jones completed for the Warehouse and Order Processing Department at the JKL Toy Company. Notice that she filled in fields only when they were different from the values set in the group profile.

Table 31. JKL Toy Company's Individual User Profile form: Warehouse Department example

Group profile names: DPTWH					
Make an entry for each member of the group:					
User Profile	**Text (description)**	**User Class**	**Limit Capability**	**Initial Program/ Library**	**Initial Menu/ Library**
WILLISR	Willis, Rose	*SYSOPR	*NO		
WAGNERR	Wagner, Ray			ICRCPT/ICPGMLIB	none
AMESJ	Ames, Janice			ICRCPT/ICPGMLIB	none
FOSSJ	Foss, Julie				
WOODBURC	Woodburt, Carol				

Table 32. Individual User Profile form: Order Processing Department example

Group profile names: DPTOP				
Make an entry for each member of the group:				
User Profile	**Text (description)**	**User Class**	**Limit Capability**	**Print Device**
HARRISOK	Harrison, Ken	*SECOFR	*NO	PRT05

RICHARDK	Richards, Karen			
UNGERJ	Unger, Jeff			PRT04
BELLB	Bell, Brad			PRT04

Next you can begin planning resource security.

Planning resource security

Now that you have completed the process for planning users on your system, you can plan the resource security which protects objects on the system. In "Setting up resource security," you learn how to set up resource security on your system.

System values and user profiles control who has access to your system and prevent unauthorized users from signing on. Resource security controls the actions that authorized system users can perform after they have signed on successfully . Resource security supports the main goals of security on your system to protect:

- Confidentiality of information
- Accuracy of information to prevent unauthorized changes
- Availability of information to prevent accidental or deliberate damage

You may plan resource security differently, depending on whether your company develops applications or purchases them. For applications you develop, you should communicate the requirements for security of the information to the programmer during the application design process. When you purchase applications, you need to determine your security needs and match those needs with the way your provider has designed your applications. The techniques described here should help you in both cases.

This topic provides a basic approach to planning resource security. It introduces the main techniques and shows how you can use them. The methods described here will not necessarily work for every company and every application. Consult your programmer or application provider as you plan resource security.

Review these topics to help you plan resource security:
- Determining your objectives for your resource security
- Understanding types of authority
- Planning security for application libraries
- Determining ownership of libraries and objects
- Grouping objects
- Protecting printer output
- Protecting workstations
- Summary of resource security recommendations
- Planning your application installation

What forms do you need?

Make copies of the following forms and fill them in as you read this topic. Work through the entire process for one application and then repeat the process for each additional application.

Table 33. Planning forms needed to plan resource security

Form name	Number of copies needed
Authorization List Form	Several

Table 33. Planning forms needed to plan resource security (continued)

Form name	Number of copies needed
Printer Output and Workstation Security Form	One

Add information to the following forms, with which you have worked previously:

Table 34. Planning forms that will be changed

Form name	Prepared in
Library Description Form	Describing library information
User Group Description Form	Planning group profiles

Refer to these forms, which you prepared previously:

Table 35. Planning forms needed to complete resource security

Form name	Prepared in:
Library Description form	Drawing an application diagram and Identifying user groups
Application Description Form	Describing application information
Individual User Profile Form	Choosing values for each user
User Group Identification Form	Identifying user groups
System Responsibilities Form	Determining who should be responsible for system functions
Physical Security Planning Form	Planning physical security

Determining your objectives for your resource security

To begin to plan resource security, you must first understand your objectives. iSeries provides flexible implementation of resource security. It gives you the power to protect critical resources exactly the way you want. But resource security also introduces additional overhead to your applications. For example, whenever an application needs an object, the system must check the user's authority to that object. You must balance your need for confidentiality against the cost of performance. As you make resource security decisions, weigh the value of security against its cost.

To prevent resource security from degrading the performance of your applications, follow these guidelines.

- Keep your resource security scheme simple.
- Secure only those objects that you need to secure.
- Use resource security to supplement, not replace, the other tools for protecting information, such as:
  - Limiting users to specific menus and applications.
  - Preventing users from entering commands (limited capabilities in user profiles).

Begin your resource security planning by defining your objectives. You can define your security objectives on either the Application Description form or Library Description form.

The form that you use depends on how your information is organized in libraries.

You may want to review an example of JKL Toy Company' security objectives before reviewing the types of authorities that you can use for resource security.

Example: JKL Toy Company's security objectives

Sharon Jones at the JKL Toy Company used the Library Description form to describe the security requirements for the Customer Records library (CUSTLIB):

Table 36. JKL Toy Company's Library Description form: Security objectives example

Library Description form	Part 1 of 2
Define the security objectives for the library, such as whether any information is confidential:	`Today, everyone in the company is allowed to look at customer information and at customer orders.  To protect the accuracy of information, we should control who is allowed to change it.`

Sharon used the Application Description form for the Contracts and Pricing application to describe security objectives for the whole application.

Table 37. JKL Toy Company's Application Description form: Security objectives example

Application Description form	Part 1 of 2
Define the security objectives for the library, such as whether any information is confidential:	`Information about contracts and special pricing is confidential. Only a few people are authorized to see and change it:` • `The Sales and Marketing personnel and all managers need to create, change, and analyze contracts. They need to use both the files and the programs.` • `The Order Processing personnel change contracts and view prices indirectly when entering and shipping orders. They are not allowed to look at contracts and prices except when they enter or change an order.`

Write your security objectives for your application on either the Application Description form or the Library Description form. You can then review the types of authorities that you can use to plan resource security.

Understanding the types of authority

After you have determined your objectives for your resource security and recorded your decisions on the Library Description form, you can begin to plan types of authority. Resource security defines how users have access to objects on the system.

Authority means how someone is authorized to use an object. For example, you may have the authority to view information or to change information on the system. The system provides several different authority types. IBM groups these authority types into categories, called **system-defined authorities**, which meet the needs of most people. The table below lists the categories and tells how they apply to securing files and programs.

Note: Refer to the tables below when you plan authorities.

Table 38. System-defined authorities

Authority name	Operations allowed for files	Operations not allowed for files	Operations allowed for programs	Operations not allowed for programs
*USE	View information in the file.	Change or delete any information in the file. Delete the file.	Run the program.	Change or delete the program.

Table 38. System-defined authorities (continued)

Authority name	Operations allowed for files	Operations not allowed for files	Operations allowed for programs	Operations not allowed for programs
*CHANGE	View, change, and delete records in the file.	Delete or clear the entire file.	Change the description of the program.	Change or delete the program.
*ALL	Create and delete the file. Add, change, and delete records in the file. Authorize others to use the file.	None	Create, change, and delete the program. Authorize others to use the program.	Change the owner of the program, if the program adopts authority.
*EXCLUDE[1]	None	Any access to the file.	None	Any access to the program.
1 *EXCLUDE overrides any authorities that you grant to the public or through a group profile.				

Understanding how object authority and library authority work together

To design simple resource security, try to plan security for entire libraries. To do this, you need to understand how the system-defined authorities apply to libraries, which the table below shows:

Table 39. System-defined authorities for libraries

Authority name	Operations allowed	Operations not allowed
*USE	• For objects in the library, any operation allowed by the authority to the specific object. • For the library, view descriptive information.	• Add new objects to the library. • Change the library description. • Delete the library.
*CHANGE	• For objects in the library, any operation allowed by the authority to the specific object. • Add new objects to the library. • Change the library description.	• Delete the library.
*ALL	• Everything allowed with change. • Delete the library. • Authorize others to the library.	• None

You also need to understand how library and object authority work together. The table below gives examples of authorities that are required for both an object and the library:

Table 40. How library authority and object authority work together

Object type	Operations	Object authority needed	Library authority needed
File	Change data	*CHANGE	*USE
File	Delete the file	*ALL	*USE
File	Create the file	*ALL	*CHANGE
Program	Run the program	*USE	*USE
Program	Change (recompile) the program	*ALL	*CHANGE
Program	Delete the program	*ALL	*USE

Directory authority is similar to library authority. You need authority to all the directories in the path name for an object in order to access the object.

Now you are ready to plan security for application libraries.

Planning security for application libraries

After you have determined your objectives for your resource security, you can begin planning security for application libraries. Choose one of your application libraries to work with as you follow the process described here. If your system stores files and programs in separate libraries, choose a library that contains files. When you finish the topic, repeat these steps for your remaining application libraries.

Review the information that you gathered about your the applications and libraries:
- Application Description form
- Library Description form
- User Group Description form for any groups that need the library
- Your diagram of applications, libraries, and user groups

Think about which groups need the information in a library, why they need it, and what they need to do with it.

Determining the contents of the library

Application libraries contain the important application files. They may also contain other objects, most of which are programming tools to make the application work properly, such as:
- Work files
- Data areas and messages queues
- Programs
- Message files
- Commands
- Output queues

Most of the objects, other than files and output queues, do not represent a security exposure. They usually contain small amounts of application data, often in a format that is not easily intelligible outside the programs. You can list names and descriptions of all the objects in a library by using the Display Library command. For example, to list contents of the CONTRACTS library: `DSPLIB LIB(CONTRACTS) OUTPUT(*PRINT)`

Next you need to decide what public authority you want to have for application libraries and program libraries.

Deciding public authority to application libraries

For purposes of resource security, **the public** means anyone you authorize to sign on to your system. **Public authority** allows a user access to an object if you have not any other more specific, access. In addition to deciding public authority for objects already in the library, you can specify the public authority for any new objects added to the library later. To do this, you use the **Create Authority (CRTAUT)** parameter. Usually, public authority to library objects and library create authority for new objects should be the same.

The QCRTAUT (Create Authority) system value determines the system-wide public authority for new objects. IBM ships the QCRTAUT system value with *CHANGE. Avoid changing QCRTAUT, because many system functions use it. If you specify *SYSVAL for the Create Authority (CRTAUT) of an application library, it uses the QCRTAUT system value (*CHANGE).

Use public authority as much as possible, for both simplicity and good performance. To determine what public authority to a library should be, ask these questions:

- Should everyone in the company have access to most of the information in this library?
- What kind of access should people have to the majority of the information in this library?

Concentrate on decisions for the majority of the people and the majority of the information. Later, you will learn how to deal with the exceptions. Planning resource security is often a circular process. You may discover that you need to make changes to public authority after considering the requirements for specific objects. Try several combinations of public and private authority to both objects and libraries before you choose one that meets your security and performance needs.

Ensuring adequate authority

*CHANGE authority to objects and *USE authority to a library are adequate for most application functions. However, you need to ask your programmer or application provider some questions to determine if certain application functions require more authority:

- Are any files or other objects in the library deleted during processing? Are any files cleared? Are members added to any files? Deleting an object, clearing a file, or adding a file member requires *ALL authority to the object.
- Are any files or other objects in the library created during processing? Creating an object requires *CHANGE authority to the library.

You may want to review an example of the choices that Sharon made for authorities to objects before deciding public authority to program libraries.

Example: JKL Toy Company's library description form:

Sharon Jones reviewed the security objectives for the Customer Records library, as well as information about the applications and departments that use customer information. She made notes about her conclusions:

- `Every department, except the Warehouse and Manufacturing departments, need to change customer information.`
- `All the users in the Warehouse and Manufacturing departments have user profiles with Limit capabilities (Yes), and they are restricted to certain menus or programs. Their menus allow them to view customer information, but not change it.`
- `Public authority for the objects in Customer Records library can be set to *CHANGE. Menu restrictions prevent unauthorized people from changing customer information. However, this should be evaluated again if other departments are added to the system later.`

This is an example of a relaxed approach to information. In this case, the exceptions are handled through user profiles, rather than by using authority restrictions. Sharon filled out the public authority part of the Library Description form for the Customer Records library (CUSTLIB).

Table 41. JKL Toy Company's Library Description form—Part 1: Customer Records example

Library name: CUSTLIB	Descriptive name (text): Customer Records
Public authority to the library:	*USE
Public authority to objects in the library:	*CHANGE
Public authority for new objects (CRTAUT):	*CHANGE

Sharon Jones discovered that some temporary files in the Customer Records library are cleared during month-end processing of the Accounts Receivable application. She chose to handle the authority for those

files individually, rather than taking the risk that other objects in the library might be accidentally deleted. For all other processing activity, *CHANGE authority is sufficient.

Even though only a few people run month-end processing, Sharon did not feel that the temporary files posed any security risk. She decided to give the public *ALL authority to those files, rather than giving that authority only to the people who run month-end. The table below shows the second part of the Library Description form for the Customer Records library:

Table 42. JKL Toy Company's Library Description form—Part 2: Customer Records example

List Specific Authorities for Library Objects				
Group profile or user profile	Object name	Object type	Authority needed	Authorization list
PUBLIC	ARFILE01	*FILE	*ALL	
PUBLIC	ARFILE02	*FILE	*ALL	
PUBLIC	ARFILE03	*FILE	*ALL	

You can now decide public authority to program libraries you want to have.

Deciding public authority to program libraries

Often, application programs are kept in a separate library from files and other objects. You are not required to use separate libraries for applications, but many programmers use this technique when they design applications. If your application has separate program libraries, you need to decide the public authority to those libraries. You can use *USE authority to both the library and the programs in the library to run programs sufficiently, but program libraries may have other objects that require additional authority. Ask your programmer a few questions:

- Does the application use data areas or message queues to communicate between programs? Are they in the program library? *CHANGE authority to the object is required for handling data areas and message queues.
- Are any objects in the program library, such as data areas, deleted during processing? *ALL authority to an object is required to delete the object.
- Are any objects in the program library, such as data areas, created during processing? *CHANGE authority to the library is required to create any new objects in the library.

Fill in all of the resource security information on both parts of the Library Description form except the library owner and the authorization list column. You then can determine ownership of libraries and objects.

You may want to review the following two examples of how Sharon Jones determined the authority to program libraries. In the first example, Sharon decided that a non-restrictive approach was fine for the Customer Order program library. The second example shows a more restrictive approach that Sharon used for the Accounts Receivable program library.

Example: JKL Toy Company's library description form—non-restrictive approach: Sharon Jones investigated the Customer Order Program library and made these notes:

- `One message queue, COMSGQ01, is used to communicate between programs.`
- `The message queue is cleared but never deleted.  *CHANGE authority to the message queue is sufficient.`

Sharon decided to give *USE authority to all the objects in the program library and define the COMSGQ01 message queue separately. The two tables below show her Library Description form for the COPGMLIB library:

Table 43. JKL Toy Company's Library Description form: Program library example

Library Description form	Part 1 of 2
Library name: COPGMLIB	Descriptive name (text): Customer Order Program Library
Public authority to the library: *USE Public authority to objects in the library: *USE Public authority for new objects (CRTAUT): *USE Library owner:	

Table 44. JKL Toy Company's Library Description form: Program library example

Library Description form				Part 2 of 2
List authorities to individual objects in the library				
Group Profile or User Profile	Object Name	Object Type	Authority Needed	Authorization Lists
PUBLIC	COMSGQ01	*MSGQ	*CHANGE	

Using authority to a program to control access

Although most people at the JKL Toy Company are allowed to change customer information, only a few people are allowed to set credit limits for customers. Credit limits are stored in the customer master file (CUSTMAS), but they are changed with a separate program called ARPGM12 in the ARPGMLIB. Sharon can restrict that program to prevent unauthorized people from changing credit limits. The tables below show the Library Description form for the ARPGMLIB:

Table 45. JKL Toy Company's Library Description form: Individual authority example

Library Description form	Part 1 of 2
Library name: ARPGMLIB	Descriptive name (text): Accounts Receivable Program Library
Public authority to the library: *USE Public authority to objects in the library: *USE Public authority for new objects (CRTAUT): *USE Library owner:	

Table 46. JKL Toy Company's Library Description form: Individual authority example

Library Description form				Part 2 of 2
List authorities to individual objects in the library				
Group Profile or User Profile	Object Name	Object Type	Authority Needed	Authorization Lists
PUBLIC	ARPGM12	*PGM	*EXCLUDE	
JACOBS	ARPGM12	*PGM	*USE	
DAVISP	ARPGM12	*PGM	*USE	
SMITHJ	ARPGM12	*PGM	*USE	

You may want to review a restrictive example that uses adopted authority before you begin determining ownership of libraries and objects.

Example: JKL Toy Company's library description form—restrictive approach: The examples so far have shown a relaxed approach to security, where most people have access to the information in a library. Contract and pricing information at the JKL Toy Company is considered confidential and requires a restrictive approach. Fortunately, all this information is stored in a separate library. The programs to update contracts and pricing are also in a special library.

Sharon reviewed the security objectives for the Contracts and Pricing application (see Determining your objectives for your resource security). She also reviewed the Application Description form and the Library Description forms. Sharon felt it would be difficult to meet their security objectives for the application. She made some notes and discussed the problem with their application provider:

- Sales and Marketing personnel and the managers need to create and change contracts. They need to use both the files and the programs.
- Order Processing personnel change contracts and view prices indirectly when entering and shipping orders, but are not allowed to view contracts and prices in any other way. However, they will be using Query to create their own reports about customers and orders. If they are given authority to the Contracts and Pricing files, they could create Query programs to view or print them.

The application provider for the JKL Toy Company suggested using the adopted authority feature of security to solve this problem. **Adopted authority** allows a user to adopt the authority of the program's owner while the program runs. The user does not need authority to the object.

The diagram below shows an example of how adopted authority works. Karen Richards (RICHARDK) in the Order Processing department does not normally have authority to use the Contracts file. However, when she enters orders, she needs to check and update contract balances. The order entry program that works with contract balances (COPGM04) adopts the authority of the OWNCP profile. While Karen is running the COPGM04 program, she has authority to use the contracts file:
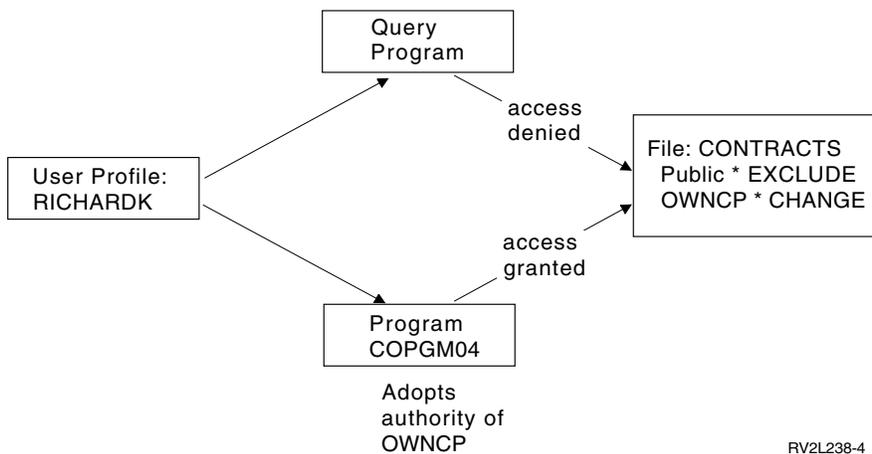
See the topic, "Determining ownership of libraries and objects" for details on object ownership. Your application provider or programmer can specify that the program adopts the owner's authority when the create (compile) the program, or a programmer can specify adopted authority for the program using the Change Program (CHGPGM) command. Make sure you understand all the functions of the program before using this technique.

Sharon decided to use the adopted authority function to give those outside the Sales and Marketing department access to Contract and Pricing files. She also determined that *CHANGE access was sufficient for all the objects used by the Contracts and Pricing application. The table below shows the Library Description form for the Contracts library:

Table 47. JKL Toy Company's Library Description form: Restrictive authority example

Library Description form	Part 1 of 2
Library name: CONTRACTS	Descriptive name (text): Contracts and Pricing Library
Public authority to the library: *EXCLUDE Public authority to objects in the library: *CHANGE Public authority for new objects (CRTAUT): *CHANGE Library owner:	

Table 48. JKL Toy Company's Library Description form: Restrictive authority example

Library Description form				Part 2 of 2
List authorities to individual objects in the library				
Group Profile or User Profile	Object Name	Object Type	Authority Needed	Authorization Lists
DPTSM	CONTRACTS	*LIB	*USE	
DPTMG	CONTRACTS	*LIB	*USE	

You do not need to restrict authority to objects in the library, because you restrict access to the library itself. Also, Sharon gave authority to the managers and the Sales and Marketing department. She used group authority, instead of giving authority to each individual in the departments.

Note: A knowledgeable programmer who has access to a library may be able to retain access to objects in the library even after you have revoked authority to the library. If a library contains objects with high security requirements, restrict the objects and the library for complete protection.

You may want to review a non-restrictive example that uses public authority before you begin determining ownership of libraries and objects.

Determining ownership of libraries and objects

After you plan security for application libraries, you can decide ownership of libraries and objects. Each object is assigned an owner when it is created. The owner of the object automatically has all authority to the object, which includes authorizing others to use the object, changing the object, and deleting it. The security officer can perform these functions for any object on the system.

The system uses the profile of the object owner to track who has authority to the object. The system completes this function internally. This may not affect the user profile directly. However, if you do not plan object ownership properly, some user profiles can become very large.

When the system saves an object, the system also saves the name of the owning profile with it. The system uses this information if it restores the object. If the owning profile for a restored object is not on the system, the system transfers ownership to an IBM-supplied profile called QDFTOWN.

Recommendations

The recommendations below apply in many, but not all, situations. After reviewing the recommendations, discuss your ideas for object ownership with your programmer or application provider. If you purchase applications, you may not be able to control what profile owns libraries and objects. The application may be designed to prevent changes of ownership.

- Avoid using an IBM-supplied profile, such as QSECOFR or QPGMR, as an application owner. These profiles own many objects in IBM-supplied libraries and are already very large.

- Normally, a group profile should not own an application. Every member in the group has the same authority as the group profile, unless you specifically assign lower authority. In effect, you would be giving every member of the group complete authority to the application.
- If you plan to delegate responsibility for control of applications to managers in various departments, those managers could be the owners of all the application objects. However, the manager of an application might change responsibilities. If that is the case, then you would transfer ownership of all the application objects to a new manager.
- Many people use the technique of creating a special owner profile for each application with the password set to *NONE. The owning profile is used by the system to manage authorities for the application. The security officer (or someone with that authority) performs the actual management of the application or it is delegated to managers with *ALL authority to particular applications.

Decide what profiles should own your applications. Enter the owner profile information on each Library Description form.

You may want to review an example of how JKL Toy Company determined application ownership before you begin deciding ownership and access for user libraries.

Example: JKL Toy Company's application ownership

Sharon Jones decided to create a special owner profile for each application. She and Ken Harrison, the backup security officer, will take responsibility for managing application security. Later, if the company's security requirements become more complex, Sharon can delegate some responsibility for managing authorities to department managers.

Sharon added a new entry to her Naming Conventions form:

Table 49. JKL Toy Company's Naming Conventions form: Owner profile example

Type of object	Naming convention
Owner Profile	An owner profile will be created for each application. It will own all the application libraries and the objects in them. The owner profile will be named OWN plus the application abbreviation. The Inventory Control owner profile will be OWNIC.

Sharon decided to begin the owner profile name with OWN so that all the owner profiles would appear together on displays and lists.

Sharon assigned owners to all the application libraries and entered that information on the Naming Conventions forms. The only library that had more than one possible application owner was the Customer Records library. Because the Accounts Receivable application is used to create new customers and set credit limits, Sharon decided it should own the customer files. These are the owners she assigned:

Library Name	Owner Name
ICPGMLIB	OWNIC
ITEMLIB	OWNIC
CONTRACTS	OWNCP
CPPGMLIB	OWNCP
COPGMLIB	OWNCO
CUSTLIB	OWNAR
ARPGMLIB	OWNAR

You can now decide ownership and access for your user libraries.

Deciding ownership and access for user libraries

If your system has the IBM Query for iSeries licensed program or another decision support program, your users need a library for storing the query programs they create. Normally, this library is the **current library** in the user profile. For more information on creating a current library for each user, see "Choosing values that affect sign on." Sharon Jones plans to use current libraries for the Sales and Marketing department and group libraries for the other departments:

- Sales and Marketing people will be heavy users of Query. Each user should have a private library. Otherwise, they would have to worry about what to name their queries, and they might accidentally delete each other's programs.
- To start, other departments will have group libraries. If they create many Query programs, we can consider individual libraries.

If a user belongs to a group, you use a field in the user profile to specify whether the user or the group owns any objects created by the user. If the user owns the objects, you can specify what authority the group members have to use the objects. You can also specify whether the group's authority is primary group authority or private authority. Primary group authority may provide better system performance. Sharon made some additional notes about user libraries:

- Sales and Marketing people should own the objects they create, rather than having the group own them. They do not need to change each other's query programs.
- Everyone in the group should be able to run each other's Query programs, which means the group gets *USE authority to any objects created by a group member.
- The group's authority should be primary group authority.
- The public should not have access to these libraries. Sales and Marketing people may have output files from their queries. Those files might contain confidential data.
- For the other departments, the group will own the group library and everything created in the library. This means any member of the group can change or delete anything in the library. If this causes problems, we may have to try another method.

The table below shows the Individual User Profile Form for the Sales and Marketing department that uses objects owned by the user:

Table 50. JKL Toy Company's Individual User Profile Form: Objects owned by the user example

Group profile names: DPTSM	
Owner of objects created: *USRPRF	Group authority to objects created: *USE
Group authority type: *PGP	

The table below shows the Individual User Profile Form for a department that has objects owned by the group:

Table 51. JKL Toy Company's Individual User Profile Form: Objects owned by the group example

Group profile names: DPTxx	
Owner of objects created: *GRPPRF	Group authority to objects created:

The **Group authority to objects created** field is not used if the owner of objects created is the group. Group members automatically have *ALL authority to any objects created.

Decide who should own and have access to user libraries. Enter your choices in the **Owner of objects created** and **Group authority over objects** fields on the Individual User Profile form. Now you are ready to begin grouping objects.

Grouping objects

After you have determined ownership of libraries and objects, you can begin grouping objects on the system. To simplify managing authorities, use an authorization list to group objects with the same requirements. You can then give the public, group profiles, and user profiles authority to the authorization list rather than to the individual objects on the list. The system treats every object that you secure by an authorization list the same, but you can give different users different authorities to the entire list.

An authorization list makes it easier to reestablish authorities when you restore objects. If you secure objects with an authorization list, the restore process automatically links the objects to the list.

You can give a group or user the authority to manage an authorization list (*AUTLMGT). Authorization list management allows the user to add and remove other users from the list and to change the authorities for those users.

Recommendations
- Use authorization lists for objects that require security protection and that have similar security requirements. Using authorization lists encourages you to think about categories of authority rather than individual authorities. Authorization lists also make it easier to restore objects and to audit the authorities on your system.
- Avoid complicated schemes that combine authorization lists, group authority, and individual authority. Choose the method that best suits the requirement, rather than using all of the methods at the same time.

You will also need to add the naming convention for authorization lists to your Naming Conventions form.

Once you have prepared an Authorization List form, go back and add that information to your Library Description form. Your programmer or application provider might have already created authorization lists. Be sure to check with them.

You may find it useful to review an example of how Sharon Jones of JKL Toy Company planned authorization lists before you plan security for printers and printer output.

Example: JKL Toy Company's authorization list form

Sharon reviewed the Library Description for the Customer Records library and decided to create an authorization list for the files that are cleared at the end of each month. Even though only three files are cleared, Sharon decided to use an authorization list to simplify managing the authorities. If other files are added to the month-end process later, she can simply secure those files with the authorization list. Sharon decided to exclude the public from the files to prevent unintentional problems during month-end processing. She gave *ALL authority only to the users who run the processing. Rose Willis, the system operator in the evening, may need to view information about the files to check month-end processing. She needs *USE authority.

The table below shows the naming convention that Sharon used for authorization lists:

Table 52. JKL Toy Company's Naming Conventions form: Authorization List example

Naming Conventions form	
Prepared by: Sharon Jones	Date: 9/5/99
Type of Object	**Naming Convention**

Table 52. JKL Toy Company's Naming Conventions form: Authorization List example (continued)

Authorization Lists	For lists that secure objects from one library, use part of the library name plus LST and a number. A list for objects in CUSTLIB would be CUSTLST1. For a list securing objects from more than one library, use an application abbreviation if possible: ARLST1. If the list applies to multiple applications, select any meaningful name. The description of the list should state its main purpose.

The table below shows the Authorization List form for the CUSTLIB library. Sharon prepared this form using the information from the Library Description form:

Table 53. JKL Toy Company's Authorization List Plan: example

Authorization List form					
Authorization List Name: CUSTLST1					
Description: Files cleared during the month-end processing.					
List the objects which the list secures					
Object name	Object type	Object library	Object name	Object type	Object library
ARFILE01	*FILE	CUSTLIB	ARFFILE02	*FILE	CUSTLIB
ARFILE03	*FILE	CUSTLIB			
List groups and users who have access to the list					
Group or user	Type of access allowed	List management?	Group or user	Type of access allowed	List management?
PUBLIC	*EXCLUDE	no	ROSSG	*ALL	no
SMITHJ	*ALL	no	JONESS	*ALL	yes
WILLISR	*USE	no			

Sharon also added the authorization list information to the Library Description form for the CUSTLIB library:

Library Description form				Part 2 of 2
Prepared by: Sharon Jones			Date: 9/9/99	
Library name: CUSTLIB				
List Specific Authorities for Library Objects				
Group Profile or User Profile	Object Name	Object Type	Authority Needed	Authorization List
PUBLIC	ARFILE01	*FILE	*AUTL	CUSTLST1
PUBLIC	ARFILE02	*FILE	*AUTL	CUSTLST1
PUBLIC	ARFILE03	*FILE	*AUTL	CUSTLST1

Notice that the public authority for each file must be changed to *AUTL for the system to use the authorization list to determine public authority.

Look at the group and individual authorities on your Library Description forms. Decide if using authorization lists is appropriate. If so, prepare Authorization List forms and update the Library Description forms with the authorization list information. You can then plan security for printers and printer output.

Planning security for printers and printer output

After you group your objects, you need to plan how to protect printer output. You have developed plans to protect information stored on your system. You also need a plan to protect confidential information while it is printing or waiting to print. Check your Physical Security Plan for printers that your company uses for confidential output.

When you run a program that prints a report, the report usually does not go directly to a printer. The program creates a copy of the report, called a **spooled file** or **printer output**. The system stores the spooled file in an object called an **output queue** until a printer is available. When the output queue contains printer output, you can view the report at your workstation. You can also hold it or direct it to a specific printer.

Spooling makes it easier to schedule printing jobs and to share printers. Spooling also helps you protect confidential output. You can create one or more special output queues to hold confidential output and restrict who can view and manage those output queues. You can also control when confidential output is sent from the queue to a printer.

Complete the Printer Output and Workstation Security form as you work through this topic.

When you create a special output queue, you can specify several parameters that relate to security:

- **Display Data (DSPDTA) Parameter**: The DSPDTA parameter of an output queue determines whether a user can view, send, or copy a spooled file that another user owns.
- **Authority to Check (AUTCHK) Parameter**: The AUTCHK parameter of an output queue determines whether a user can change or delete a spooled file that another user owns.
- **Operator Control (OPRCTL) Parameter**: The OPRCTL parameter of an output queue determines whether users with *JOBCTL special authority (or *SYSOPR user class) are allowed to control the output queue.

The output queue parameters, the user's authority to the output queue, and the user's special authority work together to determine the functions a user can perform on spooled files in an output queue. The table below shows what combinations allow users to perform different functions:

Printing Functions	Output Queue Parameters			Output Queue Authority	Special Authority
	DSPDTA	AUTCHK	OPRCTL		
Add spooled file to queue [1]	Any	Any	Any	*READ	None
	Any	Any	*Yes	Any	*JOBCTL
View list of spooled files (WRKOUTQ command)[2]	Any	Any	Any	*READ	None
	Any	Any	*Yes	Any	*JOBCTL
Display, copy, or send spooled files (DSPSPLF, CPYSPLF, SNDNETSPLF, SNTCPSPLF)[2]	*YES	Any	Any	*READ	None
	*NO	*DTAAUT	Any	*CHANGE	None
	*NO	*OWNER	Any	Owner[3]	None
	*YES	Any	*Yes	Any	*JOBCTL
	*NO	Any	*Yes	Any	*JOBCTL
	*OWNER[5]	Any	Any	Any	Any
Change, delete, hold, release spooled file (CHGSPLFA, DLTSPLF, HLDSPLF, RLSSPLF)[2]	Any	*DTAAUT	Any	*CHANGE	None
	Any	*OWNER	Any	Owner[3]	None
Change, clear, hold, and release output queue (CHGOUTQ, CLROUTQ, HLDOUTQ, RLSOUT)[2]	Any	*DTAAUT	Any	*CHANGE	None
	Any	*OWNER	Any	Owner[3]	None
	Any	Any	*YES	Any	*JOBCTL

| Start a writer for the queue (STRPRTWTR, STRRMTWTR)[2] | Any | *DTAAUT | *Any | *CHANGE[4] | None |
| | Any | Any | *YES | Any[4] | *JOBCTL |

1	This is the authority required to direct your output to the output queue.
2	Using these commands or equivalent options from a display.
3	You must be the owner of the output queue.
4	Also requires *USE authority to the printer device description.
5	You must be the owner of the spooled file or have *SPLCTL special authority to work with this command.

Review the printer portion of your Physical Security Plan. Fill in the output queue section of the Printer Output and Workstation Security form as you work through this topic.

You may find it useful to review an example of how Sharon Jones of the JKL Toy Company determined the values for these output queue parameters before you plan resource security for workstations.

Example: JKL Toy Company's output queue and workstation security form—output queue portion

The Sales and Marketing Department at the JKL Toy Company has two requirements for confidential printing:

- Preliminary price lists are printed when price changes are being planned. No one outside the Sales and Marketing Department, except company managers, can see this information.
- Contracts are confidential while they are being negotiated. A rough draft of the contract can be seen only by the person negotiating the contract, not by other members of the Sales and Marketing Department.

Sharon decided to create two special output queues:

PRICEQ

To be used for preliminary price lists. Anyone in the Sales and Marketing Department can perform any functions on this output queue. No one outside the department can use the output queue, including the system operators. PRICEQ is in the CONTRACTS library.

NEWCP

To be used for printing contracts that are being negotiated. The output queue is shared by the members of the Sales and Marketing Department, but only the person who creates a spooled file on the output queue can control that file. NEWCP is in the CONTRACTS library.

The table below shows the Output Queue and Workstation Security form that Sharon prepared for these output queues:

Table 54. JKL Toy Company's Output Queue and Workstation Security form: Printer Output Queue example

List the parameters for restricted output queues:				
Output Queue Name	Output Queue Library	Display Any File (DSPDTA)	Authority to Check (AUTCHK)	Operator Control (OPRCTL)
PRICEQ	CONTRACTS	*YES	*DTAAUT	*NO
NEWCP	CONTRACTS	*NO	*OWNER	*NO

The topic, Deciding public authority to program libraries contains an example that shows the authority for the CONTRACTS library at the JKL Toy Company. Only managers and members of the Sales and Marketing Department have access to the library. Public authority for objects in the library (including these output queues) is *CHANGE.

Because the AUTCHK parameter on the NEWCP output queue is *OWNER, only the owner of a spooled file can work with that file (see Authority Required to Perform Printing Functions table above). This prevents members of the Sales and Marketing Department from printing each other's new contracts or viewing them in the output queue.

After you plan printer output queue security, you can plan security for workstations.

Planning security for workstations

After planning resource security for printers and printer output, you can begin planning workstation security. On your Physical Security Plan, you listed workstations that represent a security risk because of their location. Use this information to determine which workstations you need to restrict.

You can encourage the people who use these workstations to be particularly aware of security. They should sign off whenever they leave their workstations. You may want to record your decision about sign off procedures for vulnerable workstations in your security policy. You can also limit which functions can be performed at those workstations to minimize the risks.

The easiest method for limiting function at a workstation is to restrict it to user profiles with limited function. Sharon Jones used this technique for the Warehouse Department at JKL Toy Company. Sharon allowed Ray Wagner and Janice Ames, who work on the loading dock, to run only the inventory receiving program. Also Sharon made them the only users that are allowed to sign on to the workstation on the loading dock.

You may choose to prevent people with security officer or service authority from signing on at every workstation. If you use the QLMTSECOFR system value to do this, people with security officer authority can sign on only at specifically authorized workstations.

Prepare the workstation portion of the Output Queue and Workstation Security form

You may want to review an example of how Sharon planned security for workstations as you prepare the workstation portion of the Output Queue and Workstation Security form. You should also review a list of resource security recommendations to ensure that your resource security plan is simple and complete. After you have reviewed the example and the recommendations you can begin planning your application installation.

Example: JKL Toy Company's output queue and workstation security form—workstation portion

Sharon Jones reviewed her Physical Security Plan to determine which workstations posed security risks. At the JKL Toy Company, for example, people outside the company can easily access the workstations on the loading dock and at the remote sales office. Sharon indicated on the Physical Security Plan that these workstations posed potential security risks.

The easiest method for limiting function at a workstation is to restrict it to user profiles with limited function. Sharon Jones used this technique for the Warehouse Department at JKL Toy Company. Sharon allowed Ray Wagner and Janice Ames, who work on the loading dock, to run only the inventory receiving program. Also Sharon made them the only users that are allowed to sign on to the workstation on the loading dock.

Sharon reevaluated her choice for the QLMTSECOFR system value. She decided she would set it to 1(Yes) as additional protection for vulnerable workstations at the loading dock and the remote sales office.

The table below shows the workstation portion of the Output Queue and Workstation Security form that Sharon prepared.

Table 55. JKL Toy Company's Output Queue and Workstation Security form: Workstation example

Security officer workstations:	
If you limit the security officer to specific workstations (system value QLMTSECOFR is yes), list below the workstations authorized for the security officer and anyone with *ALLOBJ authority: `All workstations except those listed below.`	
List below the authorities for restricted workstations:	
Workstation Name	Groups or users who are authorized (*CHANGE authority)
DSP10	AMESJ, WAGNERR
DSP11	AMESJ, WAGNERR
RMT01	UNGERJ, BELLB
RMT02	UNGERJ, BELLB

You may want to review a summary of resource security recommendations before planning your application installation.

Summary of resource security recommendations

After you finish planning workstation security, you can review the following resource security recommendations. The iSeries system offers many options for protecting the information on your system. This gives you the flexibility to design the resource security plan that is best for your company. But this wealth of options can also be confusing.

Using the JKL Toy Company as an example, this topic has tried to demonstrate a basic approach to planning resource security that uses these guidelines:
* Move from the general to the specific:
    – Plan security for libraries. Deal with individual objects only when necessary.
    – Plan public authority first, followed by group authority, and individual authority.
* To improve performance and simplify backup and recovery, define specific security only for objects whose security requirements cannot be satisfied using public authority.
* Make the public authority for new objects in a library (CRTAUT) the same as the public authority you defined for the majority of existing objects in the library.
* Try not to give groups or individuals less authority than the public has. This diminishes performance, may lead to mistakes later, and makes auditing difficult. If you know that everyone has at least the same authority to an object that the public has, it makes planning and auditing security easier.
* Use authorization lists to group objects with the same security requirements. Authorization lists are simpler to manage than individual authorities and aid in recovery of security information.
* Create special user profiles as application owners. Set the owner password to *NONE.
* Avoid having applications owned by IBM-supplied profiles, such as QSECOFR or QPGMR.
* Use special output queues for confidential reports. Put the output queue in the same library as the confidential information.
* Limit the number of people who have security officer authority.
* Be careful when granting *ALL authority to objects or libraries. People with *ALL authority can accidentally delete things.

To ensure that you have planned successfully for setting up resource security, you should have gathered the following information:
* Fill in Part 1 and Part 2 of the Library Description forms for all your application libraries.
* On your Individual User Profile forms fill in the **Owner of objects created** and **Group authority over objects created** fields.

- On your Naming Conventions form describe how you plan to name authorization lists.
- Prepare Authorization List forms.
- Add authorization list information to your Library Description forms.
- Prepare an Output Queue and Workstation Security form.

Now you are ready to plan your application installation.

Planning your application installation

To finish planning resource security, you need to prepare for your application installation. The following topics will help you plan ownership and authority to your applications after you install them. The methods described here may not work for all applications. Consult your programmer or application provider for help with developing a good installation plan.

If you plan to acquire an application from an application provider, use this information to plan the security activities you need to do before and after you load the application libraries.

If you plan to install an application that programmers developed on your own system, use this information to plan the security activities necessary to move the application from test to production status.

Work through the steps with one application. Then go back and prepare Application Installation forms for any additional applications.

What forms are needed?

Make a copy of the following forms and fill it in as you work through this topic:

Table 56. Planning forms needed to plan application installation

Form name	Number of copies needed
Application Installation form	One per application

Use these forms, on which you have worked previously to gather information for planning application installation:

Form name	Prepared in:
Library Description form	Describing library information
Authorization List form	Grouping objects

In the topic, Loading your applications you learn how to perform the steps needed to install your applications.

To plan your application installations, see the these topics:
- Determining user profiles and installation values for applications.
- Changing installation values.

Determining user profiles and installation values for applications

When you plan your application installation, you must first decide the user profiles and installation values for each application. Before you install an application that was created on another system, you may need to create one or more user profiles. The user profile that owns the application libraries and objects should exist on your system before you load the libraries on your system. Record the profiles you need to create for each library and what parameters the profiles need on the Application Installation form.

To determine the installation values necessary, ask your programmer or application provider the following questions and record their answers on the Application Installation form:

- What profile owns the application library?
- What profile owns the objects in the library?
- What is the public authority to the library (AUT)?
- What is the public authority for new objects (CRTAUT)?
- What is the public authority for objects in the library?
- What programs, if any, adopt the authority of the owner?

Find out whether your programmers or application provider have created any authorization lists for the application. Prepare an Authorization List form for each created authorization list or ask your programmer for information about the list.

You can determine whether you should change any installation values.

Changing installation values for applications

Compare the information from the Application Installation form with your resource security plan for the library on the Library Description form. If they are different, you need to decide what changes to make after the application is installed.

Changing application ownership

If your programmer or application provider has created a special profile to own the application libraries and objects, consider using that profile, even if it does not match your naming conventions. Transferring ownership of objects can take a long time and should be avoided.

If one of the IBM-supplied group profiles, such as QSECOFR or QPGMR, owns the application, you should transfer ownership to another profile after you install the application.

Sometimes programmers design applications to prevent changes in object ownership. Try to work within the restrictions and still meet your own requirements for managing security. However, if an IBM-supplied profile, such as QSECOFR, owns the application, you and your programmer or application provider need to develop a plan to change ownership. Ideally, you should change ownership before you install the application.

Changing public authority

When you save objects, you also save their public authority with them. When you restore an application library to your system, the library and all its objects will have the same public authorities they had when they were saved. This is true even if you saved the library on another system.

The CRTAUT value for a library (public authority for new objects) does not affect objects that are restored. They are restored with their saved public authority, regardless of the CRTAUT for the library.

You should change the public authority of libraries and objects to match your plan on the Library Description form.

You may want to review an example that shows how Sharon Jones of the JKL Toy Company planned application installation as you plan your application installation.

To ensure that you have planned your application installation completely, you should:

- Finish filling out your initial Application Installation form. Then go back and prepare forms for each additional application.

- Review all your forms and make sure they are complete. Make copies of your forms and keep them in a secure location until you have installed your system and your licensed programs.

After you finished these planning tasks, you are ready to set up your user security.

Example: JKL Toy Company application installation form: The JKL Toy Company purchased their Customer Orders and Accounts Receivable applications from an application provider. They hired an outside programmer to develop their Contracts and Pricing application and link it to the Customer Orders application.

Sharon Jones used the information from her Library Description forms to prepare an Application Installation form. The table below shows a copy of Sharon's Library Description form for the CUSTLIB: (See the topic "Describing library information.")

Table 57. JKL Toy Company's Library Description form: example

Library Description form	Part 1 of 2
Prepared by: Sharon Jones	Date: 9/9/99
Library name: CUSTLIB	Descriptive name (text): Customer Records Library
Briefly describe the function of this library: Holds all customer files, including orders and accounts.	
Define the security objectives for the library, such as whether any information is confidential: Today, we allow everyone in the company to look at customer orders. To protect the accuracy of information, we should limit who is allowed to change it.	
Public authority to the library: *USE Public authority to objects in the library: *CHANGE Public authority for new objects (CRTAUT): *CHANGE Library owner: OWNAR	

The table below shows the Application Installation form that Sharon prepared for the Customer Orders application. Notice that Sharon decided to use the owner profile created by the application provider. The profile COWNER will own both the file and the program libraries.

After the application is installed, Sharon should do the following:
- Change the public authorities for the libraries to match the resource security plan on her Library Description forms.
- Change the user class of the COWNER profile to *USER and remove any special authorities.
- Change the password of the COWNER profile to *NONE.

Table 58. JKL Toy Company's Application Installation form: example

Application Name: Customer Orders (CO)		Description: Enter, track, and ship orders.
List and explain any profiles that must be created to install the application: The library containing files is owned by a profile called COWNER. The program library is owned by QPGMR.		
Library Name: CUSTLIB		
	Before Installation	**After Installation**
Library owner	COWNER	COWNER
Object owner	COWNER	COWNER
Library public authority	*EXCLUDE	*USE
Object public authority	*ALL	*CHANGE

Table 58. JKL Toy Company's Application Installation form: example (continued)

Public authority for new objects	*CHANGE	*CHANGE
Library Name: COPGMLIB		
	Before Installation	**After Installation**
Library owner	QPGMR	COWNER
Object owner	QPGMR	COWNER
Library public authority	*EXCLUDE	*USE
Object public authority	*ALL	*CHANGE
Public authority for new objects	*CHANGE	*CHANGE

Now that you have finished the planning tasks, you are ready to set up user security next.

Setting up user security

This topic guides you through the tasks necessary to set up user security on your system by using the command line interface. If you are setting up a new system, you should complete these steps in sequence. The system uses information from each step as you proceed to the next step. To set up basic system security, you need to complete two sets of tasks. You must first define your user security, and then secondly, you must protect your resources on the system. The two tables below highlight each of the steps you must configure to set up user and resource security.

Note: You **MUST** complete all the steps to set up user security first, before you begin setting up resource security.

Table 59. Steps in Setting Up User Security

Step	What You Do in This Step	What Forms You Use
Setting up your overall environment	Set up initial system values and network attributes. Create a security officer user profile.	System Values Selection form
Setting system values for security	Set up additional system values.	System Values Selection form
Preparing basic security steps for loading your applications	Create owner profiles. Load your applications. Application libraries and objects should be on the system before you complete the remaining steps.	Application Installation form
Setting up user groups	Create job descriptions, group libraries, and group profiles.	User Group Description form
Setting up individual users	Create individual libraries and user profiles.	Individual User Profile form

Table 60. Steps in Setting Up Resource Security

Step	What You Do in This Step	What Forms You Use
Setting up ownership and public authority	Establish ownership and public authority for libraries and objects.	Application Installation form
Creating an authorization list	Create authorization lists.	Authorization List form
Setting up specific authorities	Set up access to libraries and individual objects.	Library Description form
Securing printer output	Protecting printer output by creating output queues and assigning output.	Output Queue and Workstation Security form

Table 60. Steps in Setting Up Resource Security (continued)

Step	What You Do in This Step	What Forms You Use
Securing workstations	Protecting workstations.	Output Queue and Workstation Security form

In addition to the topics listed in the above table, see the following topics for managing your system security:

* Testing security.
* Changing security information.
* Saving security information.
* Monitoring security.

Before you begin

If you are installing a new system, do these things before you start setting up security:

* Make sure your system unit and your devices are installed and working properly. If you do not plan to use iSeries naming for your devices, wait to attach your workstations and printers until after you change the system value that determines how devices are named (QDEVNAMING). Applying the new system values tells you when to attach the devices.
* Load any licensed programs you plan to use.

Setting up your overall environment

To begin setting up user security, you need to set up the overall environment for your users. In this topic, use the SETUP menu to set system values, and create your own user profile. You will also change user IDs and passwords for the Dedicated Service Tools (DST) profiles.

In the following procedures, you will find example command line screens that illustrate these steps. However, these do not show the entire screen. They show only the information necessary to complete the task.

What forms are needed?

Enter information from the System Values Selection form that you prepared in "Planning your overall security strategy."

To set up your overall environment, you need to complete these tasks:

1. Signing on to system.
2. Selecting the right assistance level.
3. Preventing others from signing on.
4. Entering system values for security.
5. Applying the new system values.
6. Creating a security officer profile

After you have completed the above steps, you must change Service Tool passwords to prevent someone from using them incorrectly. See Service Tools for details.

Signing on to the system

To begin setting up your system environment, you need to sign on to the system.

1. At the console, sign on as the security officer (QSECOFR). If you are signing on for the first time, use the password QSECOFR. Because the system ships this password as expired, the system will prompt you to change this password. You must change this password to successfully sign on.

2. Enter SETUP in the *Menu* field on the Sign On display.

Note: The SETUP menu is called the Customize Your System, Users, and Devices menu. This text refers to it as the SETUP menu throughout.

```
             Sign On
                          System  . . . . .
                          Subsystem . . . .
                          Display . . . . .

User  . . . . . . . . . . . . .   QSECOFR
Password  . . . . . . . . . . .   _____
Program/procedure . . . . . . .   _____
Menu  . . . . . . . . . . . . .   SETUP
Current library . . . . . . . .   _____
```
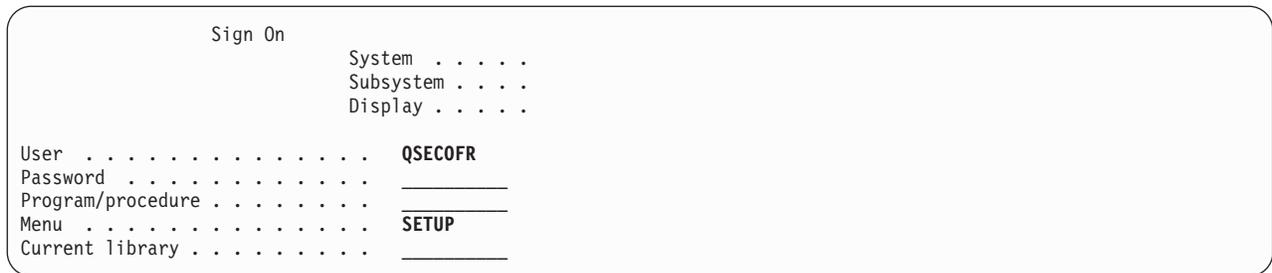
After you sign-on to the system, you must select the appropriate assistance level.

Selecting the right assistance level

After signing on to the system, you can choose the appropriate assistance level for users. The **assistance level** determines what version of a display you see. Many system displays have two different versions:

- A basic assistance level version, which contains less information and does not use technical terminology.
- An intermediate assistance level version, which shows more information and uses technical terms.

Some fields or functions are available only on a particular version of a display. The instructions tell you which version to use. To change from one assistance level to another, use **F21** (Select assistance level). **F21** is not available from all displays.

After you select your assistance level, you must prevent others from signing on to the system while you set up security.

Preventing others from signing on

After you select the right assistance level, you must prevent anyone else from signing on to the system. If you are concerned about people tampering with your system before you have a chance to secure it, you can prevent anyone from signing on at another workstation. This is optional. Do it only if you feel that temporary security is necessary:

1. From the SETUP menu, press **F9** to display a command line
2. On the command line, type GO DEVICESTS.
3. The screen shows the Device Status Tasks menu. If you see the Work with Configuration Status menu, use **F21** (Select assistance level) to change to basic assistance level.
4. Select option **1** (Work with display devices).
5. On the Work with Display Devices display, make all the workstations except the one you are using unavailable. Do this by typing **2** in front of each workstation name and pressing the **Enter** key.
6. Return to the SETUP menu by pressing **F3** (Exit) twice.
7. Press **F12** (Cancel) to remove the command line.

```
                   Work with Display Devices

Type options below, then press Enter.
  1=Make available    2=Make unavailable   5=Display
  7=Display message   8=Work with controller and line
  13=Change description

Opt  Device    Type    Status
 __   DSP01    3196    QSECOFR
 2_   DSP02    3196    Available to use
 2_   DSP03    3196    Available to use
 2_   DSP04    3196    Available to use
```

When you make a device unavailable, it does not have a Sign On display, even if it is powered on. Workstations stay unavailable only until you stop and start your system again. You may need to repeat this step.

After you prevent anyone else from signing on to the system, you can enter system values for security.

Entering system values for security

After you have prevented others from signing on, you need to enter system values into the system.

Use this procedure to enter the information from Part 1 of your System Values Selection form:

1. From the SETUP menu, select option **1** (Change system options).
2. Enter information from your System Values Selection form on the Change System Options display. If you do not want to change one of the choices on the display, you can use the Tab key to skip over it.
3. Enter the correct date and time on this display, if they were not set when you started the system.
4. After you type the information on this page, page down to the next page. The *More...* in the lower right corner of the display means that the display has at least one more page.

```
                   Change System Options
System:
Type choices below, then press Enter.

System name . . . . . . . . . .   JKLTOY     Name

Date and time options:
  System date . . . . . . . . .   09/21/99   MM/DD/YY
  System time . . . . . . . . .   10:52:57   HH:MM:SS
  Date separator  . . . . . . .   1          1=/
                                             2=-
                                             3=.
                                             4=,
                                             5=blank
  Date format . . . . . . . . .   MDY        YMD, MDY, DMY, JUL
  Time separator  . . . . . . .   1          1=:
                                             2=.
                                             3=,
                                             4=blank



                                                      More...
F1=Help   F3=Exit   F5=Refresh   F12=Cancel
```

5. Type your choices on the second page of the display and page down.

```
                    Change System Options

Type choices below, then press Enter.


Security options:
  Security level  . . . . . . .    40
      :
      :
  Allow security officers to
    sign on to any display
    station . . . . . . . . .    N
```

6. Type your choices on the third page of the display and press the **Enter** key.

```
                    Change System Options

Type choices below, then press Enter.


Device options:
  Device naming format for new
  devices . . . . . . . . . .    1


  Default system printer  . . .    PRT01

Additional options:
  Put users in S/36 environment
    at sign-on  . . . . . . . .    N
  Save job accounting
    information about completed
    printer output  . . . . . .    Y
```

7. You should see the SETUP menu again. Notice the message at the bottom of your display: **System options successfully changed. IPL required**.

   Note: The system requires an IPL only if you changed the security level.

At the end of most system task topics you will find a table that describes possible errors and recovery steps. Use these tables for assistance if your results are different from those described. These tables may not anticipate every problem. The intent of the tables is to give you guidance in problem solving and make you more comfortable using your system.

Possible Error	Recovery
The MAIN menu is displayed.	You pressed **F3** (Exit) or **F12** (Cancel). Type GO SETUP and try again.
You see another display, such as the Change Cleanup Options display.	You selected the wrong option from the SETUP menu. Press **F3** (Exit) to return to the menu and try again.
The Change System Option display is shown again after you press the **Enter** key.	Look for an error message at the bottom of the display. You probably typed a value that is not allowed. Remember to use **F1** (Help) if you need more information. Use **F5** (Refresh) if you want the system to restore all the values to what they were before you started typing. Try again.
You pressed the **Enter** key before you typed all your choices on the display.	You can use this display as many times as necessary to change system values. Select option **1** from the SETUP menu and enter the values you missed the first time. **Attention: Once your system is operational, do not change the security level without consulting a programmer. Also, do not change the system name if you are using iSeries Access or communicating with another computer.**

Possible Error	Recovery
You pressed the **Enter** key instead of paging down.	Select option **1** from the SETUP menu again and page down to display the second page. Type your choices and press the **Enter** key.

After entering your system values, you must then apply the new system values.

Applying the new system values

After you enter your system values, you need to apply some of these values. Most changes to system values take effect immediately. However, when you change the security level on your system, the change does not take effect until you stop your system and start it again. After you verify that you typed all the values on the Change System Options display correctly, you are ready to apply the new values.

Note: Attach your workstations to the system, if you have not already done so. When you start the system, it automatically configures those devices using the naming format you chose on the Change System Options display.

Use the following procedure to stop your system and start it again. When your system starts, the values you entered on the Change System Options display take effect.

1. Make sure you have signed on at the console and that no other workstations are signed on.
2. Make sure that the keylock switch on the processor unit is in the Normal position.
3. From the SETUP menu, select the option for Power On and Off Tasks.
4. Select the option to power off the system immediately and then power on. Press the **Enter** key.
5. The system shows a display that requests you to confirm your power-down request. Press **F16** (Confirm).

This causes the system to stop and then start again automatically. Your display goes blank for a few minutes. Then you should see the Sign On display again.

After you apply your new system values, you must create a security officer profile for yourself on the system.

Creating a security officer profile

A **security officer** on the system is any user with *SECOFR user class or *ALLOBJ and *SECADM special authorities.

After you apply the system values from the Change System Option display, create a user profile for yourself and for the alternate security officer. In the future, use your profile, rather than the QSECOFR profile, when you perform security officer functions.

1. Sign on to the system as QSECOFR and request the SETUP menu.

   Notice that the system name you chose appears in the upper right of the Sign On display.

```
            Sign On
                        System  . . . . .
                        Subsystem . . . .
                        Display . . . . .

User  . . . . . . . . . . . . .   QSECOFR
Password  . . . . . . . . . . .   _____
Program/procedure . . . . . . .   _____
Menu  . . . . . . . . . . . . .   SETUP
Current library . . . . . . . .   _____
```

2. From the SETUP menu, select the *Work with user enrollment* option. The Work with User Enrollment display lists the profiles currently on your system.

   Note: If you see the Work with User Profile display, press **F21** (Select assistance level) and change to basic assistance level.
3. To create a new profile, type **1** (Add) in the *Opt* (option) column and the name of your profile in the *User* column. Press the **Enter** key.

```
                    Work with User Enrollment

Type options below, then press Enter.
  1=Add   2=Change   3=Copy   4=Remove   5=Display

Opt    User            Description
1      JONESS
QDOC                        Document User Profile
QSECOFR                     Security Officer User Profile
```

4. On the Add User display, assign yourself a password.
5. Fill in the fields shown on the sample display with your own appropriate information.
6. Page down to the next page of the display.

```
                       Add User

Type choices below, then press Enter.

User  . . . . . . . . . .    JONESS
User description  . . . .    Jones, Sharon
Password  . . . . . . . .    secret
Type of user  . . . . . .    *SECOFR
User group  . . . . . . .    *NONE

Restrict command line use    _____
Default library . . . . .
Default printer . . . . .    *WRKSTN
Sign on program . . . . .    *NONE
Library . . . . . . . .

First menu  . . . . . . .
Library . . . . . . . .
```

7. Fill in the second page of the display and press the **Enter** key.
8. Check for confirmation messages at the bottom of the Work with User Enrollment display.
9. Press **F3** (Exit) to return to the SETUP menu.

```
                       Add User

Type choices below, then press Enter.

Attention key program . .    *SYSVAL
  Library . . . . . . . .
```

Possible Error	Recovery
You pressed the **Enter** key before typing information in all the fields.	Use the *Change* option from the Work with User Enrollment display to change the profile you just created. If the profile does not appear on the list, press **F5** (Refresh) and page down to find it.

After you create a security officer profile for yourself, you need to change user ID and passwords for Service Tools users. See the Service Tools topic in the Information Center.

Setting system values for security

In this topic, use the Work with System Values (WRKSYSVAL) command to change and display system values.

What Forms Are Needed?

Enter information from the System Values Selection form that you prepared in "Planning your overall security strategy."

To set up your system values, complete these tasks:
1. Changing security system values.
2. Changing individual system values.

Sign on to the command line interface

Use this information to sign on to the system:

Profile
> Your own (*SECADM and *ALLOBJ authority is required)

Menu MAIN

After you sign on, you can begin to change security system values.

Changing security system values

After signing on to the system, use this procedure to enter the security system values that appear on Part 2 of your System Values Selection form.

1. On the command line, type `WRKSYSVAL *SEC` and press the **Enter** key. The *SEC after the command name means that you want to see only the system values that relate to security.
2. On the Work with System Values display, type a **2** (Change) in the *Option* column in front of the system value you want to change. If the system value you want to change does not appear on the display, page down until you find it.

```
                    Work with System Values

Position to  . . . . . .              Starting character
Subset by Type . . . . .    *SEC         F4 for list

Type options, press Enter.
  2=Change   5=Display

         System
Option   Value       Type         Description
         QINACTMSGQ  *SEC         Inactive job message queue
2        QLMTDEVSSN  *SEC         Limit device sessions
         QLMTSECOFR  *SEC         Limit security officer device
         QMAXSGNACN  *SEC         Action to take for failed
  ⋮
```

3. Type your choice for the system value and press the **Enter** key. The screen shows the Work with System Values display again.

```
                    Change System Value
System value . . . . . :    QLMTDEVSSN
Description  . . . . . :    Limit device sessions


Type choice, press Enter.

  Limit device session . . . .   0          0=Do not
                                            1=Limit
```

4. Check the confirmation message at the bottom of the display.

Possible Error	Recovery
You see different system values than the ones shown on the example of the Work with System Values display.	You forgot to type *SEC. Compare the *Subset by type* field at the top of your display with the sample display. Move your cursor to the *Subset by type* field. Type *SEC and press the **Enter** key.
The system did not process your command. You still see a menu.	Check for error messages at the bottom of your display. You probably typed the command name incorrectly. Try again. If the message says you are not authorized, sign off and sign on again using a profile with security officer authority.
The Change System Value display appears again after you press the **Enter** key.	Check the bottom of the display for error messages. You probably typed your choice incorrectly or picked a value that was outside the permitted range. Use **F1** (Help) for additional information.
You see a menu instead of the Work System Values display.	You probably pressed the **Enter** key twice. Type WRKSYSVAL *SEC.
You selected a system value that you do not want to change.	Press **F12** (Cancel) to return to the Work with System Values display.

What Does the * (Asterisk) Mean?

You probably noticed that some values have an asterisk (*) before them. The system uses the asterisk to tell the difference between special values and regular words. For example, when you specify that the password on a user profile is *NONE, that means that the system will allow no one to sign on by using that profile. If you specify that the password is NONE, the user must type the characters NONE as the password.

While you are setting up security on your system, be sure to pay attention to the use of the asterisk in the instructions and on the forms.

After you have changed the security system values, you can change individual system values.

Changing individual system values

After you change security system values, you can change individual system values.

For example, the Disconnect Job Time-Out Interval (QDSCJOBITV) system value is not included as a security system value. It does not appear on the *SEC subset of the Work with System values display. Use this procedure to change the QDSCJOBITV system value or any individual system value:

1. Type WRKSYSVAL QDSCJOBITV and press the **Enter** key.
2. On the Work with System Values display, type a **2** (Change) in the *option* column in front of QDSCJOBITV.
3. Type your choice for QDSCJOBITV.
4. Check the confirmation message.

```
                         Change System Value
System value . . . . . :   QDSCJOBITV
Description  . . . . . :   Disconnected job time-out interval


Type choice, press Enter.

  Disconnected job time-out interval ...... 300
```

Listing your security values

After you enter all the information from your System Values Selection form, you can print a list of all the security system values. Type WRKSYSVAL *SEC OUTPUT(*PRINT). File a copy of the list with your System Values Selection form. Reprint the list whenever you change a security system value.

After you enter all of your choices for system values from the System Values Selection form, you can prepare to load your applications.

Performing security steps for loading your applications

After you set your system values, you can prepare to load your applications. This topic covers the security steps necessary to load your application libraries to your system. After you create profiles and other security objects, "Setting up ownership and public authority" and "Setting up resource security" show how to establish ownership and authority for your applications.

If possible, you should load your application libraries to your system before setting up user groups and individual profiles. You need to refer to application objects when you create job descriptions and profiles.

If you are not able to load your applications before creating group and individual profiles, you may receive warning messages, such as the following:

- The system does not find initial libraries when you create job descriptions.
- The system does not find the initial program or menu when you create profiles.

You cannot successfully test job descriptions and profiles until you load your application libraries.

Use the Application Installation forms that you prepared in "Planning your application installation."

To load each of your applications, complete these tasks:

1. Create an owner profile.
2. Load the application.

Signing on to the system

- To create owner profiles:

  Profile
  Your own (*SECADM authority is required)

  Menu MAIN

- To load application libraries:

  Check with your application provider to see if you should be signed on as the security officer or the application owner when you load the application libraries.

After you sign on, you can create an owner profile for your applications.

Creating an owner profile

After signing on to the system, check your Application Installation Plan to see if you need to create any profiles before you load the application. To create a profile:

1. Type CRTUSRPRF (Create User Profile) and press **F4** (Prompt).
2. On the Create User Profile display, fill in the fields as instructed by your programmer or application provider.
3. Use **F10** (More fields) and page down to display additional fields.

```
                    Create User Profile (CRTUSRPRF)

Type choices, press Enter.

User profile . . . . . . . . . . >
User password  . . . . . . . . .    *USRPRF
Set password to expired  . . . .    *NO
Status . . . . . . . . . . . . .    *ENABLED
User class . . . . . . . . . . .    *USER
Assistance level . . . . . . . .    *SYSVAL
Current library  . . . . . . . .    *CRTDFT
Initial program to call  . . . .    *NONE
  Library  . . . . . . . . . . .
Initial menu . . . . . . . . . .    MAIN
  Library  . . . . . . . . . . .      *LIBL
Limit capabilities . . . . . . .    *NO
Text 'description' . . . . . . .    Owner of xxxxxx
```

4. Check the bottom of your display for messages.

Note: Creating a group profile discusses creating profiles in more detail.

After you create an owner for the application, you can begin to load your application.

Loading the application

Follow your application provider's instructions for loading your application libraries. In "Setting up ownership and public authority," you learn to set up ownership and public authority to the applications.

After you load all of your applications, you can set up user groups.

Setting up user groups

After you perform security steps for loading your applications you can set up user groups. You will create group libraries, job descriptions, and group profiles. Work through the entire topic with one of your user groups, then go back and repeat the steps for any additional groups. The sample displays show information from the User Group Description forms for the Sales and Marketing Department and the Warehouse Department at the JKL Toy Company.

Use the User Group Description forms that you prepared in "Planning user groups."

Complete these tasks to set up user groups:

1. Create a library for the user group.
2. Create a job description.
3. Create a group profile.

Sign on to the system

Profile
      Your own (*SECADM authority is required)

Menu MAIN

After you sign on, you can create a library for the user group.

Creating a library for the group

After you sign on to the system, you need to create a library for the user group. If you plan to have the group share a library for objects they create, such as Query programs, create the library before you create the group profile:

1. Type CRTLIB (Create Library) and press **F4** (Prompt).
2. Fill in the display. The library name should be the group profile name.
3. Press **F10** (Additional parameters).
4. Fill in the public authority for the library and new objects that are created in the library.
5. Press the **Enter** key. Check the confirmation message.

```
                      Create Library

Type choices, press Enter.

Library  . . . . . . . . . . . .     DPTWH
Library type . . . . . . . . . .     *PROD
Text 'Description' . . . . . . .     Warehouse Library

                   Additional Parameters

Authority  . . . . . . . . . . .     *USE
Auxiliary storage pool ID  . . . .   1
Create authority . . . . . . . .     *CHANGE
Create object auditing . . . . . .   *SYSVAL
```

Possible Error	Recovery
You pressed the **Enter** key before you typed a description for the library.	Type **CHGLIB** and press **F4** (Prompt). Type the library name on the prompt display and press the **Enter** key. Type the description on the Change Library display.
You gave the library the wrong name.	Use the Rename Object (RNMOBJ) command.

After you create a library for the group, you can create a job description.

Creating a job description

After you create a library for the group, you can create a job description for each group.

If the libraries needed for the initial library list are not yet on the system, you receive a warning message when you create the job description.

1. Type **CRTJOBD** (Create Job Description) and press **F4** (prompt).
2. Fill in these fields:

   Job description:
   Same as group profile name.

   Library name:
   QGPL

   Text: Group description
3. Press **F10** (Additional parameters).
4. Page down to the *Initial library list* field.

```
                    Create Job Description

Type choices, press Enter.

Job description  . . . . . . . . .   DPTSM
  Library  . . . . . . . . . . .    QGPL
Job queue  . . . . . . . . . . .    QBATCH
  Library  . . . . . . . . . . .     *LIBL
Job priority (on JOBQ)  . . . . . . 5
Output priority (on OUTQ)  . . . .  5
Print device . . . . . . . . . .    *USRPRF
Output queue . . . . . . . . . .    *USRPRF
  Library  . . . . . . . . . . .
Text 'description' . . . . . . . .  Sales and Marketing
```

5. Type a **+** (plus) over *SYSVAL in the *Initial library list* field to specify that you want to enter a list of values. Press the **Enter** key.

```
Accounting code . . . . . . . . . .    *USRPRF
    ⋮
CL syntax check . . . . . . . . . .    *NOCHK
Initial library list  . . . . . . .    +
              + for more values
```

6. In the *Initial library list* field, type the names of libraries that are marked (✔) from your User Group Description form:
   - Put one library name per line.
   - Include QGPL and QTEMP. Every job uses a library called QTEMP to store temporary objects. **All initial library lists must have the QTEMP library**. For most applications, the QGPL library should also be on the initial library list.
   - You do not need to include the current (default) library on the library list. The system adds that library automatically at sign-on.
7. Press the **Enter** key. Check messages. (Page down to see all messages.)

```
Specify More Values for

Type choices, press Enter.

Initial library list . . . . . .      CUSTLIB
                                      ITEMLIB
                                      COPGMLIB
                                      ICPGMLIB
                                      QGPL
                                      QTEMP
```

Possible Error	Recovery
You pressed the **Enter** key instead of **F10**.	To put the correct libraries in the initial library list, type **CHGJOBD** (Change Job Description) and press **F4**.
You get error messages when you try to create the job description.	The most common error message occurs when you try to include a library that is not on the system. This is a warning message. The job description is still created with the library in the initial library list. You cannot sign on with a profile that specifies the job description until the library is on the system.

If the library is on the system, you may have typed the name incorrectly. Verify the library name and try again. |

After you create a job description, you can create a group profile.

Creating a group profile

After you create a job description, you can create the group profile. To do this, use the information from Part 2 of the User Group Description form.

1. Use the Work with User Profiles command. Type WRKUSRPRF *ALL. Initially, the display lists the profiles supplied by IBM.

    Note: If you see the Work with User Enrollment display, press **F21** to change to intermediate assistance level.

2. To create a new profile, type **1** in the *Opt* (option) column and profile name in the *User Profile* column. Press the **Enter** key.

```
                      Work with User Profiles

Type options, press Enter.
  1=Create   2=Change   3=Copy   4=Delete   5=Display
  12=Work with objects by owner

     User
Opt  Profile      Text
1    DPTSM
     QDOC         Document User Profile
     QSECOFR      Security Officer User Profile
```

3. Type information from your User Group Description form into the appropriate fields.
4. Use the **Tab** key to skip over any fields where you want to use the default value.
5. Press **F10** (Additional parameters).
6. Page down.

```
                     Create User Profile (CRTUSRPRF)

Type choices, press Enter.

User profile . . . . . . . . . . > DPTSM
User password  . . . . . . . . .   *none
Set password to expired  . . . .   *NO
Status . . . . . . . . . . . . .   *ENABLED
User class . . . . . . . . . . .   *USER
Assistance level . . . . . . . .   *SYSVAL
Current library  . . . . . . . .   *CRTDFT
Initial program to call  . . . .   cpsetup
  Library  . . . . . . . . . . .   cppgmlib
Initial menu . . . . . . . . . .   cpmain
  Library  . . . . . . . . . . .   cppgmlib
Limit capabilities . . . . . . .   *yes
Text 'description' . . . . . . .   Sales and Marke
```

7. Enter the remaining fields from your User Group Description form on the additional pages of the display and press the **Enter** key.

```
                     Create User Profile

                     Additional Parameters

Special authority  . . . . . . .    *USRCLS

   ⋮

Job description  . . . . . . . .   DPTSM
  Library  . . . . . . . . . . .   QGPL
```

```
                     Create User Profile

Group authority  . . . . . . . .    *NONE

   ⋮

Print device . . . . . . . . . .   PRT03
```

8. Check messages.

> **Remember**
>
> A group profile is just a special type of user profile. Many messages and displays refer to group profiles as users or user profiles. The system only knows that you have created a group profile if you add members to it or assign a group identification number (gid) to it.

Possible Error	Recovery
You pressed the **Enter** key before typing all the values in the group profile.	Press **F5** (Refresh) to add the profile you created to the Work with User Profiles display. Use option **2** (Change) to correct the profile.
You created a profile with the wrong name.	You cannot change the name of a profile. Use the copy option (**3**) to create a new profile with the correct name. Then delete (option **4**) the profile with the wrong name.

Possible Error	Recovery
Some of the fields from the User Group Description form do not appear on the display.	Make sure you are using intermediate assistance level. The basic assistance level version of Create User Profile is called the Add a User display. To change assistance levels, press **F12** (Cancel) to return to the Work with User Enrollment display. Use **F21** to change assistance levels. See "Selecting the right assistance level."
You accidentally erased some of the default information from the Create User Profile display.	If you leave a field blank, the system uses the default value when the user profile is created. If you want to see the default values, press **F5** (Refresh) to restore the entire display. Type your information again.

Listing your results

List the names and descriptions of all profiles on the system by using the Display Authorized Users (DSPAUTUSR) command. Type DSPAUTUSR OUTPUT(*PRINT). Check to make sure that all group profiles have a password of *NONE.

Complete the following before you set up individual users:
- Create a job description for each user group.
- Optionally, create a library for each group.
- Create a group profile for each user group.

Setting up individual users

When you set up user groups, you completed the steps to create group profiles. Now, you create individual profiles for the members of the groups.

Work through the entire topic with the members of one user group, then go back and repeat the steps for any additional groups. The sample displays show users from the Individual User Profile Forms that Sharon Jones prepared for the Sales and Marketing Department and the Warehouse Department at the JKL Toy Company. You can find copies of these forms in "Planning individual user profiles."

Use the Individual User Profile forms you prepared in "Planning individual user profiles."

To create individual profiles for the members of the groups, complete these tasks:
1. Create a personal library. (optional)
2. Copy the group profile.
3. Set the password to expire.
4. Create additional users. (optional)

   Note: Repeat Create a personal library and Create additional users until every group member has a user profile.
5. Change information about a user, if necessary.
6. Display your results.

Sign on to the system

Profile
      Your own (*SECADM authority is required)

Menu SETUP

Creating a personal library

To begin setting up individual users, you may need to create a personal library for each member for objects, such as Query programs. Create personal libraries before you create the individual user profiles.

1. Type **CRTLIB** and press **F4** (Prompt).
2. Give the library the same name as the user profile.
3. Press **F10** (Additional parameters).
4. Fill in the public authority for the library and new objects that are created in the library.
5. Press the **Enter** key. Check the confirmation message.

```
                        Create Library

 Type choices, press Enter.

 Library  . . . . . . . . . . . .    DPTSM
 Library type . . . . . . . . . .    *PROD
 Text 'description' . . . . . . .    Warehouse Library

                     Additional Parameters

 Authority  . . . . . . . . . . .    *EXCLUDE
 Auxiliary storage pool ID  . . .    1
 Create authority . . . . . . . .    *CHANGE
 Create object auditing . . . . .    *SYSVAL
```

After you create a personal library, you can create the individual profile by copying the group profile.

Copying the group profile

The group profile has two roles:

1. The system uses it to determine whether a group member is authorized to use an object.
2. You can use it as a pattern to create user profiles for the individual group members.

When you set up user groups, you created group profiles. Now, you can copy a group profile to create an individual profile and copy the individual profile to create other profiles in the group.

1. Select the Work with User Enrollment option from the SETUP menu.

    Note: If you see the Work with User Profiles display, use **F21** (Select assistance level) to change to basic assistance level.

2. Type **3** (Copy) in the *Opt* column in front of the user group. The screen shows the Copy User display. (If the user group you want to copy is not on your display, page down until you find it.) The system leaves the user name field blank and fills in the remaining fields from the group profile that you copied.

```
                   Work with User Enrollment

 Type options below, then press Enter.
   1=Add    2=Change   3=Copy   4=Remove   5=Display

 Opt     User          Description

         DPTSM         Sales and Marketing Department
 3       DPTWH         Warehouse Department
```

3. Type the name and description of the user profile that you are creating.
4. Leave the password blank. The system automatically makes the password the same as the new user profile name.

5. Put the group profile name in the *User group* field.
6. Check your Individual User Profile form to see if this user has other values that are different from the group. Enter those values.
7. Page down.

```
                         Copy User

Copy from user  . . . . :    DPTWH

Type choices below, then press Enter.

User  . . . . . . . . . .    WILLISR
User description  . . . .    Willis, Rose
Password  . . . . . . . .
Type of user  . . . . . .    *SYSOPR
User group  . . . . . . .    DPTWH

Restrict command line use   N

Default library . . . . .    DPTWH
Default printer . . . . .    PRT04
Sign on program . . . . .    *NONE
  Library . . . . . . . .

First menu  . . . . . . .    ICMAIN
  Library . . . . . . . .      ICPGMLIB
```

8. Make any changes that are necessary on the next page of the display and press the **Enter** key.
9. Check for confirmation messages at the bottom of the Work with User Enrollment display.

```
                         Copy User

Copy from user  . . . . :    DPTWH

Type choices below, then press Enter.

Attention key program . .    *SYSVAL
  Library . . . . . . . .
```

Possible Error	Recovery
You see the Create User Profile display instead of the Copy User display.	Use **F12** (Cancel) to return to the Work with User Profiles display. Use **F21** to change to basic assistance level. Start the copy operation again.
The user profile name you have selected will not fit in the user prompt.	Although user profile names may be up to 10 characters, the Copy User and Add User displays support no more than 8 character names. Either choose a shorter user name or use the intermediate assistance level to create individual user profiles.

Testing the User Profile

When you create the first individual profile in a group, you should test it by signing on with that profile. Verify that you see the correct first menu and that the sign-on program runs.

If you are unable to sign on successfully with the profile, the system probably could not find something specified in the profile. This could be the sign-on program, the job description, or one of the libraries in

the initial library list. Use the Work with Printer Output display to find the job log that was written when you tried to sign on. The job log tells you what errors occurred.

For information about testing and diagnosing problems when you make security changes, see "Testing security."

After you test the user profile, you can set the password to expire.

Setting the password to expire

Set up individual profiles to require that users change their passwords the first time they sign on. The *Set password to expire* field does not appear on the basic assistance level version of the Copy User display. You need to change it separately, after you create the user profile with the copy function. To change the *Set password to expire* field, type CHGUSRPRF *profile-name* PWDEXP(*YES).

Note: If you want to test a user profile by signing on with it, do the test *before* you set the password to expire.

Possible Error	Recovery
You tested a profile and were forced to change the password.	Type **CHGUSRPRF** *profile-name* and press **F4** (Prompt). Set the password back to the user profile name. (Type the user profile name in the password field.) Type ***YES** in the *Set password to expire* field. You need intermediate assistance level to do this.

After you create the first individual user profile, you can create additional users.

Creating additional users

After you copy a group profile to create the first individual profile, you can create additional users. Copy the first individual user profile to create additional members in the group. Look at each individual profile carefully when you create it with the copy method. Check your Individual User Profile form and make sure that you change any fields that are unique for the new user profile.

1. On the Work with User Enrollment display, type **3** (Copy) in front of the user profile you want to copy.
2. On the Copy User display, type the profile name and description.
3. Enter information into any fields that are unique for the new user.

```
                    Work with User Enrollment

Type options below, then press Enter.
   1=Add    2=Change    3=Copy    4=Remove    5=Display

 Opt     User            Description

         DPTSM           Sales and Marketing Department
         DPTWH           Warehouse Department
 3       WILLISR         Willis, Rose
```

Possible Error	Recovery
The profile you want to copy does not appear on the Work with User Enrollment display.	Press **F5** (Refresh). Page up and page down. The list is alphabetical by profile name.

If you would like to alter information about a user, see Changing information about a user.

Changing information about a user

For some users, you may need to set values that do not appear on the Copy User display. For example, some users may belong to more than one group profile. After you have created a user profile by using the copy method, you can change it.

1. On the Work with User Enrollment display, press **F21** to change to intermediate assistance level.
2. On the Work with User Profiles display, type a **2** (Change) in the *Opt* (option) column next to the profile you want to change. Press the **Enter** key.

```
                    Work with User Profiles

Type options, press Enter.
  1=Create   2=Change   3=Copy   4=Delete   5=Display
  12=Work with objects by owner

     User
Opt  Profile    Text
2    AMESJ      Ames, Janice
     DPTSM      Sales and Marketing Department
     QDOC       Document User Profile
     QSECOFR    Security Officer User Profile
     WAGNERR    Wagner, Ray
     WILLISR    Willis, Rose
```

3. On the Change User Profile display, press **F10** (Additional parameters).
4. Page down until you find the fields that you want to change. For example, if you want to make the user a member of additional group profiles, page down until you find the *supplemental groups* field.
5. Type the values you want and press the **Enter** key. You receive confirmation messages and see the Work with User Profiles display again.

```
                 Change User Profile (CHGUSRPRF)

Type choices, press Enter.

Maximum allowed storage  . . . .    *NOMAX
Highest schedule priority  . . .    3
Job description  . . . . . . . .    DPTWH
  Library  . . . . . . . . . .       QGPL
Group profile  . . . . . . . .     DPTWH
Owner  . . . . . . . . . . . .     *GRPPRF
Group authority  . . . . . . .     *USEE
Group authority type . . . . . .   *PGP
Supplemental groups  . . . . . .   DPTIC
            + for more values
```

Once you have changed the user information, you can display your results to check your profiles.

Displaying user profiles

Several methods are available to display the profiles that you created.

Displaying one profile
Use option **5** (Display) from either the Work with User Enrollment display or the Work with User Profiles display.

Listing one profile
Use the Display User Profile command: DSPUSRPRF *profile-name* DETAIL(*BASIC) OUTPUT(*PRINT).

Displaying group members
Type DSPUSRPRF *group-profile-name* *GRPMBR. You can use OUTPUT(*PRINT) to print the list.

Listing all profiles
> To list the names and descriptions of all profiles, sorted by group, use the Display Authorized Users command: DSPAUTUSR SEQ(*GRPPRF) OUTPUT(*PRINT).

Before you set up ownership and public authority, make sure that you complete these tasks:

- Finish creating all your individual user profiles.
- Set the password to expire for each profile.
- Print a list of all profiles sorted by group and keep it with your User Group Description forms. Print the list again when you add new users.

Setting up resource security

In this topic, you establish ownership and public authority to objects, as well as specific authority to your applications. You also set up resource security for workstations and printers. Work through the entire topic for one library, then go back and repeat the steps for any additional libraries used by an application. When you complete setting up resource security for one application, repeat the steps for other applications.

Use these procedures whenever you install a new application on your system or when you set up resource security for an existing application.

The sample displays in this topic show the Authorization List forms, the Library Description forms, and the Output Queue and Workstation Security form for the JKL Toy Company. You can find examples of these forms in "Setting up ownership and public authority."

What forms are needed?
- The Application Installation forms that you prepared in "Planning your application installation."
- The Authorization List forms that you prepared in "Grouping objects."
- The Library Description forms that you prepared in "Determining ownership of libraries and objects."
- The Output Queue and Workstation Security form that you prepared in "Protecting printer output" and "Protecting workstations."
- The System Responsibilities form that you prepared in "Planning your overall security strategy."

You can set up resource security in several ways. The sequence of steps in this topic matches the order of information on the Application Installation forms, the Authorization List forms, and the Library Description form:

1. Setting up ownership and public authority.
2. Creating authorization lists.
3. Securing objects with an authorization list.
4. Adding users to the authorization lists.
5. Setting up any specific authorities.
6. Securing printer output.
7. Securing workstations.
8. Restricting access to the system operator message queue.

Setting up ownership and public authority

In this topic, you establish ownership and public authority for application libraries, group libraries, and personal libraries. Work through the entire topic with one application, then go back and repeat the steps for any additional applications. The sample displays show the Application Installation forms that Sharon Jones prepared for the Customer Orders application in "Planning your application installation."

Use the procedures in this topic whenever you install a new application on your system or when you set up security for an existing application.

Use the Application Installation forms that you prepared in "Planning your application installation."

In order to set up ownership and public authority, complete these tasks:
1. Create the owner profile.
2. Change library ownership.
3. Set ownership of application objects.
4. Set public access to a library.
5. Set public authority for all objects in a library.
6. Set public authority for new objects.
7. Work with group and personal libraries.

Sign on to the system

Profile
> Your own (*ALLOBJ authority is required)

Menu MAIN

Creating the owner profile
If the owner profile does not yet exist, do the following:
* Use the CRTUSRPRF (Create User Profile) command to create it. Set the password to *NONE.

If the owner profile already exists, do the following:
* Use the CHGUSRPRF (Change User Profile) command to set the password to *NONE.

After you create the owner profile, you can change library ownership.

Changing library ownership
This step changes the ownership of a library, not the objects in the library.

Attention: Be sure to check with your application provider before you change ownership of any application objects. Some applications use functions that rely on specific object ownership.
1. Type CHGOBJOWN (Change Object Owner) and press **F4** (Prompt).
2. Fill in the library name, object type (*LIB), and new owner.
3. Check confirmation messages.

```
                    Change Object Owner (CHGOBJOWN)

Type choices, press Enter.

Object . . . . . . . . . . . . > COPGMLIB
  Library  . . . . . . . . . . >   *LIBL       Name,
Object type  . . . . . . . . .> *LIB
New owner  . . . . . . . . . .   COWNER
Current owner authority  . . . .   *REVOKE
```

Possible Error	Recovery
You receive error messages.	The most common message is that either the library is not found or the new owner profile is not found. Check your typing for errors and try again.

After you change library ownership, you can set ownership for application objects.

Setting ownership of application objects

Changing the ownership of application objects is a cumbersome task, because you must change each object individually. If possible, ask your programmer or application provider to establish ownership for you.

Listing the objects in a library

Before you change ownership, print a list of all the objects in the library, using the Display Library command. You can use it as a checklist. Type DSPLIB *library-name* *PRINT.

Choosing the best method

Choose one of these two methods to change ownership of objects in your application libraries:

Table 61. Methods for Changing Object Ownership

Method	What It Does	When To Use It
The Work with Objects by Owner command	Shows a display which lists all the objects that a profile owns. You use an option on the display to change the owner of an object.	This method is easier to use. However, if either QPGMR or QSECOFR own the objects, IBM does not recommend this method. Those profiles own many objects, and your list display would be very large.
The Change Object Ownership command	Requires using a separate command for each object. However, you can use *Retrieve* (**F9**) to repeat the previous command and reduce the amount of typing required.	This method is faster if either QPGMR or QSECOFR own the objects.

Using the Work with objects by Owner (WRKOBJOWN) command: Use this method to change the ownership of the objects in a library if IBM-supplied profiles, such as QPGMR or QSECOFR, do *not* own the objects:

1. Type WRKOBJOWN *owner-profile-name*. Your screen displays a list of all the objects which that user profile owns.
2. Type **9** (Change owner) in front of each of the objects in the library on which you are working.
3. On the *Parameters or command* line at the bottom of the display, type NEWOWN(*owner-profile-name*) and press the **Enter** key.
4. The system changes the owner of each object you indicated to the new owner you typed at the bottom. You receive confirmation messages at the bottom of your display. The objects no longer appear on your display because the profile no longer owns them.
5. Repeat steps 2 and 4 until you change ownership of all the objects in the library.

```
                    Work with Objects by Owner

User profile . . . . . . . . :   OLDOWNER

Type options, press Enter.
  2=Edit authority      4=Delete   5=Display author
  8=Display description   9=Change owner

Opt  Object          Library       Type       Attribute
     COPGMMSG         COPGMLIB      *MSGQ
9    CUSTMAS          CUSTLIB       *FILE
9    CUSTMSGQ         CUSTLIB       *MSGQ
     ITEMMSGQ         ITEMLIB       *MSGQ


   .
   .
   .

Parameters or command
===> NEWOWN(COWNER)
F3=Exit   F4=Prompt   F5=Refresh   F9=Retrieve
F18=Bottom
```

Possible Error	Recovery
You see the Change Object Owner display.	You see this display if you specify option **9** (Change owner) and do not type any parameters at the bottom of the Work with Objects by Owner display. You also see this display if you type parameters incorrectly. Press **F12** (Cancel) to return to the Work with Objects by Owner display. Try again. Make sure you type the parameter as it is shown in the example.

You can use the change object owner command to change the ownership of objects that are owned by QPGMR or QSECOFR.

Using the change object owner command: Use this method to change the owner of objects in a library if QPGMR or QSECOFR *do* own the objects.

1. Type CHGOBJOWN and press **F4** (Prompt).
2. Fill in the information on the display for the first object on your list and press the **Enter** key.

```
                  Change Object Owner (CHGOBJOWN)

Type choices, press Enter.

Object . . . . . . . . . . . . . > CUSTMAS
  Library  . . . . . . . . . . . >   CUSTLIB
Object type  . . . . . . . . . . > *FILE
New owner  . . . . . . . . . . .   COWNER
Current owner authority  . . . .   *REVOKE
```

3. You receive a confirmation message that the object ownership is changed. Check off the item on your list.
4. Press **F9** (Retrieve) to retrieve the command that you typed.
5. Press **F4** (Prompt). On the Change Object Owner display, enter information for the next object in the library and press the **Enter** key.
6. Repeat steps four and five for each object in the library.

Checking your work

To make sure that you changed ownership of all the objects in the library, use the Work with Objects by Owner command. Type WRKOBJOWN *new-owner-profile*. Compare the display with your list of objects in the library.

After you change the ownership of objects in the library, you can set public access to the library.

Setting public access to a library

After you set ownership of application objects, you can use the Edit Object Authority (EDTOBJAUT) command to change public authority to the library:

1. Type EDTOBJAUT *library-name* *LIB.
2. Move the cursor down to the line showing *PUBLIC*.
3. Type the authority which you want the public to have to the library and press the **Enter** key.

```
                        Edit Object Authority

Object . . . . . . . :   CUSTLIB       Owner  . . . . . . . :   COWNER
  Library  . . . . . :    QSYS         Primary group  . . . :   *NONE
Object type  . . . . :   *LIB

Type changes to current authorities, press Enter.

  Object secured by authorization list  . . . . . . . . . . .    *NONE

                        Object
User        Group       Authority
COWNER                  *ALL
*PUBLIC                 *CHANGE
```

4. The display shows the new authority.

You can now set public authority for all objects in a library.

Setting public authority for all objects in a library

Use the Revoke Object Authority (RVKOBJAUT) command to remove the current public authority for objects in a library. Use the Grant Object Authority (GRTOBJAUT) command to set public authority for all the objects in a library:

1. Type RVKOBJAUT and press **F4** (Prompt).
2. Fill in the display as shown, substituting the name of your application library, and press the **Enter** key.

```
                   Revoke Object Authority (RVKOBJAUT)

Type choices, press Enter.

Object . . . . . . . . . . . . .    *all
  Library  . . . . . . . . . . .      custlib
Object type  . . . . . . . . . .    *all
Users  . . . . . . . . . . . . .    *public
            + for more values
Authority  . . . . . . . . . . .    *all
```

> **Note:** If the library has a large number of objects, the system may take a few minutes to process your request.

3. Type GRTOBJAUT and press **F4** (Prompt).
4. Fill in the display as shown, substituting the name of your application library and the authority you want, and press the **Enter** key.

```
                     Grant Object Authority (GRTOBJAUT)

Type choices, press Enter.

Object . . . . . . . . . . . . .    *all
  Library  . . . . . . . . . . .      custlib
Object type  . . . . . . . . . .    *all
Users  . . . . . . . . . . . .      *public
              + for more values
Authority  . . . . . . . . . . .    *use
```

> **Note:** If the library has a large number of objects, the system may take a few minutes to process your request.

After you have completed setting public authority for all objects in a library, you can use the job log to check your work next.

Using the job log to check your work: When you use the GRTOBJAUT command to make multiple changes to authority, view your job log to verify that the changes were made.

1. Type DSPJOBLOG (Display Job Log).
2. Press **F10** (Display detailed messages).
3. You should have a message about the change in authority for each object in the library. Check off the objects on your list as you review the messages.

```
                         Display All Messages
                        System:   RCHASxxx
Job . . :   QPADEV0010    User . . :   JCHEIDEL     Number . . . :    025457

7 > GRTOBJAUT OBJ(CUSTLIB/*ALL) OBJTYPE(*ALL) USER(*PUBLIC) AUT(*USE)
  Authority given to user *PUBLIC for object CUSTMAS in CUSTLIB object type
    *FILE.
  Authority given to user *PUBLIC for object CUSTMSGQ in CUSTLIB object type
    *MSGQ.
  Authority given to 2 objects. Not given to 0 objects. Partially given to 0
    objects.
  Object authority granted.
7>> dspjoblog
```

Possible Error	Recovery
Your job log indicates that authority was not changed for some objects in the library.	Use Help (**F1**) to get more information about the message. Use EDTOBJAUT to set the authority for those objects individually.

You can now set public authority for new objects.

Setting public authority for new objects

The library description has a parameter called create authority (CRTAUT), which determines the public authority for new objects that are created in the library. The commands that create objects use the CRTAUT authority of the object library as the default. You should make the CRTAUT for a library the same as the public authority for the majority of existing objects in the library.

1. Type CHGLIB *library-name* and press **F4** (Prompt).
2. Press **F10** (Additional parameters).
3. Enter your choice in the *Create authority* field.

```
                      Change Library (CHGLIB)

Type choices, press Enter.

Library  . . . . . . . . . . . . > CUSTLIB
Library type . . . . . . . . . .   *PROD
Text 'description' . . . . . . .   'Customer Records'


                   Additional Parameters

Create authority . . . . . . . .   *CHANGE
Create object auditing . . . . .   *SYSVAL
```

If you set the CRTAUT to *SYSVAL, the system uses the current setting for the QCRTAUT system value
when you create a new object in the library. Setting a specific CRTAUT authority for each library protects
against future changes to the QCRTAUT system value.

You can now work with group and personal libraries.

Working with group and personal libraries

Your profile owns the group and personal libraries you created when you set up user groups and
individual users.

Use the procedures just covered to change ownership of group libraries to the group profile and change
ownership of personal libraries to the individual user profiles. Use the EDTOBJAUT command.

Set the Create Authority parameter for each group and personal library to determine the public authority
for any new objects in those libraries. Use the CHGLIB command.

Before you start creating authorization lists, complete these tasks:
*   Use your Application Installation forms and your Library Description forms to make sure that you
    have established ownership and public authority for all your application libraries.
*   Set ownership and create authority for all of the group and personal libraries that you created.

    Note: You can get a list of all the libraries on your system by typing DSPOBJD *ALL *LIB *PRINT.

Creating an authorization list

After you set up ownership and public authority, you are ready to set up authorization lists. Using
information from your Authorization List forms, create any authorization lists that are necessary to secure
the library. Use the Create Authorization List (CRTAUTL) command:
1. Type CRTAUTL and press **F4** (Prompt).
2. Fill in the information from your Authorization List form.
3. Press **F10** (Additional parameters).
4. Use the authority parameter to specify the public authority for objects that are secured by the list.
5. Check for confirmation messages.

```
                    Create Authorization List (CRTAUTL)

Type choices, press Enter.

Authorization list . . . . . . .    custlst1
Text 'description' . . . . . . .    Files cleared at

                      Additional Parameters

Authority  . . . . . . . . . . .    *ALL
```

Possible Error	Recovery
You typed the name of the list incorrectly.	You cannot change the name of a list, once the system has created it. Delete the list (DLTAUTL) and try again.
You forgot to specify the public authority for the list.	Use the Edit Authorization List (EDTAUTL) command.

You can now secure objects with an authorization list.

Securing objects with an authorization list

Once you create an authorization list, use the Edit Object Authority (EDTOBJAUT) command to secure the items listed on your Authorization List form:

1. Type EDTOBJAUT and press **F4** (prompt).
2. Fill in the prompt display and press the **Enter** key.
3. On the Edit Object Authority display, enter the authorization list name.
4. If the public authority for the object comes from the authorization list, change the public authority to *AUTL.
5. Repeat these steps for each object on your Authorization List form.

```
                        Edit Object Authority

Object . . . . . . . :    ARFILE01       Owner  . . . . . . . :    OWNAR
  Library  . . . . . :      CUSTLIB      Primary group  . . . :    *NONE
Object type  . . . . :    *FILE

Type changes to current authorities, press Enter.

  Object secured by authorization list  . . . . . . . . . . . .    CUSTLST1


                      Object
User        Group       Authority
OWNER                   *ALL
*PUBLIC                 *AUTL
```

You can now add users to an authorization list.

Adding users to an authorization list

Once you secure objects with an authorization list, use the Edit Authorization List (EDTAUTL) command to add the users listed on your Authorization List form:

1. Type EDTAUTL *authorization-list-name*.
2. On the Edit Authorization list display, press **F6** (Add new users).
3. Enter the names of the users or groups and the authority they should have to the items on the list and press the **Enter** key.

4. The new users should appear on the list.

```
                            Add New Users

Object . . . . . . . :    WSLST1          Owner  . .
  Library  . . . . . :     QSYS

Type new users, press Enter.

             Object    List
User         Authority Mgt
QSECOFR      *CHANGE
```

Possible Error	Recovery
You gave a user or group the wrong authority to the list.	You can change the authority on the Edit Authorization List display.
You added the wrong user or group to the list.	You can remove a user or group using the Remove Authorization List Entry (RMVAUTLE) command, or you can type blanks over the user's authority on the Edit Authorization List display.

Checking your work

Use the Display Authorization List (DSPAUTL) command to list all the user authorities to the authorization list. Use **F15** from the display to list all the objects secured by the authorization list.

Before you set up specific authorities, complete these tasks:
- Use the CRTAUTL command to create any authorization lists you need for the application.
- Secure objects with authorization lists by using the EDTOBJAUT command.
- Add users to authorization lists by using the EDTAUTL command.

Setting up specific authorities

In "Setting up ownership and public authority," you learned how to use the GRTOBJAUT command to set public authority for all the objects in a library, based on the information in Part 1 of your Library Description form. Now, you can use the Edit Object Authority (EDTOBJAUT) command to set specific authority for the library and objects in the library, based on the information in Part 2 of your Library Description form.

See these topics to set specific authorities:
- Setting specific authority for a library.
- Setting specific authority for an object.
- Setting authority for more than one object at a time.

Setting specific authority for a library

A library is really a special type of object. You set authority for a library just like you set authority for any other object, by using the EDTOBJAUT command. All libraries reside in the IBM-supplied library that is called QSYS. The displays in the following examples use Part 2 of the Library Description form for the CONTRACTS library at the JKL Toy Company:

List Specific Authorities for Library Objects				
Group Profile or User Profile	Object Name	Object Type	Authority Needed	Authorization List

| DPTSM | CONTRACTS | *LIB | *USE | |
| DPTMG | CONTRACTS | *LIB | *USE | |

1. Type EDTOBJAUT and press **F4** (Prompt).
2. Fill in the prompt display and press the **Enter** key.

```
                    Edit Object Authority (EDTOBJAUT)

Type choices, press Enter.

Object . . . . . . . . . . . .   CONTRACTS
  Library  . . . . . . . . . .      QSYS
Object type  . . . . . . . . . .  *LIB
```

3. On the Edit Object Authority display, press **F6** (Add new users) to give authority to users whom the display does not list.
4. Press the **Enter** key.

```
                         Add New Users

Object . . . . . . . :   CONTRACTS      Owner  . . . . . . . :    OWNCP
  Library  . . . . . :      QSYS        Primary group  . . . :    *NONE
Object type  . . . . :   *LIB


Type new users, press Enter.


               Object
User           Authority
DPTSM      *USE
DPTMG      *USE
```

5. The Edit Object Authority display should match the information on both Parts 1 and 2 of the Library Description form.

```
                      Edit Object Authority

Object . . . . . . . :   CONTRACTS      Owner  . . . . . . . :    OWNCP
  Library  . . . . . :      QSYS        Primary group  . . . :    *NONE
Object type  . . . . :   *LIB

Type changes to current authorities, press Enter.

  Object secured by authorization list  . . . . . . . . . . . .   *NONE

                    Object
User        Group   Authority
OWNCP               *ALL
DPTSM               *USE
DPTMG               *USE
*PUBLIC             *EXCLUDE
```

The public authority for new objects (CRTAUT) authority does not appear on the Edit Object Authority display for a library. Use the Display Library (DSPLIB) command to see the CRTAUT for a library.

You can also use this procedure to set up specific authority to an object on the system.

You can now set specific authority for an object.

Setting specific authority for an object

The procedure for setting specific authority for an object in an application library is the same as setting specific authority for a library. The example uses Part 2 of the Library Description form for the COPGMLIB library at the JKL Toy Company:

Table 62. JKL Toy Company's Library Description form

Group Profile or User Profile	Object Name	Object Type	Authority Needed	Authorization List
PUBLIC	COMSGQ01	*MSGQ	*CHANGE	

1. Type EDTOBJAUT and press **F4** (Prompt).
2. Fill in the information on the prompt display and press the **Enter** key.
3. Fill in the authority information on the Edit Object Authority display and press the **Enter** key.

```
                        Edit Object Authority

Object . . . . . . . :   COMSGQ01       Owner  . . . . . . . . :    OWNCO
  Library  . . . . . :     COPGMLIB      Primary group  . . . :    *NONE
Object type  . . . . :   *MSGQ

Type changes to current authorities, press Enter.

   Object secured by authorization list  . . . . . . . . . . . .    *NONE


                        Object
User         Group      Authority
OWNCO                   *ALL
*PUBLIC                 *CHANGE
```

You can now set authority for more than one object at a time.

Setting authority for more than one object at a time

The examples so far have used the EDTOBJAUT command to set specific authority for a single object. Use the Grant Authority (GRTOBJAUT) command to set security for multiple objects. Type GRTOBJAUT and press **F4** (Prompt). Following are some examples of making multiple changes to authority.

* The fields entered on the following display set the public authority for all message queues in the CUSTLIB library to *CHANGE.

```
                    Grant Object Authority (GRTOBJAUT)

Type choices, press Enter.

Object . . . . . . . . . . . . .     *all
  Library  . . . . . . . . . . .       custlib
Object type  . . . . . . . . . .     *msgq
Users  . . . . . . . . . . . . .     *public
             + for more values
Authority  . . . . . . . . . . .     *change
```

* The fields entered on the following display give *ALL authority to all files whose names start with the characters WRK in the CUSTLIB library to the user AMES.

```
                    Grant Object Authority

Type choices, press Enter.

Object . . . . . . . . . . . .    WRK*
  Library  . . . . . . . . . .       custlib
Object type  . . . . . . . . . .  *file
Users  . . . . . . . . . . . .    AMES
             + for more values
Authority  . . . . . . . . . .    *all
```

This example uses a technique for specifying parameters that is called **generic** naming. Many commands allow you to specify the first characters followed by an asterisk (*) for a parameter. The system performs the operation on every object whose name starts with those characters. The on-line information for a command tells which parameters allow generic names.

- You will need to follow two steps to secure all the files that start with the characters AR using an authorization list called ARLST1 and have the files get their public authority from the list. These displays show the steps that are required.

```
                    Grant Object Authority

Type choices, press Enter.

Object . . . . . . . . . . . .    AR*
  Library  . . . . . . . . . . .      CUSTLIB
Object type  . . . . . . . . . .  *FILE

   .
   .
   .
Authorization list . . . . . . .  ARLST1
```

```
                    Grant Object Authority

Type choices, press Enter.

Object . . . . . . . . . . . .    AR*
  Library  . . . . . . . . . . .      CUSTLIB
Object type  . . . . . . . . . .  *FILE
Users  . . . . . . . . . . . .    *PUBLIC
             + for more values
Authority  . . . . . . . . . .    *AUTL
             + for more values
```

Use the DSPJOBLOG command as described in "Using the job log to check your work" to verify that the system made the requested authority changes.

Before going to "Securing printer output," use the EDTOBJAUT or the GRTOBJAUT command to set up the specific authorities on Part 2 of your Library Description form.

Securing printer output

After you set up specific authorities, you can protect confidential printer output by using the information in these topics:

- Creating an output queue and controlling who can manage it.
- Assigning special printer output to the queue.

Creating an output queue

1. Type CRTOUTQ (Create Output Queue) and press **F4** (Prompt).
2. Fill in the name of the output queue and the library.
3. Press **F10** (Additional parameters).
4. Page down to the find the security information for the output queue.

```
                    Create Output Queue (CRTOUTQ)

Type choices, press Enter.

Output queue . . . . . . . . . . >   NEWCP
  Library  . . . . . . . . . . .       CONTRACTS
Maximum spooled file size:
  Number of pages  . . . . . . .    *NONE          Number, *NONE
  Starting time  . . . . . . . .                   Time
  Ending time  . . . . . . . . .                   Time
             + for more values
Order of files on queue  . . . .    *FIFO
Remote system  . . . . . . . . .    *NONE

    :
    :
Text 'description' . . . . . . .    New Contracts Queue
```

5. Fill in the information from your Output Queue and Workstation Security form to control who can use and manage the output queue.
6. Press the **Enter** key and check for confirmation messages.

```
                    Create Output Queue (CRTOUTQ)

Type choices, press Enter.


Additional Parameters

Display any file . . . . . . . .    *NO
Job separators . . . . . . . . .    0
Operator controlled  . . . . . .    *NO
Data queue . . . . . . . . . . .    *NONE
  Library  . . . . . . . . . . .
Authority to check . . . . . . .    *OWNER
Authority  . . . . . . . . . . .    *LIBCRTAUT
```

Possible Error	Recovery
You pressed the **Enter** key instead of **F10**.	Use the Change Output Queue (CHGOUTQ) command to enter additional information.
You created the output queue in the wrong library.	Use the Move Object (MOVOBJ) command to move it to the correct library.

You can now assign printer output to an output queue.

Assigning printer output to an output queue

After you create an output queue, you can assign the printer output to an output queue. A printer file usually controls the destination of printer output. Check with your application provider to find out the names and libraries of the printer files for confidential reports.

If you do not have access to this information, print the report and hold it on the output queue. Use the attribute option from the Work with Spooled Files display to find out the name of the printer file. The printer file appears in the *Device file* field on the Work with Spooled File Attributes display.

To change the destination (output queue) of a printer file, use the Change Printer File (CHGPRTF) command:
```
CHGPRTF FILE(library-name/printer-file-name)
        OUTQ(library-name/output-queue-name)
```

The report goes to the new destination whenever someone requests the report again. To change the destination for a spooled file already in an output queue, use the change option from the Work with Spooled Files display.

For example, Sharon Jones at the JKL Toy Company wants to assign the price list printer file PRCLST1 to the PRICEQ output queue. She types:
```
CHGPRTF FILE(CONTRACTS/PRCLST1) OUTQ(CONTRACTS/PRICEQ)
```

To assign all the price list reports to the PRICEQ output queue, Sharon could use a generic printer file name:
```
CHGPRTF FILE(CONTRACTS/PRCLST*) OUTQ(CONTRACTS/PRICEQ)
```

To direct all new contracts to the NEWCP output queue, Sharon could change the output queue associated with the sample document that is used to create contracts.

Checking your work

The best way to check your protection strategy for confidential printer output is to print it. Check to see if it goes to the correct output queue. Sign on as the system operator, and see if you can look at or manipulate the files on the queue.

Before you secure workstations, be sure that you:
- Create any output queues listed on your Output Queue and Workstation Security Form by using the CRTOUTQ command.
- Assign printer output to the new output queues by using the CHGPRTF command.

Securing workstations

After you secure printer output, you should secure your workstations. You authorize workstations just like you authorize other objects on the system. Use the EDTOBJAUT command to give users authority to workstations.

Users must have *CHANGE authority to sign on at a workstation. If the QLMTSECOFR system value is no (0), the security officer or anyone with *ALLOBJ authority can sign on at any workstation.

If the QLMTSECOFR system value is yes (1), use these guidelines to set authority to workstations:

Users Allowed to Sign On at Workstation	Public Authority	QSECOFR Authority	Individual User Authority
All users	*CHANGE	*CHANGE	Not required
Only selected users	*EXCLUDE	No authority	*CHANGE
Selected users and users with authority to all objects	*EXCLUDE	*CHANGE	*CHANGE
All users except users with authority to all objects	*CHANGE	No authority	Not required

Before you restrict access to the system operator message queue, use the EDTOBJAUT command to secure workstations, based on the information in your Output Queue and Workstation Security form.

Restricting access to the system operator message queue

You can improve security by securing printer output, securing workstations, and restricting access to the system operator message queue.

The option for handling messages on the ASSIST menu allows users to use a function key to display the system operator (QSYSOPR) message queue. Incorrect responses to system operator messages can cause problems on your system. Users require *CHANGE authority to respond to and delete messages in a message queue. Only system operators should have this authority. Consult your System Responsibilities form to see who should have the *CHANGE authority to the system operator message queue.

Use the EDTOBJAUT command:
1. Type EDTOBJAUT QSYSOPR *MSGQ and press the **Enter** key.
2. Press **F11** to display detailed object authority information.
3. Give the public *OBJOPR authority, as shown on the sample display, and press the **Enter** key.

```
                    Edit Object Authority

Object . . . . . . . :   QSYSOPR        Owner  . . . . . . . :    QSYS
  Library  . . . . . :     QSYS         Primary group  . . . :    *NONE
Object type  . . . . :  *MSGQ

Type changes to current authorities, press Enter.

  Object secured by authorization list  . . . . . . . . . . .    *NONE


                      Object    ----------Object-----------
User        Group     Authority Opr  Mgt  Exist  Alter  Ref
*PUBLIC               USER DEF   X
```

4. The system changes the *Object Authority* column to USER DEF (User defined).
5. Press **F11** again to display detailed data authority information.
6. Give the public *ADD authority, as shown on the sample display, and press the **Enter** key.

```
                    Edit Object Authority

Object . . . . . . . :   QSYSOPR        Owner  . . . . . . . :    QSYS
  Library  . . . . . :     QSYS         Primary group  . . . :    *NONE
Object type  . . . . :  *MSGQ

Type changes to current authorities, press Enter.

  Object secured by authorization list  . . . . . . . . . . .    *NONE


                      Object    --------------Data---------------
User        Group     Authority Read  Add  Update  Delete  Execute
*PUBLIC               USER DEF         X
```

7. Use **F6** (Add Users) to add users who need to respond to QSYSOPR messages. Give them *CHANGE authority.

Attention: Do not make the public authority *EXCLUDE. All jobs (and users) must be able to add messages to the QSYSOPR message queue.

To ensure that you have finished setting up resource security, you should:
- Use your Authorization List forms and your Library Description forms to make sure that you have established security for all your application libraries.

- Check your Output Queue and Workstation Security form to make sure that you have protected workstations and created any special output queues.
- Restrict access to the system operator (QSYSOPR) message queue.
- Save your application libraries according to the instructions provided with the applications. The system saves ownership and public authority information with the application.
- Use the Save Security Data (SAVSECDTA) command to save the security information that you have created. See "Saving security information" for more information on how to save security information.

You can now begin testing your security setup.

Testing security

This topic describes techniques for testing the security you have set up on your system. Testing in this context means making sure that what you have set up works in the way you intended. The topic "Monitoring security" discusses how to evaluate the effectiveness of security on your system.

Test security whenever you make major changes on your system. This could be adding a new application, setting up resource security for an existing application, adding a new user group, or changing the security level.

Review these topics to learn about methods for testing and for diagnosing problems when you make security changes:
- Testing user profiles.
- Testing resource security.

Testing user profiles

To begin testing your security, you will want to test a user profile whenever you set up a new group on your system. Test one of the individual profiles that you copied from the group profile.
- Can you sign on successfully with the user profile? If you cannot sign on, check the job log that was written for the unsuccessful sign-on attempt. Use the Work with Printer Output option from the ASSIST menu to locate the job log for more information.

  These are the most likely problems:
  - One of the objects that is needed, such as the initial menu, the current library, or the initial program, does not exist.
  - The library list that is specified in the job description causes errors. Either a library does not exist, or you forgot to include QGPL and QTEMP in the library list.
  - The user does not have authorization to the workstation.
- When you sign on, does the screen display the correct initial menu or program?
- If you enter an initial menu or current library on the Sign On display, what happens? If the user profile is Limited Capabilities (YES), you should get an error message.
- Do you get the correct display when you press the Attention key?
- Does output go to the correct printer? If not, use the Work with Printer Output option from the ASSIST menu to find out where it went. Check the user profile and job description to determine why the output went to a different printer.
- Can you get a command line?
- Can you perform the required application functions without security errors? See "Testing resource security" for more details.
- Can you perform necessary system tasks, such as managing printers or saving libraries?

If the system required you to assign a new password when you signed on with a profile, set the password back to the user profile name after you complete testing:

1. Sign on with your own profile (with security officer authority).
2. Type `CHGUSRPRF` *profile-name* `PASSWORD(`*profile-name*`) PWDEXP(*YES)`.

Now that you have tested the user profiles, you can test resource security.

Testing resource security

After testing user profiles, you should test your resource security as well. When you test resource security, you look for the following:

- Users who do not have enough authority to do their jobs.
- Users who have more authority than you intended.

Testing for insufficient authority

Test both interactive and batch functions to see if user profiles have enough authority.

Interactive testing

To test your resource security for an application, you may need to sign on with several different user profiles. Your objective is to test sample users to make sure that the authority you have assigned is sufficient.

- Test functions which require different levels of authority: viewing, changing, and deleting.
- Test programs, not just menus. Selecting a menu option may not be sufficient to test authority. Sometimes the system does not access a file until you actually try to perform an operation, such as deleting a record. Authority checking occurs when you have the system open a file. Application design determines when the system opens the file.
- Keep a record of security errors and resolve them. If an authority error occurs, you should see a message at your display telling you that you have insufficient authority for the operation and what object you were trying to use.

Batch testing

- Run sample batch jobs from the application using the profiles of users who will submit the jobs.
- Test batch jobs which require different levels of authority, such as: printing information, changing information, or clearing files at month-end.
- Check the QSYSOPR message queue and the QHST log for security errors. Use the DSPLOG command to view the QHST log. Security messages are in these ranges: CPF2200, CPI2200, CPC2200, CPD2200, CPF4A00, CPI4A00, CPC4A00, and CPD4A00.

  You can also use the security auditing function to log authority failures and other security-related events.

Testing for too much authority

If you set up resource security to protect confidential information, test sample user profiles to make sure that your security works. Sign on with the profile of a user who should not be able to access the confidential file.

- Can you get to a menu that allows access to the file?
- What happens if you select a menu option that uses the file?
- Can you get a command line?
- Can you run a command to list the file, such as `CPYF FROMFILE(`*file-name*`) TOFILE(QSYSPRT)`?
- Can you use a query tool to look at the file?

Your testing results may indicate that you need to change security information.

Changing security information

Now that you have planned the security for your system, you need to ensure that your plan remains effective as your business needs change.

This topic emphasizes simplicity as an essential goal in designing security. You have designed user groups as patterns for individual users. You have tried to use public authority, authorization lists, and library authority rather than specific individual authorities. Take advantage of that approach as you manage security:

- When you add a new user group or a new application, use the techniques that you used to plan security.
- When you need to make changes to security, try to take a general approach rather than creating an exception to solve a specific problem.

The topic Security commands describes what commands to use to display, change, and delete security information.

See these topics for suggestions about dealing with different types of changes:

- Adding a new user to the system.
- Creating a new user group.
- Changing a user group.
- Adding a new application.
- Adding a new workstation.
- Changing a user's responsibility.
- Removing a user from the system.

Security commands

The table below shows what commands you use to work with security objects on the system. You can use these commands to perform these tasks:

- View and list security information.
- Change security information.
- Delete security information.

Table 63. Security Commands

Security Object	How to View	How to Change	How to Delete
System Value	WRKSYSVAL DSPSYSVAL	WRKSYSVAL CHGSYSVAL	Cannot be deleted
Job Description	WRKJOBD DSPJOBD	WRKJOBD CHGJOBD	DLTJOBD
Group Profile	WRKUSRPRF DSPUSRPRF DSPAUTUSR	WRKUSRPRF CHGUSRPRF	DLTUSRPRF[1,2]
User Profile	WRKUSRPRF DSPUSRPRF DSPAUTUSR	WRKUSRPRF CHGUSRPRF CHGUSRAUD	DLTUSRPRF[1]
Object Authorities	DSPAUT DSPOBJAUT DSPUSRPRF TYPE(*OBJAUT)	CHGAUT EDTOBJAUT GRTOBJAUT WRKAUT	EDTOBJAUT RVKOBJAUT WRKAUT

Table 63. Security Commands (continued)

Security Object	How to View	How to Change	How to Delete
Object Ownership	WRKOBJOWN DSPOBJAUT DSPUSRPRF TYPE(*OBJOWN)	CHGOBJOWN CHGOWN	CHGOBJOWN CHGOWN allows you to revoke the rights of the previous owner.
Primary Group	DSPOBJAUT WRKOBJPGP DSPUSRPRF TYPE(*OBJPGP)	CHGOBJPGP CHGPGP	CHGOBJPGP CHGPGP set primary group to *NONE
Object Auditing	DSPOBJD	CHGOBJAUD CHGAUD	CHGOBJAUD (set to *NONE) CHGAUD
Authorization List	DSPAUTL DSPAUTLOBJ	EDTAUTL (user authority to a list) EDTOBJAUT (object secured by list) ADDAUTLE CHGAUTLE GRTOBJAUT	DLTAUTL (entire list)[3] RMVAUTLE (remove user authority to the list) EDTOBJAUT (object secured by list) RVKOBJAUT

1. IBM recommends using the remove option from the Work with User Enrollment display for deleting a profile. Using this option, you can delete any objects that are owned by the profile or reassign them to a new owner. Certain DLTUSRPRF command parameters allow you to delete all objects that are owned by the user or assign them all to a new owner. You cannot delete a profile unless you delete or reassign owned objects. You also cannot delete a profile that is the primary group for any objects.

2. You cannot delete a group profile that has any members. Use the *GRPMBR option of the DSPUSRPRF command to list the members of the group. Change the *group profile* field in each of the individual group profiles before deleting the group profile.

3. You cannot delete an authorization list that is used to secure objects. Use the DSPAUTLOBJ command to list the objects that are secured by the list. Change the authority of any objects that are secured by the list by using the EDTOBJAUT command.

Viewing and listing security information

You can list security information by using a display (DSP) command with a print (*PRINT) option. For example, to display an authorization list called MYLIST, type `DSPAUTL MYLIST *PRINT`.

Some display commands provide options for different types of lists. For example, when you created individual user profiles, you used the *GRPMBR option of the DSPUSRPRF command to list all the members of a group profile. Use prompting (**F4**) and online information to find out what lists are available for security objects.

You can use the Display commands to view security information at your display station. You can also use the Work with... (WRK) commands, which provide more function. The Work with... commands give you a list display. You can use this display to change, delete, and view information.

You can also use security commands to list or view information by using a generic name. If you type `WRKUSRPRF DPT*`, your Work with User Enrollment display or Work with User Profile display shows only profiles that start with the characters *DPT*. Use online information for a command to find out which parameters allow generic names.

Changing security information

You can change security information interactively by using a Work with... (WRK) or Edit... (EDT) command. You can view the information, change it, and view the information again after the change.

You can also change security information without viewing it before and after the change by using a Change... (CHG) or Grant... (GRT) command. This method is particularly useful for making a change to more than one object at a time. For example, you used the GRTOBJAUT command to set public authority for all the objects in a library (see "Setting public authority for all objects in a library" on page 95).

Deleting security information

You can delete or remove certain types of security information interactively by using the Work with... (WRK) or Edit... (EDT) commands. You can also use Delete... (DLT), Remove... (RMV), and Revoke... (RVK) commands to delete security information. Often, you must meet certain conditions before the system allows you to delete security information. The notes that are in Security commands describe some of those conditions.

Adding a new user to the system

When you need to add a new user to the system, use the following procedure:

1. Assign the person to a user group. Use the User Group Description form for reference.
2. Decide if the new user needs to perform system functions. If so, add that information to the System Responsibilities form.
3. Add the person to the Individual User Profile form.
4. Review the System Responsibilities form and the User Group Description form to determine if the new user needs values that are different from those of the group.
5. Create a user profile by copying the group profile or the profile of a group member. Be sure to set the password to expire. (See "Copying the group profile.")
6. Give the new user a copy of your security memo.

To learn how to create a new user group, see "Creating a new user group."

Creating a new user group

You might need to create new user groups for several reasons:

- Additional departments need to use the system.
- You discover that you need to make user groups more specific to meet your resource security needs.
- Your company reorganized some departments.

To create a new user group, do the following:

1. Fill out a User Group Description Form by following the instructions in "Planning user groups."
2. Add the user group to your diagram of applications, libraries, and user groups.
3. Evaluate whether any group members need to perform system functions. Update your System Responsibilities form. (See "Determining who should be responsible for system functions.")
4. Use the information from the User Group Description form and the System Responsibilities form to fill out an Individual User Profile form.
5. Create a group library.
6. Create a job description for the group.
7. Create a group profile.

   Note: See "Setting up user groups" for instructions on performing steps five, six, and seven.
8. Create individual user profiles for the group members. (See "Setting up individual users.")
9. Evaluate the Library Description forms for all the applications that are needed by the group. Take whatever steps are necessary to give the group access to application objects by using the techniques described in " Setting up resource security."
10. Give all the members of the group a copy of your security memo.

To learn how to change a user group, see "Changing a user group."

Changing a user group

You will need to handle different types of changes to the characteristics of a group in different ways. Following are some examples of changes and how to deal with them:

Changing the group's authority

You may discover that the group needs authority to objects that you did not anticipate in your initial planning. Do the following:

1. Use the Edit Object Authority (EDTOBJAUT) command to give the group the correct access to the objects or to an appropriate authorization list. "Setting up specific authorities" on page 99 shows an example of how to do this. Every member of the group gets authority to the object when you give the group authority.
2. If you give the group authority to a confidential resource, you may want to verify the current members of the group. Use the Display User Profile command (DSPUSRPRF *group-profile-name* *GRPMBR) to list the group members.

Changing the customizing for the group

You may need to change the user environment setup for members of a group. For example, if a department gets its own printer, you want the new printer to be the default for the members of that department's user group. Or, when your system gets a new application installed, members of a user group may want a different initial menu when they sign on.

The group profile provides a pattern that you can copy to create individual profiles for group members. The customizing values in the group profile do not affect the individual user profiles after you create them, however. For example, changing a field, such as *Printer device* in the group profile, has no affect on the group members. You need to change the *Printer device* field in each individual user profile.

You can use the Work with User Profile display to change a parameter for more than one user at a time. The example shows changing the output queue for all members of a group:

1. Type WRKUSRPRF *ALL and press the **Enter** key.
2. If you see the Work with User Enrollment display, use **F21** (Select assistance level) to change to the Work with User Profile display.

```
                    Work with User Profiles

 Type options, press Enter.
   1=Create   2=Change   3=Copy   4=Delete   5=Display
   12=Work with objects by owner

         User
 Opt     Profile      Text

           HARRISOK        Harrison, Keith
 2         HOGANR          Hogan, Richard
           JONESS          Jones, Sharon
 2         WILLISR         Willis, Rose

    :
    :
                                                    More...
 Parameters for options 1, 2, 3, 4 and 5 or command
 ===> PRTDEV(PRT02)
 F3=Exit   F5=Refresh   F12=Cancel   F16=Repeat position to   F17=Position to
 F21=Select assistance level        F24=More keys
```

3. Type a **2** (Change) next to each profile that you want to change.

4. On the parameter line at the bottom of the display, type the parameter name and the new value. If you do not know the parameter name, press **F4** (Prompt).

5. Press the **Enter** key. You receive a confirmation message for each profile that changed.

   Although changing a customizing field in the group profile has no affect on the group members, it may help you in the future. The group profile provides a pattern when you want to add members to the group later. It is also a record of the standard field values for the group.

Giving the group access to a new application

When a user group needs access to a new application, you need to analyze information about the group and about the application. Following is a suggested method:

1. Look at the Application Description form for the new application and your diagram of applications, libraries, and user groups to see which libraries the application uses. Add those libraries to the User Group Description form.

2. Update your diagram of applications, libraries, and user groups to show the new relationship between the user group and application.

3. If the group's initial library list should include the libraries, change the group's job description by using the Change Job Description (CHGJOBD) command. See "Creating a job description" on page 83 if you need help for working with job descriptions.

   Note: When you add libraries to the initial library list in a job description, you do not need to change the user profiles that use the job description. When the user signs on next, their initial library list automatically adds those libraries.

4. Evaluate whether you need to change either the initial program or the initial menu for the group to provide access to the new application. You need to make an individual change to the initial menu or program of each user profile by using the CHGUSRPRF command.

5. Review the Library Description forms for all the libraries that are used by the application. Determine whether the public access that is available for the libraries is sufficient for the group's needs. If it is not, you may need to give the group authority to the library, to specific objects, or to authorization lists. Use the Edit Object Authority (EDTOBJAUT) and the Edit Authorization List (EDTAUTL) commands to do this. (See "Setting up resource security" if you need more information.)

To add applications to your system, see "Adding a new application."

Adding a new application

You should plan the security for any new applications as carefully as you planned for your original applications. Follow the same procedures:

1. Prepare an Application Description form and Library Description forms for the application.

2. Update your diagram of applications, libraries, and user groups.

3. Follow the procedures in "Planning resource security" to decide how to secure the new application.

4. Prepare an Application Installation form by using the method described in "Planning your application installation."

5. Evaluate whether any printer output from the application is confidential and needs protection. Update your Output Queue and Workstation Security form, if necessary.

6. Follow the steps described in "Setting up ownership and public authority" and "Setting up resource security" to install and secure the application.

To add a workstation to your system, see "Adding a new workstation."

Adding a new workstation

When you add a new workstation to your system, consider security requirements:

1. Does the physical location of a new workstation pose any security risks? (See "Planning physical security" to refresh your memory.)

2. If the workstation does pose a risk, update your Output Queue and Workstation Security form.

3. You should normally create new workstations with public authority *CHANGE. If this does not meet your security requirements for the workstation, use the EDTOBJAUT command to specify a different authority.

To change a user's responsibility on the system, see "Changing a user's responsibilities."

Changing a user's responsibilities

When a system user gets a new job or a new set of responsibilities in your company, you need to evaluate how that affects the user profile.

1. Should the user belong to a different user group? You can use the CHGUSRPRF command to change the user group.

2. Do you need to change any customizing values in the profile, such as the printer or the initial menu? You can use the CHGUSRPRF command to change these also.

3. Are the application authorities of the new user group sufficient for this person?
   - Use the Display User Profile (DSPUSRPRF) command to look at the authorities for the old and new group profiles.
   - Also look at the authorities of the individual user profile.
   - Make any changes necessary by using the EDTOBJAUT command.

4. Does the user own any objects? Should you change ownership of those objects? Use the Work with Objects by Owner (WRKOBJOWN) command.

5. Does the user perform system functions? Does the user need to perform system functions for the new job? Update the System Responsibilities form and change the user profile, if necessary.

To learn how to remove a user from the system, see "Removing a user from the system."

Removing a user from the system

If someone leaves your company, you should remove the user profile from the system immediately. Before you can delete a user profile, you must either delete or transfer ownership of any objects that are owned by the profile. You can use the WRKOBJOWN command to do this, or you can use option **4** (Remove) from the Work with User Enrollment display.

When you select option **4** (Remove) for a profile from the Work with User Enrollment display, you see additional displays that allow you to handle any objects the user owns. You can choose to give all the objects to a new owner or handle the objects individually:

```
                        Remove User

User . . . . . . . . . . . :   HOGANR
User description . . . . . :   Sales and Marketing Department

To remove this user type a choice below, then press Enter.

    1. Give all objects owned by this user to a new owner
    2. Delete or change owner of specific objects owned by this user.
```

If you choose to handle the objects individually (option **2**), the screen displays a list of all the objects that are owned by the user:

```
                          Remove User

User . . . . . . . . . . . :   HOGANR
User description . . . . . :   Sales and Marketing Department

New owner  . . . . . . . . .                 Name, F4 for list

To remove this user, delete or change owner of all objects.
Type options below and press Enter.
   2=Change to new owner   4=Delete   5=Display details

Opt  Object       Library      Description
 4   HOGANR       QUSRSYS      Hogan, Richard message queue
 4   QUERY1       DPTWH        Inventory Query
```

If you choose to delete objects, you see the Confirm Delete display. Once the system deletes the objects, you can remove the user profile. You then see the Work with User Enrollment display again with a message that tells you that the system has removed the user.

Saving security information

This topic presents an overview of how you save and restore security information. When you plan the backup and recovery of your system, you need to consider the security of your information as well as the information itself. See the Information Center topic, Backup, Recovery, and Availability to help you design a complete backup and recovery plan.

The following topics describe how you back up and restore the security information that you create when you set up security:
* Saving system values.
* Saving group and user profiles.
* Saving job descriptions.
* Saving resource security information.
* Using the default owner profile (QDFTOWN).
* Recovering from a damaged authorization list.

Saving system values

System values are stored in the system library, QSYS. You save the QSYS library when you do the following:
* Use the Save System (SAVSYS) command.
* Use the option to save the entire system from the Save menu.
* Use the option to save system information from the Save menu.
* Use the option to back up the entire system from the Run Backup (RUNBCKUP) menu.

If you need to recover your entire system, you automatically restore your system values when you restore your operating system.

See "Saving group and user profiles" next.

Saving group and user profiles

Group and user profiles are stored in the QSYS library. You save them when you use the Save System (SAVSYS) command or select the menu option to save the entire system.

You can also save group and user profiles by using the Save Security Data (SAVSECDTA) command.

Restore user profiles by using the Restore User Profile (RSTUSRPRF) command. The normal sequence follows:

1. Restore the operating system, which restores library QSYS.
2. Restore user profiles.
3. Restore the remaining libraries.
4. Restore authority to objects using the Restore Authority (RSTAUT) command.

See "Saving job descriptions" next.

Saving job descriptions

When you create a job description, you specify a library where it should reside. IBM recommends creating job descriptions into the QGPL library.

You can save job descriptions by saving the library in which they reside. Use the Save Library (SAVLIB) command to do this. You can also save a job description by using the Save Object (SAVOBJ) command.

You can restore the contents of a library by using the Restore Library (RSTLIB) command. You can restore an individual job description by using the Restore Object (RSTOBJ) command.

See "Saving resource security information" next.

Saving resource security information

Resource security, which defines how users can work with objects, consists of different types of information that is stored in several different places:

Table 64. Saving and restoring resourse security information

Type of Information	Where It Is Stored	How It Is Saved	How It Is Restored
Public authority	With the object	SAVxxx command [1]	RSTxxx command [2]
Object auditing value	With the object	SAVxxx command [1]	RSTxxx command [2]
Object ownership	With the object	SAVxxx command [1]	RSTxxx command [2]
Primary group	With the object	SAVxxx command [1]	RSTxxx command [2]
Authorization list	QSYS library	SAVSYS or SAVSECDTA	RSTUSRPRF USRPRF(*ALL)
Link between object and authorization list	With the object	SAVxxx command [1]	RSTxxx command [2]
Private authority	With user profile	SAVSYS or SAVSECDTA	RSTAUT

1. You can save most object types by using the SAVOBJ or SAVLIB commands. Some object types, such as configurations, have a special save command.

2. You can restore most object types by using the RSTOBJ or RSTLIB commands. Some object types, such as configurations, have a special restore command.

When you need to recover an application or your entire system, you need to plan the steps carefully, including recovery of the authority to objects. Following are the basic steps necessary to recover the resource security information for an application:

1. If necessary, restore user profiles, including the profiles which own the application. You can restore specific profiles or all profiles with the RSTUSRPRF command.

2. Restore any authorization lists that are used by the application. You restore authorization lists when you use RSTUSRPRF USRPRF(*ALL).

   Note: This restores all the user profile values, including passwords, from the backup media.

3. Restore the application libraries by using the RSTLIB or RSTOBJ command. This recovers object ownership, public authority, and the links between objects and authorization lists.
4. Restore private authority to objects by using the RSTAUT command. The RSTAUT command also restores user authorities to authorization lists. You can restore authority for specific users or all users.

See "Using the default owner profile (QDFTOWN)" for information on restoring an object and owner profile that is not on your system.

Using the default owner profile (QDFTOWN)

If you restore an object and the owner profile is not on the system, the system transfers ownership of the object to a default profile that is called QDFTOWN. Once you recover the owner profile or create it again, you can transfer ownership back by using the Work with Object by Owner (WRKOBJOWN) command.

For information on authorization list recovery, see "Recovering from a damaged authorization list."

Recovering from a damaged authorization list

When an authorization list secures an object and the authorization list becomes damaged, only users who have all-object (*ALLOBJ) special authority have access to the object.

Recovering from a damaged authorization list requires two steps:
1. Recover users and their authorities on the authorization list.
2. Recover the association of the authorization list with the objects.

A user with *ALLOBJ special authority can accomplish these steps.

Step 1: Recovering the authorization list

If you know the user authority to the authorization list, delete the authorization list, create it again, and add users to it.

If you do not know all the user authorities to the authorization list, restore it from your last SAVSYS or SAVSECDTA tapes by using these steps:
1. Delete the damaged authorization list:

   ```
   DLTAUTL AUTL(authorization-list-name)
   ```
2. Restore the authorization list:

   ```
   RSTUSRPRF USRPRF(*ALL)
   ```
3. Add users to the list by using the Restore Authority (RSTAUT) command.

Step 2: Recovering the association of objects to the authorization list

When you have restored the authorization list or created it again, you need to establish the link between the list and the objects secured by the list:
1. Use the Reclaim Storage (RCLSTG) command. RCLSTG assigns objects that are secured by damaged or missing authorization lists to a default list that is called QRCLAUTL.
2. List the objects that are secured by the QRCLAUTL authorization list:

   ```
   DSPAUTLOBJ AUTL(QRCLAUTL)
   ```
3. Use the GRTOBJAUT command to secure the objects with the correct authorization list. For example, to secure the ARWRK01 file in the CUSTLIB library with authorization list ARLST01, type

   ```
   GRTOBJAUT OBJ(CUSTLIB/ARWRK01) OBJTYPE(*FILE) +
             AUTL(ARLST01)
   ```

Monitoring security

This topic provides basic suggestions for monitoring the effectiveness of the security safeguards on your system.

Monitoring security regularly has two basic goals:
- Making sure that you protect your company resources adequately.
- Detecting unauthorized attempts to access your system and your company's information.

Review your security policy statement and your security memo to users as you decide which monitoring tasks you need to perform regularly.

See the following topics for more information on monitoring security:
- Checklists for monitoring security.
- Security auditing.

Checklists for monitoring security

Following are checklists for reviewing different aspects of security on your system. Use them to develop your plan.

Monitoring physical security
- Protect backup media from damage and theft.
- Restrict access to workstations in public areas. Use the DSPOBJAUT command to see who has *CHANGE authority to the workstations.

Monitoring system values
- Verify that the settings match your System Values Selection form. Use the Print System Security Attributes (PRTSYSSECA) command.
- Review your decisions about system values, particularly when you install new applications.

Monitoring group profiles
- Verify that group profiles have no passwords. Use the DSPAUTUSR command to verify that all group profiles have a password of *NONE.
- Verify that the correct people are members of the group. Use the DSPUSRPRF command with the *GRPMBR option to list the members of a group.
- Check the special authorities for each group profile. Use the DSPUSRPRF command. If you are running at security level 30, 40, or 50, group profiles should not have *ALLOBJ authority.

Monitoring user profiles
- Verify that user profiles on the system belong to one of these categories:
  - User profiles for current employees
  - Group profiles
  - Application owner profiles
  - IBM-supplied profiles (start with Q)
- Remove their user profile when the company transfers a user or when a user leaves the company. Use the Change Expiration Schedule Entry (CHGEXPSCDE) command to automatically delete or disable the profile as soon as the user leaves.
- Look for inactive profiles and remove them. Use the Analyze Profile Activity (ANZPRFACT) command to automatically disable profiles after they have been inactive for a certain time.

- Determine which users have a password that is the same as their user profile name. Use the Analyze Default Passwords (ANZDFTPWD) command. Use the option of this command to force users to change their passwords the next time they sign on to the system.

  Attention: Do not remove any IBM-supplied profiles from the system. IBM-supplied profiles start with the character Q.
- Be aware of who has a user class other than *USER and why. Use the Print User Profile (PRTUSRPRF) command to get a list of all users, their user class, and their special authorities. Match this information with your System Responsibilities form.
- Control which user profiles have the *Limit capabilities* field set to *NO.

Monitoring critical objects
- Review who has access to critical objects. Use the Print Private Authorities (PRTPVTAUT) command and the Print Publicly Authorized Objects (PRTPUBAUT) command to monitor objects. If a group has access, verify the members of the group with the *GRPMBR option of the DSPUSRPRF command.
- Verify who can use application programs that provide access to objects through another security method, such as adopted authority. Use the Print Adopting Objects (PRTADPOBJ) command.

Monitoring unauthorized access
- Instruct system operators to be alert for security messages in the QSYSOPR message queue. In particular, have them notify a security officer of repeated unsuccessful attempts to sign on. Security messages are in the range of 2200 to 22FF and 4A00 to 4AFF. They have prefixes CPF, CPI, CPC, and CPD.
- Set up security auditing to log unauthorized attempts to access objects.

See Security auditing next.

Security auditing

When monitoring your security, the operating system can log security events which occur on your system. These events are recorded in special system objects called **journal receivers**. You can set up journal receivers to record different types of security events, such as changing a system value or user profile, or an unsuccessful attempt to access an object. The following values control which events are logged:
- The audit control (QAUDCTL) system value
- The audit level (QAUDLVL) system value
- The audit level (AUDLVL) value in user profiles
- The object auditing (OBJAUD) value in user profiles
- The object auditing (OBJAUD) value in objects.

The information in the audit journals is used:
- To detect attempted security violations.
- To plan migration to a higher security level.
- To monitor the use of sensitive objects, such as confidential files.

Commands are available to view the information in the audit journals in different ways.

Basic system security planning forms

You can copy or print these forms from a browser.

To print the entire security-basic information, select the right pane, and then click the PDF icon in the Information Center banner.

To print a single planning form, click on the link that corresponds with the planning form that you would like to print. Click the right pane, and then click the Print icon in your browser. This will print the selected form for you.

Here is a complete listing of all the planning forms that are necessary for you to successfully plan and use your basic system security:
- Physical Security Planning form
- Application Description form
- Naming Conventions form
- Library Description form
- System Values Selection form
- System Responsibilities form
- User Group Identification form
- User Group Description form
- Individual User Profile form
- Authorization List form
- Output Queue and Workstation Security form
- Application Installation form

Physical Security Planning form

Table 65. Physical Security Planning form

Physical Security Planning form	
Prepared by:	Date:
Instructions • Learn about this form in "Planning resource security." • Use this form to describe any security issues that are related to the physical location of your system unit and attached devices. • You do not need to enter the information on this form into the system.	
System unit:	
Describe your security measures to protect the system unit (such as a locked room):	
What keylock position is normally used?	
Where is the key kept?	
Other comments relating to the system unit:	
Backup media and documentation:	
Where are backup tapes stored at your business location?	
Where are backup tapes stored away from your business location?	
Where are the security officer, service, and DST passwords kept?	
Where is important system documentation, such as the serial number and the configuration, kept?	

Physical Security Planning form	Part 2 of 2

Additional instructions for Part 2
• List below any workstations or printers whose location might cause security exposures. Indicate what protective measures you will take. For a printer, list examples of confidential printed reports under the *Security Exposure* column.
• If you allow the system to automatically configure your local devices, you may not know the names of workstations and printers until after your system is installed. If you do not know the names when you prepare this form, fill in the descriptions (such as location) and add names later.

Physical security of workstations and printers			
Workstation or printer name	Its location or description	Security exposure	Protective measures to be taken

Application Description form

Table 66. Application Description form

Application Description form	
Prepared by:	Date:
Instructions • Learn about this form in ″Describing your application″ and ″Planning resource security.″ • Prepare a separate form for each application. • You do not need to enter the information on this form into the system.	
Application name:	Abbreviation:
Brief description of the application:	
Primary menu name:	Library:
Initial program name:	Library:
List the libraries used by the application for both files and programs:	
Define the security objectives for the application, such as whether any information is confidential:	

Naming Conventions form

Table 67. Naming Conventions form

Naming Conventions form	
Prepared by:	Date:
Instructions • Learn about this form in ″Describing your applications .″ • You do not need to enter information from this form directly into the system. • Use this form to describe how you will assign names to the objects on your system. Give examples of each one.	
Type of object	**Naming convention**

Table 67. Naming Conventions form (continued)

Group profiles	
User profiles	
Authorization lists	
Libraries	
Files	
Calendars	
Devices	
Tapes	

Library Description form

Table 68. Library Description form

Library Description form	Part 1 of 2
Prepared by:	Date:
Instructions: • Learn about this form in ″Planning user security″ and ″Planning resource security.″ • Use this form to describe your main libraries and define resource security requirements for them. • Fill out one form for each major application library on your system. • Learn how to enter the information from this form in ″Setting up resource security.″	
Library name:	Descriptive name (text):
Briefly describe the function of this library:	
Define the security objectives for the library, such as whether any information is confidential:	
Public authority to the library:	
Public authority to objects in the library:	
Public authority for new objects (CRTAUT):	
Library owner:	

Library Description form				Part 2 of 2
Prepared by:			Date:	
Library name:				
Additional instructions for Part 2: • In the chart below, list any individuals or objects requiring specific authority. • Specify the type of authority required: *ALL, *CHANGE, *USE, or *EXCLUDE.				
List specific authorities for library objects				
Group profile or user profile	Object name	Object type	Authority needed	Authorization list

System Values Selection form

Table 69. System Values Selection form

System Values Selection form		Part 1 of 2
Prepared by:		Date:
Instructions • Learn more about this form in ″ Planning your overall approach.″ • Use this form to record your choices for the system values that affect security and customizing. • Use option **1** from the SETUP menu to enter Part 1 of this form.		
Values from the Change System Options display		
System value/network attribute	**Recommended choice**	**Your choice**
System name		
Date separator (QDATSEP)		
Date format (QDATFMT)		
Time separator (QTIMSEP)		
Device naming format for new devices (QDEVNAMING)	1 (iSeries system)	
System printer (QPRTDEV)		
Security level (QSECURITY)	40	
Allow security officers to sign on to any display station (QLMTSECOFR)	N	
Save job accounting information about completed printer output (QACGLVL)	N (*NONE)	

System Values Selection form		Part 2 of 2
Additional instructions for Part 2 • Learn more about Part 2 of this form in ″Setting system values.″ • Use the Work With System Value (WRKSYSVAL) command to enter Part 2.		
Security system values		
System value	**Recommended choice**	**Your choice**
Inactive job time-out interval (QINACTITV)	30 to 60	
Inactive job message queue (QINACTMSGQ)	*DSCJOB	
Limit device sessions (QLMTDEVSSN)	1 (YES)	
Action to take for failed sign-on attempts (QMAXSGNACN)	3 (Disable both)	
Maximum sign-on attempts allowed (QMAXSIGN)	3 to 5	
Password expiration interval (QPWDEXPITV)	30 to 60	
Maximum password length (QPWDMAXLEN)	8	

Minimum password length (QPWDMINLEN)	6	
Require different passwords (QPWDRQDDIF)	7 (6 unique passwords)	
Other system values		
System value	**Recommended choice**	**Your choice**
Disconnected job time-out interval (QDSCJOBITV)	300	
Note: You may want to set some other security-related system values. See Chapter three of the *Security-Reference* (SC41-5302-04) for the complete list of security-related system values and the recommendations for them.		

System Responsibilities form

Table 70. System Responsibilities form

System Responsibilities form			
Prepared by:		Date:	
Instructions: • Learn about this form in ″Planning individual user profiles.″ • Use this form to list everyone who has a user class other than *USER. • Transfer information from this form to the *User Class* column of the Individual User Profile form.			
Who is your primary security officer? Who is your backup security officer?			
Profile name	User name	Class	Comments

User Group Identification form

Table 71. User Group Identification form

User Group Identification form								
Prepared by:		Date:						

Instructions:
• Learn about this form in ″Planning user groups.″
• This form helps you identify groups of users who have similar application needs.
  1. List your major applications across the top of the form.
  2. List your users in the left-hand column.
  3. Mark needed applications for every user.
• You do not need to enter the information on this form into the system.								

		Access needed for applications						
User name	Department	APP:	APP:	APP:	APP:	APP:	APP:	APP:

Table 71. User Group Identification form (continued)

Note:
- If you have a *relaxed* security environment, use an **X** to mark which applications users need.
- If you have a *strict* security environment, you may need to use **C** (change) and **V** (view) to specify *how* the applications are used.

User Group Description form

Table 72. User Group Description form

User Group Description form	Part 1 of 2
Prepared by:	Date:

Instructions for Part 1
- Learn how to prepare this form in "Planning user groups."
- Learn how to enter this form in "Setting up user security."
- Prepare a separate form for each group which will use the system.
- Use the Create Job Description (CRTJOBD) command to create a job description for the group. The job description has the initial library list of the group.

Group profile name:

Description of the group:

Primary application for the group:

List other applications needed by the group:

List each library the group needs. Mark (✔) each library that should be in the initial library list for the group:

Note: Look at the Application Description form for each application that is listed in the previous section to find out which libraries that application uses.

User Group Description form		Part 2 of 2
Additional instructions for Part 2		

- The tables below list all of the fields that appear on the Create User Profile display. The fields are divided into two groups: those where you need to make a choice and those where IBM recommends the default value.
- Use the Work with User Profiles display or the Create User Profile (CRTUSRPRF) command to enter the information from this part of the form into your system.

Choose values for these fields in the group profile:

Field name	Recommended choice	Your choice
Group profile name (User)		
Password	*NONE	
User class (Type of user)	*USER	
Current library (Default library)	*same as group profile name*	
Initial program to call (Sign on program)		

Initial program library		
Initial menu (First menu)		
Initial menu library		
Limit capabilities (Restrict command line use)	`*YES`	
Text (User description)		
Job description	*same as group profile name*	
Job description library		
Group profile name (User group)	`*NONE`	
Print device (Default printer)		
Output queue	`*DEV`	
Note: These fields are in the order in which they appear on the Create User Profile display (using F4).		
Use the system-supplied values (defaults) for the fields below:		
Accounting code	Keyboard buffering	Public authority
Assistance Level	Language ID	Set password to expire
Attention program	Limit device sessions	Sort sequence
Coded character set ID	Maximum storage	Special authority
Country or Region ID	Message queue	Special environment
Display sign-on information	Password expiration interval	Status
Document password	Priority limit	User options
Note: The fields in this list are arranged in alphabetical order.		

Individual User Profile form

Table 73. Individual User Profile form

Individual User Profile form						
Prepared by:			Date:			
Instructions: • Learn how to prepare this form in ″Planning individual user profiles.″ • Use this form to record information about individual system users. Fill out one form for each user group (group profile) that is on your system. • Use the blank columns at the right for any additional fields that you wish to specify for individual users. • Learn how to enter this form in ″Setting up individual users.″						
Group profile names:						
Owner of objects created:			Group authority to objects created:			
Group authority type:						
Make an entry for each member of the group:						
User profile	Text (description)	User class	Limit capability			

Table 73. Individual User Profile form (continued)

Authorization List form

Table 74. Authorization List form

Authorization List form					
Prepared by:			Date:		
Instructions • Learn about this form in ″Planning resource security.″ • Prepare one form for each authorization list. • Use the form to list the objects that the list and the groups and individuals who have access to the list secure. • Learn how to enter this form in ″Setting up resource security.″					
Authorization list name:					
Description:					
List the objects which the list secures					
Object name	Object type	Object library	Object name	Object type	Object library
List groups and users who have access to the list					
Group or user	Type of access allowed	List management?	Group or user	Type of access allowed	List management?

Printer Output Queue and Workstation Security form

Table 75. Printer Output Queue and Workstation Security form

Printer Output Queue and Workstation Security form				
Prepared by:		Date:		
Instructions • Learn about this form in "Protecting printer output." • Make an entry on this form for any workstation or output queue that requires special protection. • Learn how to enter this form in "Protecting workstations."				
List the parameters for restricted output queues:				
Output queue name	Output queue library	Display any file (DSPDTA)	Authority to check (AUTCHK)	Operator control (OPRCTL)
Security officer workstations: If you limit the security officer to specific workstations (system value QLMTSECOFR is yes), list below the workstations authorized for the security officer and anyone with *ALLOBJ authority:				
List below the authorities for restricted workstations:				
Workstation name	Groups or users who are authorized (*CHANGE authority)			
Note: Restricted workstations should have public authority set to *EXCLUDE.				

Application Installation form

Table 76. Application Installation form

Application Installation form		Part 1 of 2
Prepared by:		Date:
Instructions • Learn about this form in "Planning your application installation." • Prepare one form for each application that you will install. • Use the form to plan how you will establish ownership and public authority to your applications after you load them. • Learn how to enter this form in "Setting up resource security."		
Application name:		
Description:		
List and explain any profiles that must be created to install the application:		
Library name:		
	Before installation	After installation
Library owner		
Object owner		
Library public authority		

Table 76. Application Installation form (continued)

	Before installation	After installation
Object public authority		
Public authority for new objects		
Library name:		
	Before installation	After installation
Library owner		
Object owner		
Library public authority		
Object public authority		
Public authority for new objects		

Application Installation form	Part 2 of 2
Library name:	

	Before installation	After installation
Library owner		
Object owner		
Library public authority		
Object public authority		
Public authority for new objects		
Library name:		
	Before installation	After installation
Library owner		
Object owner		
Library public authority		
Object public authority		
Public authority for new objects		
Library name:		
	Before installation	After installation
Library owner		
Object owner		
Library public authority		
Object public authority		
Public authority for new objects		

Appendix. Notices

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

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

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

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

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, 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.

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 49XA
3605 Highway 52 N

129

Rochester, MN 55901
U.S.A.

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

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

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.

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

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

Trademarks

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

Application System/400
AS/400
e (logo)
IBM
iSeries
Operating System/400
OS/400
400

Lotus®, Freelance, and WordPro are trademarks of International Business Machines Corporation and Lotus Development Corporation in the United States, other countries, or both.

C-bus is a trademark of Corollary, Inc. in the United States, other countries, or both.

ActionMedia, LANDesk, MMX™, Pentium®, and ProShare are trademarks or registered trademarks of Intel® Corporation in the United States, other countries, or both.

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

SET™ and the SET Logo are trademarks owned by SET Secure Electronic Transaction™ LLC.

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

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

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

Terms and conditions for downloading and printing publications

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

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

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

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

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

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations. IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE

All material copyrighted by IBM Corporation.

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

IBM ®

Printed in USA