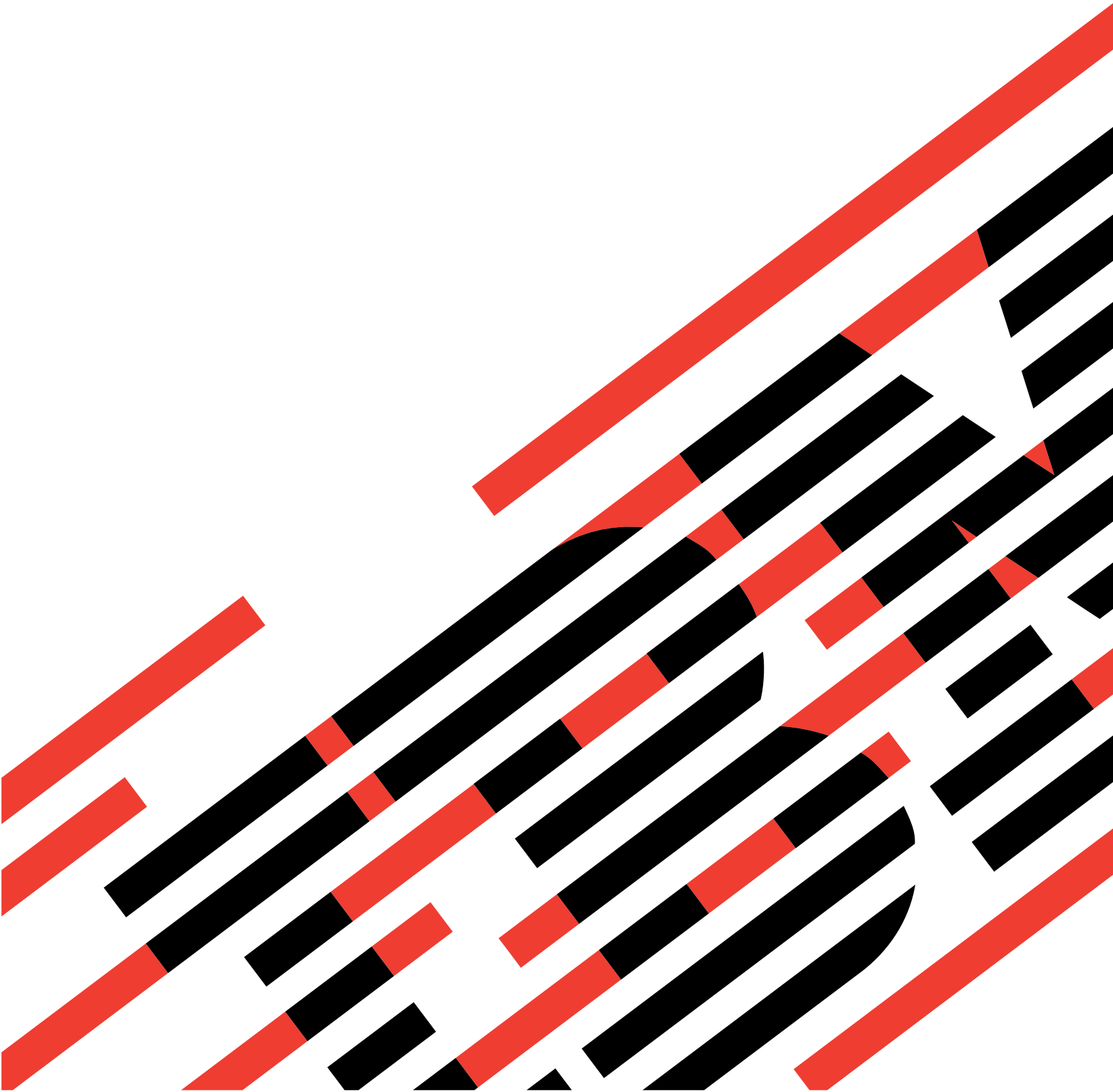
IBM

eserver

iSeries

基本系统安全性和计划



IBM

@server

iSeries

基本系统安全性和计划

目录

第 1 部分 基本系统安全性和计划 . . . 1

第 1 章 新增内容 3

第 2 章 打印本主题 5

第 3 章 基本系统安全性入门 7
关于基本系统安全性的常见问题 8
基本系统安全性概述 9
内置系统安全性 9
基本术语 10
安全性的用户视图 10
定制系统的用户视图 12
用于安全性和定制的系统工具 12
计划基本系统安全性的方法 15
示例: 介绍 JKL Toy 公司 15
安全性计划过程中的步骤 15

第 4 章 计划用户安全性. 17
计划物理安全性 17
系统部件的物理安全性 18
示例: JKL Toy 公司的物理安全性计划表单 — 系统部件部分 19
系统文档和存储媒体的物理安全性 19
示例: JKL Toy 公司的物理安全性计划表单 — 备份媒体和文档部分 20
计划工作站的物理安全性 20
打印机和打印机输出的物理安全性 21
示例: JKL Toy 公司的物理安全性计划表单 — 工作站和打印机部分 22
计划您的安全性策略 22
计划您的应用程序安全性 22
描述您的应用程序 23
示例: JKL Toy 公司的应用程序描述表单 . . 24
描述命名约定 25
示例: JKL Toy 公司的命名约定表单 25
描述库信息 26
示例: JKL Toy 公司的库描述表单 26
绘制应用程序图表 27
计划您的整体安全性策略 27
编写您的安全性策略 28
选择您的安全级别 29
选择影响注册的系统值 30
限制注册尝试次数（QMAXSIGN 和 QMAXSGNACN） 30
示例: 限制注册尝试次数 31
每次将用户限制于一个工作站 32
计划不活动作业的系统值 32
示例: 用 QINACTITV、QINACTMSGQ 和 QDSCJOBITV 系统值处理不活动的作业 . . 33
限制安全主管可以注册的位置 34
选择影响密码的系统值 34
确定密码持续时间 35
确定密码长度 35
限制重复密码 36
使用系统值来定制您的系统 36
示例: JKL Toy 公司的安全性策略 39
计划用户组 39
标识用户组 40
示例: 标识用户组 41
计划组概要文件 42
示例: JKL Toy 公司的用户组描述表单 . . . 44
选择影响注册的值 45
选择限制用户可以执行什么操作的值 46
选择设置用户环境的值 47
示例: JKL Toy 公司的用户组描述表单 — 第二部分 48
计划单个用户概要文件 49
确定谁应该负责系统功能 50
示例: JKL Toy 公司的系统责任表单 51
为每个用户选择值 52
示例: JKL Toy 公司的单个用户概要文件表单 53

第 5 章 计划资源安全性. 55
确定您的资源安全性的目标 56
示例: JKL Toy 公司的安全性目标 56
了解权限类型 57
计划应用程序库的安全性 59
决定对应用程序库的公共权限 59
示例: JKL Toy 公司的库描述表单 60
决定对程序库的公共权限 61
示例: JKL Toy 公司的库描述表单 — 非限制方法 61
示例: JKL Toy 公司的库描述表单 — 限制方法 62
确定库和对象的所有权 64
示例: JKL Toy 公司的应用程序所有权 65
决定用户库的所有权和访问权 65
将对象分组 66
示例: JKL Toy 公司的权限列表表单 67
计划打印机和打印机输出的安全性 69
示例: JKL Toy 公司的输出队列和工作站安全性表单 — 输出队列部分 69
计划工作站的安全性 70
示例: JKL Toy 公司的输出队列和工作站安全性表单 — 工作站部分 71
资源安全性建议摘要 71
计划您的应用程序安装 72
确定应用程序的用户概要文件和安装值 73
更改应用程序的安装值 73
示例: JKL Toy 公司应用程序安装表单 . . . 74

第 6 章 设置用户安全性 77
设置整体环境 78
注册到系统 78
选择正确的辅助级别 78
防止其它用户注册 79
输入安全性的系统值 81
应用新的系统值 81
创建安全主管概要文件 83
设置安全性的系统值 83
更改安全性系统值 84
更改单个系统值 85
执行用于装入应用程序的安全性步骤 86
创建所有者概要文件 86
装入应用程序 87
设置用户组 87
为组创建库 88
创建作业描述 89
创建组概要文件 91
设置单个用户 92
创建个人库 92
复制组概要文件 94
将密码设置为到期 95
创建附加用户 95
更改关于用户的信息 95
显示用户概要文件 96

第 7 章 设置资源安全性 99
设置所有权和公共权限 99
创建所有者概要文件 100
更改库所有权 100
设置应用程序对象的所有权 101
使用“按所有者使用对象”（WRKOBJOWN）命令 102
使用更改对象所有者命令 102
设置对库的公共访问权 103
设置库中所有对象的公共权限 103
使用作业记录来检查您的工作 104
设置新对象的公共权限 104
使用组和个人库 105
创建权限列表 106
用权限列表保护对象 106
将用户添加到权限列表 107
设置特定权限 107
设置库的特定权限 107
设置对象的特定权限 109
同时设置多个对象的权限 109
保护打印机输出 110
创建输出队列 111
将打印机输出指定到输出队列 111
保护工作站 112
限制对系统操作员消息队列的访问 113

第 8 章 测试安全性 115
测试用户概要文件 115
测试资源安全性 116

第 9 章 更改安全性信息 117
安全性命令 117
查看与列示安全性信息 118
更改安全性信息 119
删除安全性信息 119
将新用户添加到系统 119
创建新用户组 119
更改用户组 120
添加新应用程序 122
添加新工作站 122
更改用户的责任 122
从系统除去用户 123

第 10 章 保存安全性信息 125
保存系统值 125
保存组和用户概要文件 125
保存作业描述 126
保存资源安全性信息 126
使用缺省所有者概要文件（QDFTOWN） 127
从已损坏的权限列表恢复 127

第 11 章 监控安全性 129
用于监控安全性的核对表 129
安全性审计 130

第 12 章 基本系统安全性计划表单 . . . 131
“物理安全性计划”表单 131
“应用程序描述”表单 132
“命名约定”表单 132
“库描述”表单 133
系统值选择表单 134
“系统责任”表单 135
“用户组标识”表单 135
“用户组描述”表单 136
“单个用户概要文件”表单 137
“权限列表”表单 138
“打印机输出队列和工作站安全性”表单 139
“应用程序安装”表单 140

第 1 部分 基本系统安全性和计划

基本系统安全性和计划提供有关计划和设置 iSeries 安全性的详细信息。本主题着重介绍了计划，并提供了可以用来计划并记录安全性决定的表单。它也提供基本系统安全性的逐步设置指示信息。因为本主题的工作簿性质，您可能需要打印来更彻底地查看材料。

设置 iSeries 的最佳安全性包括两组主要活动: 计划任务和配置任务。要确保设置符合商业需要的安全性，您应该查看下列计划主题:

- 基本系统安全性入门概述了一般安全性概念，并回答有关基本系统安全性的问题。
- 计划用户安全性提供有关如何计划影响系统上用户的安全性的信息。这包括物理安全性、应用程序安全性、安全性的整体策略和系统上的用户概要文件。
- 计划资源安全性提供有关如何计划系统上对象的安全性的信息，包括库和库中的对象、打印机、打印机输出和工作站。

完成计划活动之后，可以查看下列主题来帮助您设置系统的安全性:

- 设置用户安全性提供有关设置用户和组安全性的详细信息。
- 设置资源安全性提供有关如何设置对象的所有权、对象的公共和特定权限和打印机和工作站的安全性的信息。
- 测试安全性提供有关测试安全性的信息。
- 更改安全性信息提供有关更新和修改用户和组概要文件和资源安全性的信息。
- 保存安全性信息提供有关备份安全性信息的信息。
- 监控安全性提供核对表，以跟踪安全性和有关审计安全性的信息。

除这些主题以外，使用计划表单来为您的计划策略和安全性决定提供资料。

第 1 章 新增内容

对于 V4R5，基本系统安全性和计划是“信息中心”的新增内容。最初，此信息是在 *Security-Basic*（SC41-5301-00）一书中。已更新它来反映有关设置 V4R5 系统的安全性的当前信息。

第 2 章 打印本主题

可以查看或下载本文档的 PDF 版本以进行查看或打印。必须已安装 Adobe® Acrobat® Reader 才能查看 PDF 文件。可以从 Adobe 主页  下载副本。

要查看或下载 PDF 版本，选择基本系统安全性和计划（950 KB 或 164 页）。

要在您的工作站上保存 PDF 以进行查看或打印:

1. 在您的浏览器中打开该 PDF（单击以上链接）。
2. 在您的浏览器菜单中，单击**文件**。
3. 单击**另存为...**
4. 导航至您想要将该 PDF 保存在其中的目录。
5. 单击**保存**。

第 3 章 基本系统安全性入门

从系统管理员到用户，每个人都应该关心安全性。系统安全性保护 iSeries 和您的秘密商业信息免受有意的和无意的安全性破坏。

基于您的安全性环境和需要，您可以定制您的系统安全性。

将安全性看作是您的系统的入口。使用安全性功能部件来**锁定**或保护您的信息不被未授权使用。

还使用安全性功能部件来**解锁**系统的灵活性并为每个用户定制灵活性。

良好的安全性计划可以保护您的系统，但它不能保证您的设备或您的信息的安全。应该将系统责任划分到多个雇员身上，以确保无人对您的系统具有独占控制权。

基本系统安全性和计划为您提供了计划和设置您的基本系统安全性的逐步方法。本主题强调计划系统安全性的重要性并提供用来记录您的安全性决定的计划表单。为了帮助您作出关于安全性的决定，在本主题中，您将会找到正计划其安全性的商业示例。

要确保您成功实现系统安全性，良好的和周到的计划是必不可少的。查看以下主题以了解有关基本安全性需要和安全性计划的重要性:

- 关于基本系统安全性的常见问题
- 基本系统安全性概述
- 计划基本系统安全性的方法

还应该有一个备份与恢复您系统上的所有信息的良好计划。另外，还应该计划万一发生灾难时如何更换您的设备。有关设计良好的备份计划的更多信息，参见“信息中心”中的备份与恢复主题。

关于用户安全性的详细计划信息

以下主题提供用于计划用户安全性的技术:

- 计划您的应用程序的安全性
- 计划您的安全性策略
- 计划用户组
- 计划单个用户概要文件

关于资源安全性的详细计划信息

以下主题为用户提供计划资源安全性的系统方法。

- 了解权限类型
- 计划应用程序库的安全性
- 确定库和对象的所有权
- 将对象分组
- 保护打印机输出
- 保护工作站

- 计划您的应用程序安装

可打印的计划表单

基本系统安全性和计划提供可打印的计划表单，这些表单允许您记录您的所有安全性决定。通过使用您的浏览器的打印按钮，可以用 PDF 格式打印整个主题或单个的计划表单。

基本系统安全性的逐步设置指示信息

在您完成安全性计划之后，本主题提供使您的安全性计划生效的步骤。以下主题将有助于您设置系统安全性。
- 设置用户安全性
- 设置资源安全性

关于基本系统安全性的常见问题

查看关于安全性的这些常见问题解答可帮助您更好地了解您系统的安全性的重要性。

安全性为什么重要?

在您的系统上存储的信息是您最重要的商业资产之一。当您考虑如何保护您的信息资产时，记住三个重要的目标:

- **机密性**: 良好的安全性措施可以防止人们查看和泄露机密信息。
- **完整性**: 在某种程度上，设计良好的安全性系统可确保系统计算机上信息的正确性。使用正确的安全性，您可以防止数据的未授权更改或删除。
- **可用性**: 如果有人意外或故意损坏您系统上的数据，则在恢复那些资源之前不能访问它们。良好的安全性系统可以防止这种损坏。

当人们考虑系统安全性时，他们通常考虑保护其系统以防止公司外的人（如商业对手）访问。实际上，针对正常用户的好奇心或他们造成的系统意外事件的保护常常是设计良好的安全性系统的最大优点。在没有良好安全性功能的系统中，用户可能会无意地删除重要文件。设计良好的安全性系统有助于防止此类型的意外事件。

当决定在您的系统上需要多大的安全性时，问您自己以下问题:

- 您的计算机（和存储在其中的数据）对您的企业有多重要？
- 您有需要特定安全级别的公司策略吗？
- 您的审计员需要存储在您的计算机上的信息的安全级别吗？
- 在可预知的将来，您将需要某种程度的安全性吗？

为什么定制您的系统?

iSeries 涵盖大范围的用户。小型系统可能有三到五个用户运行几个应用程序。大型系统可能在一个大型通信网络上有数千用户正在运行许多应用程序。

iSeries 设计提供许多灵活性以满足大范围的用户和情况。您有机会更改关于用户看到的系统外观和系统如何执行的许多情况。

第一次使用系统时，可能不需要或不想执行许多定制。IBM 交付您的系统时为许多选项设置了初始设置，称为**缺省值**。这些缺省值通常是最适合新安装的选项。

注: 所有新系统在交付时都设置了缺省安全级别 **40**。此安全级别确保只有已定义的用户才能使用系统。它还可以防止来自可以绕过安全性的程序的潜在完整性或安全性风险。

然而，如果进行某些定制，可以使您的系统成为您的用户的一个更简单和更有效的工具。例如，可以确保注册时用户始终获取正确的菜单。可以确保每个用户的报表转至正确的打印机。如果您进行某些初始定制来使系统看起来好象用户自己的系统，则您的用户将会对系统感到更自信。

谁应该负责?

不同的公司对于安全性采取不同的方法。有时，程序员负责安全性的所有方面。在其它情况下，管理系统的人也负责安全性。如果您对于在您的公司如何分配责任没有把握，以下是建议的方法:

- 计划资源安全性的方法取决于您的公司是购买还是开发应用程序。如果您开发您自己的应用程序，则在开发过程期间，通知您的资源安全性要求。如果您购买应用程序，则了解并使用应用程序设计器。在两种情况下，设计应用程序的人都应该将安全性作为设计的一部分考虑。
- 设置安全性应该是安全主管的责任。安全主管定义系统用户及其对系统的访问权。安全主管经常负责您的系统上的其它事情，如信息的备份和恢复。
- 安全主管还应该定制您的系统，因为许多安全性元素在系统定制中起重要的作用。

无论您使用什么方法来分配安全性的责任，都应**通知安全性策略**。您公司中的主管人员应该告诉每个人（最好用书面方式）计算机中的信息是重要资产。应该保护该信息，正如将保护公司的任何其它资产一样。有关安全性策略的示例，参见 “示例: JKL Toy 公司的安全性策略”。

既然您了解对于您的系统上的安全性，您可能想要查看关于系统安全性注意事项的概述。

基本系统安全性概述

要有效地计划，需要了解您要完成的视图如何与系统提供的工具联系。需要了解用户和系统功能部件如何一起工作来帮助您达到目标。

以下主题介绍安全性和定制的重要部分并显示它们如何一起配合。这些主题将在您开始计划之前给您一个概述。正如在计划过程中需要的那样，此处所介绍的所有概念解释得更详细。

- 内置系统安全性
- 基本术语
- 安全性的用户视图
- 安全性和定制的系统工具

内置系统安全性

系统方面安全性的所有部分都构建在系统中。它们不是您购买的单独产品。此集成方法具有几个益处:

- 安全性与操作系统的其余部分一致。它使用相同的屏幕、命令和术语。
- 用户不能绕过安全性，因为它不是软件的一个独立部分。

- 正确设计的安全性对性能具有最小影响。
- 安全性始终不落后于新的软件开发。当新功能可用时，这些功能的安全性也可用。

iSeries 交付时设置为安全级别 40，该级别防止未授权用户注册到系统中。它还可以防止来自可以绕过安全性的程序的潜在完整性或安全性风险。然而，您可以定制某些安全性设置或更改安全级别。在主题“选择安全级别”中描述了安全级别。

既然对内置安全性如何操作有了更好的了解，您可能想熟悉一下公共 iSeries 术语。

基本术语

这组一般术语对于了解 iSeries 安全性很重要。

对象 对象是系统上可以操作的已命名的空间。对象的最常见的示例是文件和程序。其它类型的对象包括命令、队列、库和文件夹。系统上的对象由对象名称、对象类型和对象驻留在其中的库标识。系统上的每个对象都可受保护。

库 库是用于将其它对象分组的一种特殊类型的对象。系统上的许多对象驻留在库中。

目录 目录是将系统上的对象分组的另一种方法。对象可以驻留在目录中。一个目录可以驻留在另一目录中，从而形成一种分层结构。

既然您已对一般 iSeries 安全性术语有了更好的了解，您可能要查看用户查看安全性的方式。

安全性的用户视图

从用户的观点来看，安全性会影响他们如何在系统上使用和完成任务。安全性还包括他们如何与系统进行交互来完成那些任务。考虑用户将如何查看安全性很重要。例如，将密码设置为每 5 天到期将会破坏和干扰用户完成其作业的能力。在另一方面，密码策略过于宽松会导致安全性问题。

要为系统提供正确的安全性，需要将安全性分成可以计划、管理和监控的特定部分。从用户的观点来看，可以将系统安全性分成以下几个部分:

对系统的物理访问

物理安全性保护系统部件、所有系统设备和备份存储媒体（如软盘、磁带或 CD）免受意外或有意的丢失或损坏。

您为确保系统的物理安全性所采取的大多数措施对系统来说是外部的。然而，系统交付了一个密钥锁或电子密钥杆来防止未授权使用系统部件上的功能。

主题“计划物理安全性”提供了详细信息来帮助您计划系统的物理安全性。

用户如何注册

注册安全性防止系统上未标识的人注册。为了注册，个人必须输入用户标识和密码的有效组合。

可以使用系统值和单个用户概要文件来确保不会违反注册安全性。例如，可以要求定期更改密码。还可以防止使用易于猜中的密码。

允许用户执行什么操作

安全性以及系统定制的重要作用是定义用户可以执行的操作。从安全性观点来看，这常常是一种**限制**功能，如防止人们查看某些信息。从系统定制方面来看，这是一种**授权**功能。正确定制的系统使得人们能够通过排除不必要的任务和信息将其作业做好。

用于定义用户可以执行的操作的一些方法适合于安全主管，而其它方法则是程序员的责任。此信息主要强调安全主管通常执行的那些操作。可以在 *Security-Reference*（SC41-5302）的第三章 “Security System Values” 中找到所有系统值的描述。

参数在单个用户概要文件、作业描述和类中可用，以控制用户在系统上可以执行的操作。以下列表简要描述可用的技术:

将用户限制于几个功能

可以根据用户概要文件将用户限制于特定程序、菜单或菜单组和几个系统命令。通常，安全主管创建和控制用户概要文件。

限制系统功能

系统功能允许您保存和恢复信息、管理打印机输出以及设置新的系统用户。每个用户概要文件指定用户可以执行哪些最常见的系统功能。

在 iSeries 中，通过使用控制语言（CL）命令和应用程序编程接口（API）执行系统功能。因为每个命令和 API 是一个对象，所以您可以使用对象权限来控制谁可以使用它们和完成系统功能。

确定哪些用户可以使用文件和程序

资源安全性提供控制使用系统上每个对象的能力。对于任何一个对象，可以指定哪些用户可以使用它以及他们可以如何使用它。例如，可以指定一个用户只能查看文件中的信息；另一个用户可以更改文件中的数据；第三个用户可以更改文件或删除整个文件。

防止滥用系统资源

对您的业务而言，对系统的处理能力可以变得对与在系统上存储的数据一样重要。安全主管帮助确保用户不会通过以高优先级运行其作业、首先打印其报表或使用过多的磁盘存储器来滥用系统资源。

您的系统如何与其它计算机通信

如果您的系统与其它计算机或与可编程工作站通信，则附加安全性措施可能是必要的。如果没有正确的安全性控制，则网络中另一个计算机上的某个人可以在您的计算机上启动作业或访问信息，而不需完成注册过程。

可以同时使用系统值和网络属性来控制您的系统是上是否允许远程作业、远程数据访问或远程 PC 访问。如果允许远程访问，则可以指定要强制哪种安全性。可以在 *Security-Reference*（SC41-5302）的第三章 “Security System Values” 中找到所有系统值的描述。

如何保存安全性信息

需要定期备份系统上的信息。除保存系统上的数据之外，还需要保存安全性信息。如果发生灾难，则需要能够恢复有关系统用户、权限信息和信息本身的信息。

主题“保存安全性信息”解释如何保存安全性信息。“信息中心”中的备份与恢复主题提供有关备份和恢复安全性数据的更详细信息。

如何监控安全性计划

系统提供几种用于监控安全性效果的工具:

- 当发生某些安全性违规时，将消息发送至系统操作员。
- 各种与安全性有关的事务都可记录在特殊的审计日志中。

主题“监控安全性”概括地讨论了这些工具的使用。可以在 *Security-Reference*（SC41-5302）的第九章“Auditing Security on the System”找到关于安全性审计的更多详细信息。

要更好地了解如何定制系统，应该从用户视图中了解定制。

定制系统的用户视图

可以定制系统来帮助用户完成日常工作。要为用户最好地定制您的系统，考虑他们成功完成工作所需要的功能。可以定制系统按几种方式来显示菜单和应用程序:

显示用户想看到的内容

大多数人安排书桌和办公室以便使他们很容易找到最需要的东西。以同样的方式考虑用户对系统的访问。在用户注册到系统中之后，用户应该首先看到最常用的菜单或屏幕。可以容易地设计用户概要文件来实现此功能。

消除不必要的内容

大多数系统都在系统上有许多不同的应用程序。大多数用户只想查看他们完成其作业所需要的内容。将他们限制于系统上的几个功能使其作业更容易完成。使用用户概要文件、作业描述和适当的菜单，可以给每个用户一个特定的系统视图。

将某些内容发送至正确位置

用户应不必担心如何将其报表发送到正确的打印机或其批处理作业应该如何运行。系统值、用户概要文件和作业描述执行这些任务。

提供辅助

无论在定制系统时如何成功，用户仍可能想知道“我的报表在哪里？”或“我的作业已运行了吗？”**操作辅助**屏幕提供与系统功能的简单接口，它帮助用户回答这些问题。不同版本的系统屏幕（称为**辅助级别**）为具有不同级别技术经验的用户提供帮助。当系统到达时，“操作辅助”屏幕自动对所有用户可用。然而，应用程序的设计可能要求您更改用户访问“操作辅助”菜单的方式。

iSeries 提供了一些系统工具，这些工具允许您定制系统安全性来保护您的资源，同时还允许用户访问这些资源。

用于安全性和定制的系统工具

要有效地计划，需要了解您的安全性目标视图如何与系统提供的工具联系。可以使用这些系统工具来定制系统上的安全性。

安全级别

IBM 用安全级别 40 交付所有新的 iSeries。安全级别 40 提供密码和资源安全性以及系统完整性。如果要更改系统上的活动安全级别，可以更改 QSECURITY 系统值。然而，IBM 强烈建议将安全级别设置保留为 40。为了要更改安全级别，用户需要 *SECOFR 用户类或 *ALLOBJ 和 * SECADM 特权。

系统提供 4 种级别的安全性，如下表中所示:

表 1. 系统上可用的安全级别

安全级别	描述
安全级别 20	仅提供密码安全性。
安全级别 30	提供密码和资源安全性。
安全级别 40	提供密码和资源安全性；完整性安全性。
安全级别 50	提供密码和资源安全性；增强的完整性保护。

主题“选择安全级别”提供有关如何确定哪个安全级别最能满足您的需要的详细信息。

系统值

可以设置系统值来控制操作系统的某些功能如何在您的 iSeries 上工作。将系统值看作是公司策略。除非某些更特定的情况（如用户概要文件）覆盖系统值，否则系统值适用于使用系统的每个人。

系统值确定诸如主打印机、系统如何显示日期以及需要多长时间更改密码。

网络属性

网络属性定义您的系统如何与其它计算机（包括个人计算机）通信的某些特征。网络属性适用于您的整个系统。

组概要文件

组概要文件定义一组用户。将组概要文件看作是部门策略。可以将组概要文件用作创建单个用户概要文件的模式。还可以使用组概要文件来定义允许组的成员如何访问系统上的对象。有关组概要文件的更多信息，参见主题“计划用户组”。

用户概要文件

用户概要文件是系统上功能最强大的通用对象。它包含诸如用户密码以及用户注册后看到哪个菜单。用户概要文件定义用户在系统上可以执行和不能执行的操作。它确定用户的唯一系统视图。主题“计划用户安全性”讨论用于计划用户概要文件的技巧。

作业描述

作业描述使用系统值和用户概要文件来确定系统处理用户作业的方式。作业描述设置用户的初始库列表，该库列表确定用户在注册之后自动获取其访问权的库。

资源安全性

安全主管通过确定谁具有使用系统上的资源（对象）的权限以及用户可以如何访问这些对象来保护资源（对象）。安全主管可以为单个对象或对象组设置对象权限（权限列表）。文件、程序和库是最常见的需要保护的对象，但系统安全性允许您为系统上的任何对象设置对象权限。

如果预先计划一种一般且简单的方法，则可以简单有效地管理资源安全性。未预先计划的资源安全性方案会变得复杂且无效。主题“计划资源安全性”描述计划资源安全性的方法。

系统提供几种工具来在设计简单的资源安全性方案时帮助您:

- **组概要文件**: 可以在单一组概要文件之下将类似的用户分组。然后，用户组可以完全共享对象的相同权限。
- **权限列表**: 可以在一个列表中将具有类似安全性需求的对象分组。然后，可以对列表而不是对单个对象授予权限。
- **对象所有权**: 系统上的每个对象具有一个所有者。组概要文件或单个用户可以拥有对象。正确指定对象所有权有助于您（1）管理应用程序，（2）对信息的安全性授权责任。
- **主组**: 可以为对象指定主组权限。系统将主组权限与对象一起存储。使用主组权限可以简化权限管理并提高权限检查性能。
- **库权限**: 可以将需要保护的文件和程序放在一个库中并限制对该库的访问。这通常比限制对每个单独对象的访问更简单。要保护关键对象，您可能要同时保护对象和库。
- **对象权限**: 在对库的访问不受限制而对库的访问不够明确的情况下，可以限制对单个对象（如文件）权限。
- **公共权限**: 对于每个对象，可以定义哪种访问可用于对对象不具有任何其它权限的任何系统用户。公共权限是用于保护不保密的对象的有效方法并提供良好的系统性能。
- **目录权限**: 可以用与使用库权限相同的方式使用目录权限。可以将目录中的对象分组并保护目录而不是保护单个对象。
- **权限持有者**: 当删除对象时，也删除对象的权限信息。权限持有者维护程序定义的文件（删除并由应用程序再次创建该文件）的权限信息。可以使用权限持有者来帮助从 System/36 迁移。

安全性工具

可以使用安全性工具来帮助您管理和监控 iSeries 上的安全性环境。还可以使用用户概要文件工具来帮助您:

- 找出哪些用户概要文件具有缺省密码。
- 调度在一天或一周的某些时间用户概要文件不可用。
- 调度在雇员离开时除去用户概要文件。
- 找出哪些用户概要文件具有特权。
- 找出谁沿用对系统上对象的权限。

可以使用对象安全性工具来跟踪与秘密对象关联的公共和专用权限。可以定期（例如，每月）打印这些报表来帮助您将对安全性的精力集中在当前问题上。可以运行报表来仅显示自上次运行报表以来的更改。

其它工具提供监控以下项的能力:

- 触发程序
- 通信输入、子系统描述、输出队列、作业队列和作业描述中与安全性有关的值。
- 改变或篡改的程序

既然了解了系统安全性的重要性，您可能要查看本主题用作示例的计划方法的描述。

计划基本系统安全性的方法

应该通过从外到里并从一般到特定来计划安全性。例如，要计划用户概要文件，需要首先考虑用户应该看到的内容（外部）。然后，您需要确定如何使该内容出现（内部）。

首先计划系统值和组概要文件（一般），然后决定对于单个用户的例外情况（特定）。

依次完成“计划用户安全性”中的计划任务。这些任务提供描述如何计划使用系统和决定如何保护和定制系统的合理进度。在这些主题中，使用计划工作表来记录您的安全性决定和实现。确保将这些计划表存储在安全位置。在每个主题中的计划工作表上收集的信息将帮助您以后设置安全性。

计划和设计系统安全性时，从基础向上构建。需要从最基本的安全性表单开始，然后构建至更复杂的安全性问题。从您的系统的物理安全性开始，到描述您的应用程序和系统值。最后，需要考虑您系统上的用户和对象的安全性。

贯穿这些计划主题，可以找到一个典型公司（JKL Toy 公司）使用此方法的示例。尽管此公司是虚构的，但此公司是现实世界的许多公司中具有代表性的公司。主题“示例: 介绍 JKL Toy 公司”描述了此样本公司。

示例: 介绍 JKL Toy 公司

示例使事情更易于解释和更易于理解。记住，本主题使用 JKL Toy 公司作为示例。JKL Toy 公司（一个小型但发展快速的玩具制造商）要在 iSeries 系统上设置安全性。公司总裁 John Smith 想要他的新的 iSeries 系统减轻 JKL Toy 公司爆炸性增长的负担。

John 给予 Sharon Jones（会计经理）系统管理员和安全主管的责任。她需要确保整个安装（包括安全性）平稳运行。Sharon 相信计划的重要性。目前，该公司不大，且其大多数雇员对大部分信息有访问权。但 Sharon 知道，这将会随着公司的发展而更改。她第一次担心不能正确处理事情。

最初，JKL Toy 公司计划在其系统上运行以下应用程序: “客户订单”、“库存控制”、“合同及定价”以及“应收帐款”。当您阅读计划主题时，您将会了解更多关于 JKL Toy 公司如何处理安全性的信息。

主题“计划过程中的步骤”解释当您计划您的系统安全性时需要遵循的每个步骤。

安全性计划过程中的步骤

以下图表描述计划过程中的每个步骤以及该步骤与过程的其余部分的关系。

表 2. 安全性计划过程中的步骤

步骤	在此步骤中执行什么操作	此步骤互相之间的关系
计划物理安全性	描述如何计划来保护系统部件、设备和备份媒体。	此信息大部分独立于过程的其余部分。不将物理安全性计划信息输入到系统中；然而，您需要此信息的某些部分来计划系统值和资源安全性。
计划您的应用程序	描述用途、主菜单和您的所有应用程序的库。	为计划过程的其余部分和您的其它安全性决定提供基础。不将此信息输入到系统中。
计划您的整体方法	确定哪种整体方法将用于安全性。选择支持该方法的系统值。	使用您的应用程序计划信息来帮助确定您的整体方法。您选择的系统值影响您如何计划用户和组概要文件。
计划用户组	决定如何将您的用户分成组。决定每个组具有什么特征以及如何在系统上定义这些特征。	使用应用程序描述来确定系统上的组。您定义的用户组影响您在系统上计划单个用户的方式。
计划单个用户概要文件	将每个系统用户分配到一个组。定义每个用户，包括不同于组的其余用户的特征。例如，用户需要与组中其余用户不同的应用程序或库的访问权。	使用应用程序计划和用户组计划信息来帮助定义单个用户。
计划资源安全性	确定哪些应用程序对系统上的每个人都应该可用。如果您需要限制某些应用程序，则决定应该允许哪些用户或组使用它们。	使用应用程序计划和组概要文件计划信息来帮助计划资源安全性。
计划您的应用程序安装	决定如何建立对于您的应用程序库的所有权和公共权限。	使用资源安全性计划信息来计划您的应用程序安装。

您应该通过计划用户安全性来开始安全性计划过程。

第 4 章 计划用户安全性

计划用户安全性包括计划安全性影响系统中用户的所有方面。您必须描述以下方面:

物理安全性

物理安全性包括保护您 iSeries 免受意外（或有意）损坏和盗窃。另外，它还包括所有的工作站、打印机和存储媒体。“计划物理安全性”包含关于计划物理安全性、风险和 IBM 建议的更多信息。

应用程序安全性

应用程序安全性涉及您在系统上所存储的应用程序以及将如何保护那些应用程序而同时还允许用户访问它们。“计划应用程序的安全性”提供关于描述您的应用程序及其命名约定的详细信息。

整体安全性策略

计划整体安全性包括制订一个安全性计划，该计划同时考虑企业目前的情况和将来的计划。“计划整体安全性策略”提供关于确定您的安全性策略、安全级别、密码注意事项和系统值的更多信息。

用户组安全性

一个用户组是一组用户，他们需要以相同的方式使用相同的应用程序。计划用户组安全性包括确定计划使用那些组的系统和应用程序需要的工作组。“计划用户组”提供关于标识用户组、计划组概要文件、选择系统值和确定用户环境的详细信息。

单个用户安全性

确定了需要哪些用户组之后，可以计划所需要的单个用户概要文件。“计划单个用户概要文件”提供关于命名系统上的用户、确定单个用户的责任和选择系统值的更多信息。

将会在这些计划主题中找到链接至可以用来记录您的计划决定的计划表单。

计划物理安全性

当您准备安装您的 iSeries 时，您应该通过询问以下问题来创建物理安全性计划:

- 您要将系统部件放在何处？
- 您要将每个显示站放在何处？
- 您要将打印机放在何处？
- 您需要哪些附加设备，如配线、电话线、家具或存储区域？
- 您将采取什么措施来保护您的系统以避免发生紧急事件，如火灾或电源中断？

物理安全性应该是您的整体安全性计划的一部分。取决于您将系统及其设备放在何处，您可能需要特殊措施来保护它们。

您可以使用物理安全性计划表单来记录您关于系统的物理安全性的决定。要确保涵盖物理安全性的所有方面，查看以下主题:

- 系统部件的物理安全性提供关于保护系统自身的详细信息。
- 系统文档和存储媒体的物理安全性包含关于保护系统文档和您的存储媒体的信息。

- 工作站的物理安全性讨论保护工作站的方法。
- 打印机和打印机输出的物理安全性提供关于物理上保护打印机及其输出的详细信息。
- 计划您的安全性策略解释如何准备用户指导和安全性策略。

每个系统部件都有一个控制面板，以用于维修机器和执行特殊系统操作，如打开和关闭系统。要防止未授权使用这些系统操作，每个系统部件有一个密钥锁开关或电子密钥杆。它们提供对于系统部件的某些保护，但密钥锁开关或电子密钥杆并不是足够物理安全性的替代品。

系统部件的物理安全性

iSeries 不要求具有特殊环境控制的机房。通常您会在办公室区域中间发现系统部件，许多人可以接近它。客户喜欢 iSeries 的外形小巧和易于维护；然而，这些功能也可能造成安全性风险。例如，一个人可以很容易地偷窃系统部件或从中卸下贵重组件。

您应该采取措施来确保您的系统部件位于安全地方。最好的位置是位于专用的已锁上的房间。至少，系统部件应该位于在正常营业时间之外可以锁上的地方。

系统部件的风险

除偷窃系统部件或其组件外，此处也是由您的系统部件的不充分的物理安全性造成的一些其它风险:

无意识地中断系统操作

许多安全性问题都来自授权系统用户。假定您的系统上的显示站之一已锁定。系统操作员离开去开会了。发生故障的显示站用户向系统部件走去，并想“或许，如果我按此按钮，它将会更正问题”。该按钮可能在许多作业正在运行时关闭或重新装入系统。您可能需要几个小时来恢复部分地更新的文件。您可以使用系统部件密钥锁开关来防止此情况。

使用专用服务工具（DST）功能来绕过安全性

安全性不控制系统执行的服务功能，因为当您需要执行这些功能时，您的系统软件可能不在正常操作。一个知道或猜中“服务工具”用户标识和密码的有经验的人可能会对您的系统造成相当大的损坏。要了解有关“服务工具”的更多内容，参见“信息中心”中的服务工具主题。

建议

- 理想情况下，将您的系统部件保存在已锁上的房间。如果不能做到这点，则将您的部件放在外人不能接近的地方。同时选择一个负责的雇员可以监视它的位置。以下物理安全性功能可帮助您保护您的系统免于意外的或故意的篡改:
- 使用电子密钥杆或密钥锁:
  - 如果您要能够不使用钥匙而启动您的系统，则将操作方式设置为“正常”。
  - 如果您计划使用“自动加电／断电”功能来启动和停止您的系统，则将操作方式设置为“自动”。
  - 取下钥匙并将其放在一个安全地方。
- 在您安装您的系统并在服务人员使用它之后，立即更改“服务工具”（DST）用户标识和密码。“信息中心”中的主题服务工具以更多详细信息的方式解释如何这样做。

在您计划系统文档和存储媒体的物理安全性之前，您可能想查看对于部件安全性的 JKL Toy 公司计划示例。

示例: JKL Toy 公司的物理安全性计划表单 — 系统部件部分

以下是 Sharon Jones 用于系统的“物理安全性计划”表单的系统部件部分的示例:

表 3. JKL Toy 公司的“物理安全性计划表单”: 系统部件示例

物理安全性计划表单	
准备人: Sharon Jones	日期: 99/2/9
系统部件:	
描述保护系统部件的安全性措施（如已锁上的房间）:	系统部件在会计区域。在白天，会计人员总是在该区域，并可以看守系统部件。会计人员也对零用现金和重要记录负责。在营业时间以外，该区域是锁上的。
通常使用什么密钥锁位置？	正常
钥匙保存在何处？	Sharon 办公室的小保险箱。
与系统部件相关的其它注释:	系统部件将是容易接近的。告诫会计区域中的人员，他们应该确保没有人损坏它。

在您计划系统部件的物理安全性之后，可以计划系统文档和存储媒体的物理安全性。

系统文档和存储媒体的物理安全性

您的物理安全性计划的另一个方面涉及重要的系统文档和存储媒体的存储。系统文档包括 IBM® 随系统一起发送的信息、密码信息、您的计划表单以及系统生成的任何报表。

取决于您的系统，备份媒体可以包括磁带、CD-ROM、软盘或 DVD 存储器。您应该在您的营业位置和另一个远程位置同时存储系统文档和备份媒体。万一发生灾难，您将需要此信息来恢复您的系统。以下信息建议几种方式来存储您的系统文档和存储媒体。在确定了您的方法之后，在物理安全性计划表单的“备份媒体和文档”部分中记录您的选择。

安全地存储系统文档

服务工具和安全主管密码对于您系统的操作很关键。您应该写下这些密码并将它们存储在一个安全秘密的位置。另外，将这些密码的副本保存在远离现场的位置，以帮助您从灾难中恢复。

考虑将其它重要系统文档（如配置设置和您的主要应用程序库）存储在远离您的企业位置，以帮助您从灾难中恢复。

安全地存储您的存储媒体

当您安装系统时，作出计划，以定期将系统上的所有信息保存到磁带或其它存储媒体。这些备份允许您在必要时恢复您的系统。您应该将这些备份保存在一个安全位置并远离现场。

风险

- 对备份媒体的损坏: 如果灾难或故意破坏者破坏了您的系统备份媒体，则除已打印的报表外，您无法恢复您系统上的信息。

- 备份媒体或密码的偷窃: 您可能已将秘密的商业信息保存在您的备份媒体上。有经验的人可能能够将此信息恢复到另一个计算机并打印或处理它。

建议

- 将所有密码和备份媒体存储在一个已锁上并防火的箱子里。
- 将您的备份媒体的副本定期（例如至少每星期）放到一个安全且远离现场的位置。

在您为您的工作站计划物理安全性之前，您可能想查看 JKL Toy 公司用于存储系统文档的计划示例。

示例: JKL Toy 公司的物理安全性计划表单 — 备份媒体和文档部分

JKL Toy 公司的 Sharon Jones 完成了“物理安全性计划”表单的“备份媒体和文档”部分，如下所示:

表 4. JKL Toy 公司的“物理安全性计划表单”: 备份媒体和文档示例

物理安全性计划表单	
准备人: Sharon Jones	日期: 99/2/9
备份媒体和文档:	
备份磁带存储在企业位置的何处？	在一个大型且防火的保险箱中。
备份磁带存储在远离企业位置的何处？	在公司会计办公室的防火保险箱中。
安全主管、服务和 DST 密码保存在何处？	John Smith 办公室中的组合保险箱中。
重要系统文档（如序列号和配置）保存在何处？	在一个远离现场的大型保险箱中和会计的办公室中。

在计划存储和文档安全性之后，可以计划工作站的物理安全性。

计划工作站的物理安全性

在大多数情况下，您想要所有用户都能够在任何可用的工作站上注册并执行所有已授权的功能。然而，如果您具有很公开或很秘密的工作站，您可能想采取特殊预防措施。例如，可以存储按键的显示站和个人计算机需要特殊的注意事项。使用它来帮助您完成物理安全性计划表单的“第二部分”（工作站和打印机的物理安全性）。

与工作站相关联的风险

在公共位置未授权而使用工作站

如果公司外的人可以很容易接近某些位置，则他们可能有机会查看机密信息。如果系统用户离开已注册的工作站，来自公司外的某个人可能会走过去并访问机密信息。

在秘密位置未授权而使用工作站

位于很秘密位置的工作站使计算机窃贼有机会花费较长的时间来尝试绕过您的安全性而不被看到。

在显示站上使用回放功能或 PC 注册程序来绕过安全性措施

许多显示站都有记录和回放功能，这使用户能够存储经常使用的按键并通过按单个键来重复它们。当您将个人计算机用作 iSeries 系统上的工作站时，您可以编写程序来使注册过程自动进行。因为用户经常使用注册过程，所以他们可能决定存储其用户标识和密码，而不是在每次注册时输入它们。

建议

当设置工作站的物理安全性时，考虑以下建议:

- 如果可能的话，避免将工作站放在很公开或很秘密的位置。
- 对系统用户强调离开工作站之前注销的重要性。您应该将注销过程包括在您的安全性策略中。
- 强调将密码记录在显示站或记录在 PC 程序中违反系统安全性。您应该将记录密码信息包括在您的安全性策略中。
- 通过使用不活动的计时器系统值（QINACTITV 和 QINACTMSGQ）来采取措施，以防止用户离开公共位置的工作站而不注销系统。
- 通过仅授权具有限制权限的用户使用公共工作站来限制用户在公共工作站可以执行哪些功能。
- 防止具有安全性或服务权限的用户在专用工作站注册。使用 QLMTSECOFR 系统值来控制用户使用这些权限在哪里注册。
- 限制用户同时在多个工作站上注册。可以使用限制设备会话（QLMTDEVSSN）的系统值来控制用户在哪里注册。

要使这些建议生效，参见主题“选择影响注册的系统值”和“计划工作站的资源安全性”，以获取详细信息。

对于“物理安全性计划”表单，您需要标识哪些工作站可能由于物理位置而造成风险。您可能要查看 Sharon Jones 如何计划 JKL Toy 公司的工作站物理安全性的示例。

在您计划工作站安全性之后，您可以计划打印机和打印机输出的物理安全性。

打印机和打印机输出的物理安全性

一旦开始打印信息，系统安全性就不能控制谁可以看到它。要最小化某些人看到秘密商业信息的威胁，应该保护打印机和打印机输出。您还应该创建处理打印秘密商业信息的策略。

与打印机和打印机输出关联的风险

以下风险可能适用于您企业的情况。这些是与打印机和打印机输出关联的最常见的安全性风险。然而，您应该调查可能适用于您的特定企业情况的其它风险。

- 位于公共位置的打印机可能会使未授权人员能看到机密信息。
- 放在桌子上的打印机输出可能会暴露信息。
- 您的系统可能只有一台或两台打印机。您可能需要打印重要或机密信息（如薪水支票），因此您公司的雇员会应该会看到该信息。

建议

以下建议可帮助您减小与打印机及其输出关联的安全性风险。

- 对系统用户强调保护机密打印机输出的重要性。在安全性策略中包括关于打印机的物理安全性决定。
- 避免将打印机放在公共位置。
- 调度高度机密输出的打印，并在打印时让一个授权人员留在打印机旁边。

“计划打印机和打印机输出的安全性”讨论用于处理机密打印机输出的建议。

在开始计划您的安全性策略之前，您可能要查看 JKL Toy 公司的打印机安全性计划示例。

示例: JKL Toy 公司的物理安全性计划表单 — 工作站和打印机部分

以下是 Sharon Jones 用于 JKL Toy 公司的 “物理安全性计划” 的 “第二部分” 的示例:

表 5. JKL Toy 公司的物理安全性计划表单: 工作站和打印机示例

“物理安全性计划” 表单			第二部分（共两部分）
工作站和打印机的物理安全性			
工作站或打印机的名称	它的位置或描述	安全性暴露	要采取的保护措施
DSP06	装运码头	太公开	自动注销。限制可以在工作站上完成的功能。
DSP09	客户服务办公桌	太公开	自动注销。限制可以在工作站上完成的功能。
RMT12	远程销售办公室	太秘密	不要让安全主管在此处注册。
PRT02	会计，在系统部件附近	机密信息（如价格列表）不能被看到	指定某人来监控打印机输出

完成物理安全性计划表单之后，继续转至主题 “计划您的安全性策略”。

计划您的安全性策略

您可能会发现向您的所有雇员发送安全性准则来强调关于物理和系统安全性的安全性策略很有用。您可以将相同的准则给予后来添加至您系统的新用户。

在这些准则中，您应该包括关于如何保护系统安全性的一些一般指示信息，如注销工作站和不共享密码。准则还应该包括关于您所作出的特定安全性决定的信息。

当您阅读完此计划信息时，记下您自己的安全性准则应该包括的内容。您可能还要记下您的安全性策略。

例如，当 JKL Toy 公司的 Sharon Jones 计划系统的物理安全性时，记下了她的安全性准则:

确保对装运码头、客户服务和远程营业部强调注销的重要性。会计人员将看护系统部件。

在您完成物理安全性计划表单之后，您就随时可以计划您的应用程序的安全性。

计划您的应用程序安全性

要计划应用程序的恰当安全性，您需要了解:

- 计划在系统上存储什么信息？
- 谁需要访问该信息？
- 人们需要哪种访问？他们需要更改信息还是只查看信息？

当您看完这些应用程序计划主题时，回答第一个有关您计划在系统上存储什么信息的问题。在后续主题中，决定谁需要该信息以及人们需要哪种访问。不将应用程序计划信息输入到系统中；然而，当您设置用户和资源安全性时您将需要该信息。

什么是应用程序?

在应用程序安全性的第一个计划步骤中，您需要描述计划在系统上运行的应用程序。应用程序是一组逻辑上属于一起的功能。例如，在 JKL Toy 公司，输入订单、交付订单和打印发票都是称为“订单处理”的应用程序的一部分。

通常，两种不同类型的应用程序在 iSeries 上可以运行:

- **商业应用程序**: 您购买或开发以执行特定商业功能（如订单处理或库存管理）的应用程序。
- **特殊应用程序**: 您提供的应用程序，在整个公司使用该应用程序来执行不是特定于某个商业过程的各种活动。

您需要什么表单?

使用以下表单来帮助计划应用程序安全性:

- 应用程序描述表单
- 库描述表单
- 命名约定表单

要打印这些表单，在您的浏览器中，单击链接，选择正确的框架，然后单击**打印**图标。

阅读以下信息来帮助您完成这些计划表单。

- 描述您的应用程序
- 描述命名约定
- 描述库信息
- 绘制应用程序图表

描述您的应用程序

此时，需要收集关于您的每个商业应用程序的一些一般信息。将关于您的应用程序的信息添加至“应用程序描述”表单上的适当字段中，如下所述。稍后您可以使用此信息来帮助您计划用户组和应用程序安全性:

应用程序名称和缩写

给予应用程序一个简短的名称和缩写，它们在表单中可以用作简写并用于命名应用程序使用的对象。

描述性信息

简要描述应用程序的功能。

主菜单和库

标识哪个菜单是用于访问应用程序的主菜单。指示该菜单所在的库。通常，主菜单导向具有特定应用程序功能的其它菜单。用户在注册到系统中之后，喜欢立即查看其主要应用程序的主菜单。

初始程序和库

有时，应用程序运行设置用户背景信息或执行安全性检查的初始程序。如果应用程序具有初始程序或设置程序，在表单中列示它。

应用程序库

每个应用程序通常具有一个用于其文件的主库。包括应用程序使用的所有库，

其中包括程序库和其它应用程序拥有的库。例如，JKL Toy 公司的客户订单应用程序使用库存库来获取商品余额和描述。

可以使用库和应用程序之间的关系来确定谁需要访问每个库。

查找关于应用程序的信息

如果您尚未了解关于应用程序您所需要的信息，则可能需要与您的程序员或应用程序供应商联系。

如果您对关于在您的系统上运行的应用程序的此信息没有访问权，则以下是自己收集该信息的方法。

- 应用程序的用户可能会告诉您主菜单和库的名称，或您可以观察他们注册到系统上。
- 如果用户在注册之后立即看到应用程序，则查看其用户概要文件中的**初始程序**字段。此字段包含应用程序的初始程序。您可以使用 DSPUSRPRF 命令来查看初始程序。
- 可以列示您的系统上所有库的名称和描述。使用 DSPOBJD *ALL *LIB。这会显示您的系统上的所有库。
- 您可以在用户正在运行应用程序时观察活动作业。用中间辅助级别使用“使用活动作业”（WRKACTJOB）命令来获取关于交互式作业的详细信息。显示作业并同时查看库列表及其对象锁定来找出正在使用的库。
- 可以使用“使用用户作业”（WRKUSRJOB）命令来应用程序中的批处理作业。

要确保收集计划您的应用程序安全性所需要的所有信息，应该完成下列任务之后才继续:

- 完成您的每个商业应用程序的“应用程序描述”表单。填写整个表单，安全性需求部分除外。将使用该部分来计划应用程序的资源安全性，如在主题“计划资源安全性”中所述。
- 准备每个特殊应用程序（如果适用的话）的“应用程序描述”表单。使用该表单帮助您确定如何提供对应用程序的访问。

注: 可选择从 IBM（如 IBM Query iSeries 版）准备每个特殊应用程序的“应用程序描述”表单。对于这些应用程序所使用的库的访问不需要任何特殊计划。然而，您会发现收集信息和准备表单很有用。

在您转至描述命名约定之前，您可能想要查看 JKL Toy 公司的“应用程序描述”表单示例。

示例: JKL Toy 公司的应用程序描述表单

Sharon Jones 在“应用程序”描述表单上列示公司应用程序的缩写。她还简要描述了用户如何使用这些应用程序。

客户订单（CO）
输入、跟踪和交付订单。打印发票。

库存控制（IC）
管理成品和原料的库存级别。处理所有库存变更。

合同及定价（CP）
管理特殊定价和与客户的合同。

应收帐款（AC）

跟踪当前余额。打印月报表。

下表包含 Sharon Jones 对“客户订单”应用程序的描述。她系统地准备了她的表单，以一个应用程序开始，然后描述其它程序。

表 6. JKL Toy 公司的“应用程序描述”表单：示例

“应用程序描述”表单	
准备人：Sharon Jones	日期：99/3/9
应用程序名称：客户订单	缩写：CO
应用程序的简要描述：	输入客户订单，在交付前跟踪客户订单、交付订单和打印发票和货运票据。
主菜单名称：COMAIN	库：COPGMLIB
初始程序名称：NA	库：NA
为文件和程序列示由应用程序使用的库： • CUSTLIB • ITEMLIB • CONTRACTS • COPGMLIB	
定义应用程序的安全性目标，如是否有任何信息是机密的：	

除“客户订单”应用程序以外，Sharon Jones 还在 JKL Toy 公司系统上为以下应用程序准备了“应用程序描述”表单：

- 库存控制
- 合同和订价
- 应收帐款。

下一步，您可以为系统上的对象描述命名约定。

描述命名约定

当您了解系统如何命名对象时，可以计划和监视安全性，解决问题并计划备份与恢复。大多数应用程序具有给对象（如库、文件和程序）指定名称的规则。如果您的应用程序来自不同的源，则它们可能每个都具有其各自独特的命名系统。

确保在“命名约定”表单中记录应用程序和对象的所有命名约定。在“命名约定”表单中，列示您的应用程序用于命名库和文件的规则。您可能想要对其它命名约定（例如程序和菜单）使用空白行。如果您的应用程序来自不同的源，则它们可能每个都具有其各自独特的命名约定。描述每个应用程序的命名约定。您可能需要准备多个“命名约定”表单。

在您转至描述库信息之前，您可能要查看 Sharon 在 JKL Toy 公司的系统上如何使用对象命名约定的示例。

示例：JKL Toy 公司的命名约定表单

下表仅显示库和文件的命名约定。您还将需要描述系统上其它类型对象的命名约定。“命名约定”表单包含几个公共对象；然后，您可能具有其它将需要准备的对象。

表 7. JKL Toy 公司的“命名约定”表单: 示例

“命名约定”表单	
准备人: Sharon Jones	日期: 99/3/9
对象类型	**命名约定**
库	包含文件的库具有有意义的名称，如 CONTRACTS 或 ITEMLIB。程序库使用应用程序缩写后跟 PGMLIB，如 ICPGMLIB。
文件	大多数文件都具有有意义的名称，如 CUSTMAST 表示“主客户”文件，或 ITEMMAST 表示“主商品”文件。其它应用程序文件（仅用于为了程序员理解）以应用程序缩写后跟 FILE 和一个数字来命名，如 ICFILE14。

完成“命名约定”表单之后，可以开始描述库信息。

描述库信息

在描述了命名约定之后，应该描述系统上的库。库标识和组织系统上的对象。将类似的文件一起放在一个库中允许用户容易地访问关键的应用程序和文件。还可以定制用户的权限，以便他们可以访问某些库，但不能访问其它库。为每个应用程序描述系统上的所有库。您可能需要准备多个“库描述”表单

注: 只填写关于库的描述性信息。当计划库的资源安全性时，将填写“库描述表单”的其余部分。以后需要将有关权限的信息添加至库中。有关完成“库描述表单”的剩余部分的详细信息，参见“计划应用程序库的安全性”。

继续之前，确保完成以下操作:

- 填写“命名约定表单”的库和文件部分。
- 填写每个应用程序库的“库描述”表单中的描述性信息。

在您绘制应用程序图表之前，您可能要查看 JKL Toy 公司的 Sharon Jones 如何描述库的示例。

示例: JKL Toy 公司的库描述表单

以下两个表描述了 JKL Toy 公司的“客户订单应用程序”使用的两个库。第一个表描述包含文件的库，第二个表描述包含程序的库。

表 8. JKL Toy 公司的“库描述表单”: 包含文件的库示例

“库描述”表单	
准备人: Sharon Jones	日期: 99/3/9
库名称: CUSTLIB	描述性名称（文本）: 客户记录库
简要描述此库的功能:	容纳所有客户文件，包括订单和应收帐款。

表 9. JKL Toy 公司“库描述表单”: 包含程序的库示例

“库描述”表单	
准备人: Sharon Jones	日期: 99/3/9
库名称: COPGMLIB	描述性名称（文本）: 客户订单程序库
简要描述此库的功能:	容纳用于客户订单应用程序的所有程序。

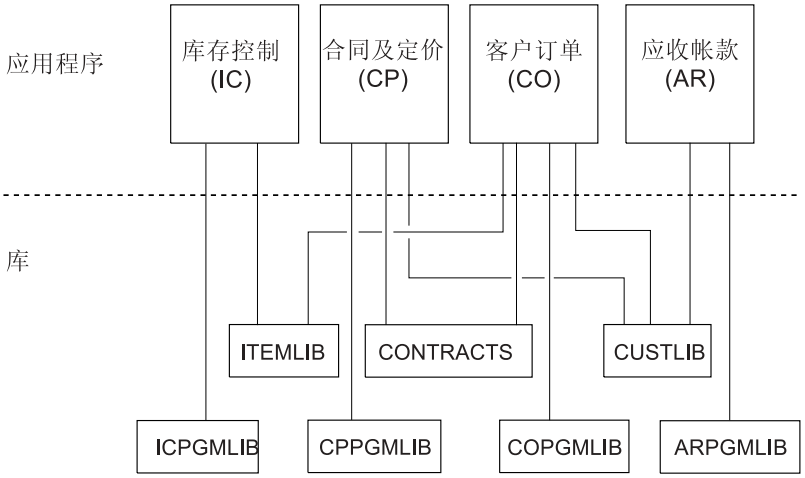
在描述库后，应该为系统绘制应用程序图表。

绘制应用程序图表

当准备“应用程序描述”和“库描述”表单时，可能会发现绘制显示应用程序和库之间关系的图表很有用。图表将有助于您计划用户组和资源安全性。

下图显示 Sharon Jones 绘制的 JKL Toy 公司的应用程序和库的图表:

JKL Toy 公司的应用程序和库图表



现在收集关于应用程序和库的一些信息将帮助您作出需要作出的许多安全性决定。将这看作是更了解您的系统和应用程序的机会。

要确保收集了所需要的应用程序信息，您应该:
- 完成系统上每个商业应用程序的“应用程序描述”表单。
- 可选择为系统上的每个特殊应用程序准备“应用程序描述”表单。
- 填写“命名约定”表单的库和文件部分。
- 为每个应用程序库准备“库描述”表单。
- 绘制您的应用程序和库之间的关系图。

当您完成了这些表单时，可以开始计划您的整体安全性策略。

计划您的整体安全性策略

在计划应用程序的安全性之后，您随时可以开始您的整体安全性策略。首先，需要对系统上安全性的整体方法作出决定。当您作出这些决定时，在公司目前的需要与未来的需要之间进行权衡。

使用此信息帮助完成计划过程，以确定您的安全性策略和目标。还可以使用此信息来帮助您选择基本系统值，这些值影响系统上的所有用户。

您需要什么表单?

要完成计划您的应用程序，使用系统值选择表单。

当查看这些主题来作出关于系统值的决定时，应该使用已完成的“物理安全性计划”表单和“应用程序描述”表单。

查看以下主题来计划您的安全性策略:

- 编写安全性策略
- 选择您的安全级别
- 选择影响注册的系统值
- 选择影响密码的系统值
- 使用系统值来定制您的系统

编写您的安全性策略

在开始计划之前，准备系统上关于安全性的公司策略的声明。此声明是您和公司的最高领导之间的协议。它帮助您作出决定并确定什么是最重要的。您的安全性策略应该陈述您的整体方法是什么以及哪些信息资产需要保护。

每个系统都应该具有安全性。您可以对您的安全性采用以下方法之一:

- **严格的**: 某些人将这称为“需要知道（need-to-know）”安全性方案。在严格的安全性环境中，仅给予用户对他们完成其作业所需要的信息和功能的访问权。排除所有其他人。许多审计员都建议使用严格的方法。
- **一般的**: 一般的安全性方法根据已分配给用户的权限来给予用户对对象的访问权。
- **不严格的**: 在不严格的安全性环境中，允许授权用户访问系统上的大多数对象。因为单个部门或小公司通常在其系统上使用不严格的方法，所以应限制对于特定的关键或机密资源的访问。

您的整体方法可以帮助您作出关于特定安全性需要的决定。系统的安全性方法应该与用于访问整个公司的信息的方法匹配。如果您不能确定要使用什么方法，则尝试以下方法:

- 使用已完成的“应用程序描述”表单来确定谁应该或不应该具有对于那些应用程序的访问权。
- 检查您在公司中使用的技术。例如，如果计划将您的系统或网络连接至因特网，则您将需要一个更限制的安全性环境来保护您的系统不让来自外部因特网用户的访问。
- 与组织的其它成员（如安全性审计员）讨论来更好地确定安全性需要。

记住，您始终可以更改您的策略。大多数公司发现，随着公司规模的扩长，需要更严格的安全性。此信息帮助您设置这样一个安全性方案，该方案允许您以后添加更多的安全性，而不必作大量更改或再次测试全部应用程序。

要保护什么内容

除了在您的安全性策略中说明安全性的整体方法外，还需要标识您公司的关键信息资产。应该将您的安全性系统设计成保护此信息。可以使用几种要求来确定关键资产:

- **机密性**: 对于公司中的人通常不可用的信息。工资单是机密信息的一个示例。
- **竞争力**: 给予您竞争优势的信息，如产品规格和配方。
- **运作**: 您计算机上对于企业的日常运作所必需的信息，如客户记录和库存余额。

Sharon Jones（安全主管）和 John Smith（公司总裁）一起工作来准备其安全性策略的声明。John Smith 使用这些注意事项来起草 JKL Toy 公司的安全性策略。在他们完成

计划和设置其安全性之后，您可能想查看 JKL Toy 公司发送至所有雇员的安全性策略。当您遍历这些计划主题时，记住记下您想要添加至您的安全性策略的内容。

表 10. JKL Toy 公司的安全性策略：示例

整体方法

不严格的：大多数人需要访问大部分信息。

关键信息

- 合同和特殊定价
- 工资单
- 客户和库存记录只对公司雇员可用。

一般规则

- 每个系统用户都将有一个用户概要文件。用户不能共享概要文件或密码。
- 用户必须每隔 60 天更改一次密码。

记下关于您的安全性策略的内容之后，您可以选择您的安全性级别。

选择您的安全级别

QSECURITY 系统值允许您控制在系统上需要多大级别的安全性。要了解安全级别如何工作，将您的系统看作是一个建筑物，人们正尝试进入其中。

级别 20：密码安全性

如果您选择级别 20，则您具有一些安全性保护。建筑物门口的守卫询问标识和密码。只允许具有两者的人进入建筑物。但是，一旦人们进入到里面，他们就可以到处走并执行他们想要做的任何事情。

如果某个人偷听到密码并使用它通过门口的守卫，则您不具有保护。

级别 30：密码和资源安全性

级别 30 给予您在级别 20 所具有的一切，并且您可以控制谁进入您的建筑物的某些地方以及当他们到达那里时作什么。您可以将您建筑物的某些地方指定为公共的，而其它地方受门口的守卫限制。

可以允许对受限制区具有访问权的人作他们想作的任何事情，或可以要求他们对授权信息职员程序（程序）提出其信息请求。使用别人的密码进入的闯入者可能仍必须通过里面的守卫才可到达受保护的部分。

级别 40：完整性保护

在级别 40，您获取级别 30 的所有保护，但系统验证用户的访问权。建筑物内门口的守卫检查密码并记录进入房间的所有用户。

级别 50：高级完整性保护

在级别 50，通过验证签名记录的任何人的标识，守卫执行一组更严格的规则来防止具有特殊知识的人通过受限制的门。

建议

iSeries 交付时安全级别设置为 40。无论您的安全性策略是严格的、一般的还是不严格的，安全级别 40 都是大多数安装的最好选择。如果您选择不严格的方法，则可以设置您系统上大多数资源的公共访问权。通过最初使用安全级别 40，您可灵活地使您的系统将来更安全，而不需作许多更改。

如果您正购买应用程序，则与您的应用程序供应商一起检查以确保在级别 40 测试过程序。某些应用程序使用在安全级别 40 导致错误的操作。如果尚未在级别 40 或 50 测试过您的应用程序，则用级别 30 开始。使用审计日志功能来查看您的应用程序是否记录权限故障。如果未记录，则可以更改为级别 40 或 50。

安全级别 50 防止在大多数系统上不正常发生的事件。无论何时在您的系统上运行程序，系统进行附加检查。此附加检查会对性能有负面影响。

在系统值选择表单中输入您的安全级别的选择之后，您可以选择影响注册的系统值。

选择影响注册的系统值

在选择您的安全级别之后，通过使用系统值，您可以定制在屏幕上用户看到的内容以及它们与系统如何进行交互。您将需要计划这些系统值并使用“系统值选择”表单来记录您的选择。

下表描述本主题中所使用的系统值。

表 11. iSeries 系统值及其描述

系统值	描述
QMAXSIGN	限制连续注册尝试次数。
QMAXSGNACN	指定如果达到连续注册尝试次数时，系统执行的操作。
QLMTDEVSSN	确定用户是否可以使用相同的用户概要文件在多个工作站上注册。
QINACTITV	确定系统何时对不活动作业执行操作。
QINACTMSGQ	确定当交互式作业已在 QINACTITV 系统值所指定的时间内不活动时系统执行的操作。
QDSCJOBITV	控制系统是否结束以及何时结束已暂时断开连接的作业。
QLMTSECOFR	限制安全主管，该主管对特定设备的系统上所有对象都具有权限。

限制注册尝试次数（QMAXSIGN 和 QMAXSGNACN）

两个系统值确定某个人可以尝试注册到您的系统上的次数和一旦达到限制时系统执行的操作。

最大注册尝试次数（QMAXSIGN）系统值限制在执行某个操作之前系统允许的连续不正确的注册尝试次数。不正确的注册尝试指某个人尝试使用对工作站无效的密码或不正确的权限来使用特定用户概要文件。

最大注册操作（QMAXSGNACN）系统值指定如果某个人连续太多次尝试注册，系统将执行的操作。可能的值为:

1 防止对设备的更多次注册尝试。这称为禁用设备。在授权人员使用

WRKCFGSTS 命令使设备联机之前，没有人可在设备上注册。此选项通常不具有足够的保护，特别是当从个人计算机或远程系统尝试注册到您的系统时。

系统操作员或对设备具有 *USE 权限的任何人都可以使设备再次可用。

2 防止对用户概要文件的更多次注册尝试。这称为禁用用户概要文件。在授权人员通过使用“更改用户概要文件”（CHGUSRPRF）命令启用该概要文件之前，没有人可以使用该概要文件注册。

要启用某个用户概要文件（更改状态），您必须是具有使用该概要文件权限的安全性管理员。

3 同时禁用用户概要文件和设备。

风险和建议

某些喜欢恶作剧的人喜欢进行猜测密码和闯入系统的挑战。通过限制您允许的注册尝试次数，可以限制他们的猜测次数。

最大无效注册（QMAXSIGN）系统值确定您允许多少次注册尝试。将其设置为足够高，以避免阻止用户。将其设置为足够低，以防止粗心输入并防止给潜在的闯入者过多猜测次数。应该将最大注册尝试次数的值设置为在 3 和 5 之间。

建议的最大注册操作（QMAXSGNACN）为 3，尽管禁用设备以及用户概要文件可能会对系统用户造成不方便。位于秘密地方的工作站可能给予闯入者尝试许多不同的用户概要文件和密码组合的机会。如果您的系统没有因为其位置而造成风险的工作站，则只禁用用户概要文件可能就会提供足够的保护。

检查已完成的“物理安全性”表单。如果您在远程位置具有工作站或具有远程用户（通过电话线或 VPN 连接访问您的系统的用户），则您可能要更严格地限制注册。确保将您对 QMAXSIGN 和 QMAXSGNACN 的选择添加至“系统值选择”表单的“第二部分”。

在您选择每次将用户限制于一个工作站的系统值之前，您可能会发现查看说明这些系统值如何一起工作来限制注册尝试次数的示例很有用。

示例：限制注册尝试次数： Sharon Jones 将注册尝试次数限制为 3（QMAXSIGN 为 3），且选择了如果超过该限制时则同时禁用概要文件和设备（QMAXSGNACN 为 3）。以下是当达到这些值时可能发生的情况：

1. Roger 两次不正确地输入他的密码。
2. 在第二次尝试之后，他接收到一个消息，警告他再次不正确注册尝试将会禁用用户概要文件。
3. 他犯了另一个错误。
4. 系统禁用他的概要文件且工作站不再显示“注册”屏幕。如果 Roger 尝试在另一个工作站上注册，则他会接收到一条错误消息。
5. 现在，他需要请求 Sharon 启用他的概要文件，以便他再次尝试。Sharon 或系统操作员还需要使 Roger 的工作站可用。如果 Roger 不记得他的密码，则 Sharon 可以给他一个临时密码，当他再次注册时，必须更改该密码。

接着，您可以查看每次将用户限制于一个工作站的系统值。

每次将用户限制于一个工作站

限制设备会话（QLMTDEVSSN）系统值确定同一用户是否可以同时在多个工作站上注册。可能的值为:

0 系统允许无限制数目的用户用相同的用户概要文件同时注册。

1 每次只能在一个设备上使用一个用户概要文件。在同一设备上用户可以有多个会话。

风险和建议

允许用户每次只注册到一个工作站会促进良好的安全性习惯。懒惰的安全性习惯会造成安全性风险:

- 如果将用户限制于一个设备，则阻止共享用户标识和密码。如果人们共享用户标识，则您丢失了控制权和责任。您不再能辨别谁在系统上真正执行什么功能。
- 用户必须记住在移动到另一个工作站之前注销工作站。处于注册状态的工作站（但未在使用中）会造成安全性风险。

系统值 QLMTDEVSSN 的建议设置为 1，它将用户限制于单个设备。给予每个系统用户具有适当权限的唯一用户标识和密码，然后将他们限制为每次使用一个工作站。确保将您对 QLMTDEVSSN 的选择添加至“系统值选择”表单的“第二部分”。

接着，您可以开始计划不活动作业的系统值。

计划不活动作业的系统值

三个系统值一起工作来确定当用户忘记注销工作站时系统执行什么操作。

不活动作业超时时间间隔（QINACTITV）

QINACTITV 系统值确定如果已注册屏幕但在指定的时间周期内不活动时系统是否执行操作。

注: 不活动指在指定的时间间隔期间用户未按执行键或功能键。

不活动作业消息队列（QINACTMSGQ）

QINACTMSGQ 系统值的设置确定当在系统值 QINACTITV 中指定的时间限制于期时，系统执行什么操作。如果您选择 ENDJOB，则系统结束不活动时间超过为 QINACTITV 选择的超时时间间隔的任何作业。如果您选择 DSCJOB，则系统与不活动作业断开连接。如果您指定消息队列的名称，则当作业过长时间不活动时系统将警告消息发送至该队列。

当系统与工作站上的作业**断开连接**时，它临时暂挂该作业。工作站返回到注册屏幕。当同一用户在同一工作站上再次注册时，已断开连接的作业恢复。

断开连接的作业超时时间间隔（QDSCJOBITV）

QDSCJOBITV 系统值控制系统是否结束以及何时结束已暂时断开连接的作业。作为 QINACTITV 和 QINACTMSGQ 系统值的结果，系统可以与作业自动断开连接。使用“操作辅助”菜单中的选项或“与作业断开连接”（DSCJOB）命令，用户还可以请求临时注销（断开连接）其作业。

风险和建议

如果 Sharon 在离开前忘记注销她的工作站，John 可以走到工作站并执行允许她在系统上执行的任何功能。

特别由于以下两个原因，您应该管理不活动的屏幕:

- 您具有严格的安全性环境且在系统上存储了机密信息。
- 您将工作站放在您公司外的人可以容易地接近它们的地方。

正常作业责任经常会在用户的工作站上中断用户。利用这三个系统值一起工作的方式来允许正常中断而仍保护您的系统安全性。

要消除这些风险，IBM 建议使用 QINACTITV、QINACTMSGQ 和 QDSCJOBITV 系统值一起来允许正常的工作中断而仍保护您的系统安全性。

不活动作业超时时间间隔（QINACTITV）：使该时间间隔足够短以防止无人照管工作站，但不会短到不方便用户。建议的设置为 30 分钟。当作业已 30 分钟不活动时，系统执行在不活动作业消息队列中所指定的操作。

不活动作业消息队列（QINACTMSGQ）：选择断开连接作业。系统将已在不活动作业超时时间间隔中指定的时间段内不活动的任何作业断开连接。系统暂挂作业并注销屏幕。当同一用户再次注册时，作业将从它离开的地方继续。

这对用户更方便，因为系统暂挂而不是结束其作业。将不活动作业断开连接为您的系统提供与结束该作业同样多的保护。

注: 系统不能将某些作业断开连接。如果系统不能将不活动作业断开连接，则它结束该作业。这可能会导致丢失信息。考虑设置 QINACTMSGQ 来将消息发送至系统操作员消息队列。

断开连接的作业超时时间间隔（QDSCJOBITV）：希望系统用户在他们需要短时间离开其工作站时临时注销系统，以及在他们要较长时间离开时希望他们完成其工作并注销。

在您的系统启动夜间处理（如“自动清除”）之前，使用 QDSCJOBITV 结束已断开连接的作业。将其设置为足够长，以给予用户在营业日的大部分时间来返回到工作站，但设置为足够短，以在夜间处理启动之前结束作业。选择 300 分钟（5 小时），该时间给予夜间处理足够时间来完成，而不会干预用户的作业。

注: 为了防止两个用户尝试同时更改同一信息，在更新记录之前，系统**锁定**该记录。当系统将用户的作业断开连接时，对资源的任何锁定仍起作用。取决于您的应用程序设计和系统上的用户数，锁定可能会在您的系统上导致性能问题。与您的程序员或应用程序供应商一起检查来确定锁定是否会影响您的性能。

您可能要查看关于这些系统值如何一起工作来处理系统上不活动的作业的示例。

在“系统值选择”表单记录对不活动作业的决定之后，您可以决定如何限制安全主管可以注册的位置。

示例: 用 QINACTITV、QINACTMSGQ 和 QDSCJOBITV 系统值处理不活动的作业:
假定已将不活动的作业超时时间间隔（QINACTITV）设置为 30 分钟。系统将不活动的作业断开连接（QINACTMSGQ 为 DSCJOB）。断开连接的作业超时时间间隔（QDSCJOBITV）是 300 分钟（5 小时）。例如，如果 Sharon 在上午 9:30 忘记注销，则系统在上午 10:00 将她的作业断开连接，并将在下午 3:00 结束该作业。

在“系统值选择”表单的“第二部分”上添加您对 QINACTITV、QINACTMSGQ 和 QDSCJOBITV 系统值的选择。

在“系统值选择”表单记录对不活动作业的决定之后，您可以决定如何限制安全主管可以注册的位置。

限制安全主管可以注册的位置

您可能要将具有更改安全性和控制对象的权限的用户限制于一定的工作站。这就防止这些用户在远程位置注册到工作站而您不知道。系统值 QLMTSECOFR（限制安全主管）允许您这样作。如果您将 QLMTSECOFR 设置为 1，则具有所有对象（*ALLOBJ）或服务（*SERVICE）特权的用户只能在您指定的控制台或其它工作站上注册。

QLMTSECOFR 将安全主管、对系统上所有对象都具有权限的用户以及服务人员限制于控制台。您可以使用“授予对象权限”（GRTOBJAUT）命令来给予这些用户对其它设备的访问权。

注: 为了 QLMTSECOFR 系统值起作用，您的系统安全级别需要为 30 或更高。

风险和建议

您应该将 QLMTSECOFR 系统值设置为 1。如果某个人偷听或猜测到具有安全主管概要文件的某个人的密码，则他们还必须获取允许他们注册的设备的访问权。

在“系统值选择”表单的“第二部分”中填写了对于 QLMTSECOFR 的选择之后，您可以选择影响密码的系统值。

选择影响密码的系统值

应该允许用户指定其自己的密码，而不是安全主管指定其密码。当用户创建其自己的密码时，他们通常不需要写下它们。写下的密码往往存储在明显的位置而造成安全性风险。

创建密码的技巧

您的用户可能很难想出好的密码。建议使用此技术：使用易于记住的句子来帮助您创建难于猜测的密码。例如，度假之后，您可以使用句子 “July 4th fishing was poor” 来创建密码 J4FWP。

几个系统值管理密码。您可以控制需要用户多长时间更改密码。还可以建立许多规则来防止使用易于猜测的密码。这些系统值的其中许多都对大型组织很重要。一些则对每个人都重要。

通过使用 ASSIST 菜单中的一个选项或“更改密码”（CHGPWD）命令，用户可以指定其自己的密码。当用户更改其自己的密码时，系统对照密码系统值检查新的密码。如果用户使用 CHGUSRPRF 命令更改密码，则系统不会对照安全性系统值检查新的密码。

注: 如果您已设置任何密码系统值，则除非您使用 CHGUSRPRF 命令来设置密码，否则系统不允许新的密码与用户概要文件名称相同。

下表显示影响密码及其定义的系统值:

表 12. iSeries 与密码有关的系统值

系统值	描述
QPWDEXPITV	要求用户在指定的持续时间之后更改其密码。
QPWDMAXLEN	允许您为密码指定最大字符长度。
QPWDMINLEN	允许您为密码指定最小字符长度。
QPWDRQDDIF	防止用户在两个不同的密码之间变换。

这些主题提供关于这些与密码有关的系统值的更多详细信息:

- 确定密码持续时间
- 确定密码长度
- 限制重复密码

在 CL 命令行输入 `WRKSYSVAL *SEC` 并查看从字符 QPWD 开始的系统值的联机信息。

确定密码持续时间

QPWDEXPITV 系统值确定需要用户多长时间更改其密码。

当用户的密码接近到期日期时，系统通知用户。如果密码到期，则系统提示用户在下次注册时更改其密码。

建议

用户应该定期更改其密码。这就阻止了与其它系统用户共享密码。而且，如果授权用户了解某人的密码，则该密码将只在短时间内起作用。将密码时间间隔设置为足够长，以避免激怒用户，但设置为足够短，以提供良好的安全性。要避免这些问题，设置时间间隔在 45 到 60 天之间。

在“系统值选择”表单的“第二部分”中为 QPWDEXPITV 系统值输入您的选择之后，您可以确定密码的长度。

确定密码长度

某些用户不喜欢输入。如果您让他们输入，则他们将选择一个字母的密码或其首写字母。不幸的是，简短的密码使闯入者较易于有幸猜中。QPWDMINLEN 系统值让您设置您的系统上所有密码的最小长度。

如果您的系统与其它系统通信，则用户可以在两个计算机之间交换密码。某些通信方法将密码限制为最多 8 个字符。QPWDMAXLEN 系统值允许您为密码指定最大长度。

建议

按 6 设置您的最小密码长度。这就排除使用首写字母并促使用户在选择密码时更具创造性。如果您的系统与其它系统通信，则按 8 设置您的最大密码长度。

在您“系统值选择”表单的“第二部分”中为 QPWDMINLEN 和 QPWDMAXLEN 系统值输入您的选择之后，您可以决定要如何限制重复密码。

限制重复密码

“更改密码”（CHGPWD）命令要求新密码与旧密码不同。然而，用户可以在两个不同的密码之间来回变换（除非您使用 QPWDRQDDIF 系统值来防止它）。下表显示对于 QPWDRQDDIF 系统值的选择。

表 13. QPDRQDDIF 系统值的值

值	检查重复的密码数
0	0 允许重复密码。
1	32
2	24
3	18
4	12
5	10
6	8
7	6
8	4

建议

使用密码到期时间间隔和重复密码值来要求该密码一年内是唯一的。例如，如果密码在 60 天内到期，则为 QPWDRQDDIF 系统值选择 1。

在“系统值选择”表单的“第二部分”中为 QPWDRQDDIF 系统值输入您的选择之后，您可以决定如何使用系统值来定制您的系统。

使用系统值来定制您的系统

iSeries 使用系统值和网络属性来控制安全性以外的许多事情。系统和应用程序程序员使用其中的大多数系统值和属性。安全主管应该设置几个系统值和网络属性来定制您的系统。

给予您的系统一个名称

使用 SYSNAME 网络属性来将名称指定给您的系统。系统名称出现在您的注册屏幕的右上角和系统报表中。当您的系统与另一个系统或与使用 iSeries Access Windows 版的个人计算机通信时，也使用该系统名称。

当您的系统与其它系统或个人计算机通信时，系统名称标识您的系统并将它与网络上的其它系统区分开。每当计算机通信时，它们交换系统名称。一旦指定了系统名称，就不应该更改它，因为更改它会影响您的网络中的其它系统。

建议

为您的系统选择一个有意义的且唯一的名称。即使您现在不与其它计算机通信，但可能将来会通信。如果您的系统是网络的一部分，则网络管理员将可能告诉您要使用什么系统名称。

例如，JKL Toy 公司的 Sharon Jones 决定将系统命名为 JKLTOY。

显示系统上的时间与日期

可以设置系统打印或显示日期时的年、月和日出现的顺序。还可以指定在年（Y）、月（M）和日（D）之间系统应该使用什么字符。

系统值 QDATFMT 确定日期格式。以下图表显示对于每个可能的选择，系统如何打印日期 2000 年 6 月 16 日:

表 14. QDATFMT（ “系统日期” 格式）

您的选择	描述	结果
YMD	年、月和日	00/06/16
MDY	月、日和年	06/16/00
DMY	日、月和年	16/06/00
JUL	儒略日期	00/168

注: 这些示例使用斜杠（/）日期分隔符。

系统值 QDATSEP 确定系统在年、月和日之间使用什么字符。下表显示您的选择。使用一个数字来指定您的选择:

表 15. QDATSEP（系统日期分隔符）

分隔符字符	QDATSEP 值	结果
/（斜杠）	1	16/06/00
-（连字符）	2	16-06-00
.（句点）	3	16.06.00
,（逗号）	4	16,06,00
（空白）	5	16 06 00

注: 以上示例使用 DMY 格式。

QTIMSEP 系统值确定系统在显示时间时使用什么字符来分隔小时、分钟和秒。使用一个数字来指定您的选择。下表显示将如何使用每个值来格式化上午 10:30 这个时间:

表 16. QTIMSEP（系统时间分隔符）

分隔符字符	QTIMSEP	结果
:（分号）	1	10:30:00
.（句点）	2	10.30.00
,（逗号）	3	10,30,00
（空白）	4	10 30 00

决定如何命名您的系统设备

系统自动配置连接至它的任何新的显示站和打印机。系统给每个新设备一个名称。QDEVNAMING 系统值确定如何指定名称。以下图表显示系统如何命名连接至系统的第三个显示站和第二个打印机:

表 17. 系统设备命名

您的选择	命名格式	显示站名称	打印机名称
1	iSeries	DSP03	PRT02
2	S/36	W3	P2

表 17. 系统设备命名 (续)

您的选择	命名格式	显示站名称	打印机名称
3	设备的地址	DSP010003	PRT010002

注: 在以上示例中，将显示站和打印机连接至第一根电缆。

建议

除非正运行要求 S/36 命名的软件，否则使用 iSeries 命名约定。显示站和打印机的 iSeries 名称比使用设备地址的名称简单一点。显示站和打印机名称出现在几个“操作辅助”屏幕上。打印机名称还用来管理打印机输出。

在系统配置了一个新设备之后，使用“更改显示设备”（CHGDEVDSP）命令或“更改打印机设备”（CHGDEVPRT）命令来输入有意义的设备描述。在描述中包括设备的物理地址及其位置，如 *John Smith 的办公室，线路 1 地址 6*。

选择您的系统打印机

使用 QPRTDEV 系统值来指定您的系统打印机。此系统值、用户概要文件和作业描述确定作业使用哪个打印机。除非用户概要文件或作业描述指定另一个打印机，否则作业使用系统打印机。

建议

通常，系统打印机应该是系统中最快的打印机。对于长的报表和系统输出，使用系统打印机。

注: 在安装和配置系统之后，才会知道打印机的名称。现在记下系统打印机的位置。以后填写打印机的名称。

允许显示已完成的打印机输出

系统给用户提供查找其打印机输出的能力。“使用打印机输出”屏幕显示当前正在打印或正等待打印的所有输出。还可以允许用户查看已完成的打印机输出列表。此屏幕显示输出是何时打印的以及是在哪个打印机上打印的。这在查找丢失的报表时很有用。

作业记帐功能和 QACGLVL 系统值允许您显示已完成的打印机输出。QACGLVL 系统值的 *PRINT 选项允许保存关于已完成的打印机输出的信息。

建议

存储关于已完成的打印机输出的信息会占用系统上的空间。除非认为用户将打印许多报表，否则您可能不需要提供此功能。在“系统值选择”表单中，输入“否”。此值将作业记帐级别设置为 *NONE。

- 确保为您自己的公司编写了与 Sharon Jones 和 John Smith 所准备的 JKL Toy 公司示例相似的安全性策略声明。
- 确保在“系统值选择”表单中对系统值输入了您的选择。
- 记下有关想要在您的安全性备忘录中包括的内容。

在“系统值选择”表单中输入了所有系统选项并写好安全性策略之后，您可以计划用户组。

示例: JKL Toy 公司的安全性策略

以下备忘录说明 John Smith（JKL Toy 公司的总裁）发送给他的雇员的安全性策略。他使用他和 Sharon 创建的注意事项来制订此安全性备忘录。

表 18. 示例: JKL Toy 公司的安全性备忘录

自: John Smith 总裁

JKL Toy 公司

至: 所有 JKL Toy 公司雇员

主题: 新系统的安全性

您们都已出席有关新系统的信息会议。将使用该系统的雇员都已开始培训，并将在下周开始处理客户订单。我们期望此系统将很快成为我们的企业成功的关键。

我想回顾我们的安全性决定和策略，并强调它们的重要性。已设计这些策略来保护对我们企业的关键信息。

- Sharon Jones 负责新系统的安全性。Ken Harrison 将辅助她。如果您们有任何问题，或怀疑存在安全性问题，请与他们联系。
- 有关谁能在系统上执行此功能的决定是基于关于信息的当前策略作出的。例如:
  - 合同和特殊定价信息被认为是机密的。不应对公司以外的任何人透露。
  - 仅可以设置“会计”并更改我们的客户的信用限制。
- 需要使用该系统的每个人都将接收一个用户标识和密码。将要求您在第一次注册到系统上时更改密码，并此后每 60 天更改一次。选择您能够记住但不明显的密码。用您的用户标识接收到的表单有一些创建密码的建议。
- *密码不可与别人共享。*希望您们能够在系统上执行工作所必需的任何事情。如果需要访问信息，与 Sharon 或 Ken 联系。如果忘记密码，Sharon 或 Ken 可以立即为您设置一个新密码。任何人都不应使用别人的用户标识和密码来注册。
- 您可能已经了解如何在工作站中使用记录和回放功能来保存输入。不要使用此功能来存储您的密码。
- 当您离开办公桌时，不要让工作站处于注册状态。您在培训中已了解如何临时注销工作站。如果需要暂时离开办公桌，使用此功能。如果您将长时间离开，则完成您的工作，并正常地注销。

  在一般公众能够访问的位置，如装运码头、客户服务区域和远程销售办公室，离开工作站时注销特别重要。
- 尽管系统部件非常坚固，但仍请避免冲撞它，或在它的顶部放置任何东西。系统部件上的控制面板正常情况下将已释放，但请不要触及它们。“会计”部门的成员有责任确保没有人损坏系统部件。

记住，新系统是为了让我们的工作更容易并提高商业性能。安全性策略应该有助于您，而不是阻碍您。如果有任何问题或建议，不要犹豫，请与 Sharon、Ken 或我联系。

在创建安全性策略的草稿之后，您可以开始计划用户组。

计划用户组

计划过程中的第一个步骤（决定您的安全性策略）类似于设置公司策略。现在您随时可以计划用户组，这类似于决定部门策略。

什么是用户组?

用户组正是其名称所表示的：需要以相同的方式使用相同的应用程序的一组人。通常，用户组由在同一部门工作且具有相似的作业责任的人组成。通过创建组概要文件来定义用户组。

组概要文件起什么作用?

组概要文件在系统上提供两种用途:

- **安全性工具**：组概要文件提供组织谁可以使用系统上某些对象（对象权限）的一种简单方式。可以为整个组定义对象权限，而不是为组中每一单个成员定义对象权限。
- **定制工具**：可以将组概要文件用作创建单个用户概要文件的模式。大多数人（是同一组的一部分）具有相同的定制需要，例如初始菜单和缺省打印机。可以在组概要文件中定义这些内容并将它们复制到单个用户概要文件。

组概要文件使您易于维护安全性和定制的简单且一致的方案。

需要什么表单?

要为您的用户组计划，需要以下表单:

- “用户组标识”表单
- “用户组描述”表单

注: 对于将在您的系统上的每个用户组，将需要一个“用户组描述”表单。

查看这些主题以帮助您完成以下表单:

- 标识用户组。
- 计划组概要文件。
- 选择影响注册的值。
- 选择限制用户做什么的值。
- 选择设置用户的环境的值。

标识用户组

当您计划您的用户组时，首先必须标识系统上的用户组。这允许您计划对这些组所需要的资源的访问。尝试使用简单的方法来标识您的用户组。考虑计划使用系统的部门或工作组。查看以前绘制的应用程序的应用程序图表。查看在工作组和应用程序之间是否存在自然的关系。

- 可以为每个工作组标识一个主应用程序吗？
- 了解每个组需要哪些应用程序吗？它们不需要哪些应用程序？
- 了解哪个组应该拥有每个应用程序库中的信息吗？

如果您对于那些问题可以回答“是”，则您可以开始计划您的用户组。然而，如果您回答“有时”或“可能”，则您可能会发现使用系统方法来标识您的用户组很有帮助。

您可能要查看使用此方法来标识用户组的示例。

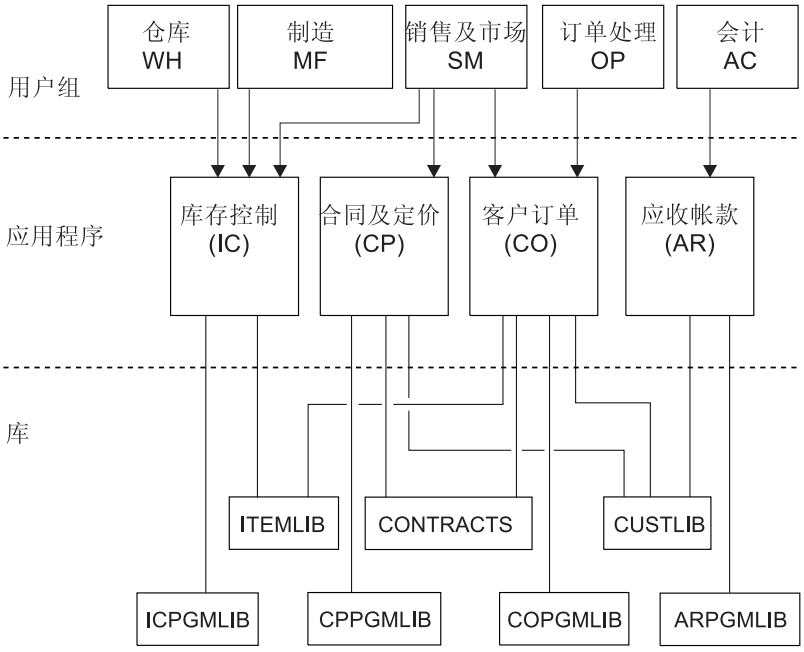
注: 使用户只成为一个组概要文件的成员可以简化安全性管理。然而，某些情况可以从让用户属于多个组概要文件中获益。

让用户属于多个组概要文件通常比将许多专用权限给予单个用户概要文件更易于管理。

示例: 标识用户组

如果工作组和应用程序之间的关系似乎复杂或含糊，则使用与“用户组标识”表单相似的矩阵技术可能会使事情更清楚。当在矩阵中绘制系统用户及其应用程序需求时，应该看到类似的模式出现。除填写“用户组标识”表单之外，Sharon Jones 还使用她的应用程序图表来标识哪些用户组需要访问应用程序。

以下插图显示 JKL Toy 公司应用程序图表。



如果您的安全性方法是不严格的，则使用 X 来指示用户需要应用程序。如果您的安全性方法是限制性的，则需要考虑人们如何使用应用程序。与在矩阵中放置 X 不同，如果某个人只需要查看应用程序中的信息，则使用 V（查看）。如果某个人需要对信息进行更改，则使用 C（更改）。如果某个人对该信息具有主要责任，则使用 O（所有者）。

例如，在 JKL Toy 公司，不同的组需要“定价和合同”应用程序:

- “销售及市场”部门设置价格和创建客户合同。他们*拥有*定价和合同信息。
- 客户订单部门间接更改合同信息。当他们处理订单时，合同中的数量会更改。他们需要*更改*定价和合同信息。
- 订单处理人员需要查看信用限制信息来计划其工作，但不允许他们更改该信息。他们需要*查看*信用限制文件。

表 19. JKL Toy 公司的“用户组标识”表单: 示例

“用户组标识”表单					
准备人: Sharon Jones		日期: 99/2/9			
		应用程序所需要的访问权			
用户名	部门	APP: CO	APP: IC	APP: PC	APP: AR
Ken H.	订单处理（OP）	O	C	C	C

表 19. JKL Toy 公司的“用户组标识”表单: 示例 (续)

Karen R.	订单处理（OP）	O	C	C	C
Kris T.	会计（AC）	V		V	O
Sandy J.	会计（AC）	V	C	V	O
Peter D.	会计（AC）	C		V	O
Ray W.	仓库（WH）	V	O	V	
Rose Q.	仓库（WH）	V	O	V	
Roger T.	销售及市场（SM）	C	C	O	C
Sharon J.	经理（MG）	C	C	C	C

注:

- 如果安全性环境是*不严格的*，则使用 X 来标记用户需要的应用程序。
- 如果安全性环境是*一般的*，则使用 A 来标记哪些用户将对哪些应用程序具有权限。
- 如果安全性环境是*严格的*，则可能需要使用 C（更改）、V（查看）和 O 来指定*如何*使用应用程序。

当 Sharon Jones 准备矩阵时，她记下了她的决定:

- 订单处理和会计互相提供支持。现在，它们需要类似的应用程序。然而，它们应该是单独的组，因为随着添加更多人，它们在将来将会变得更专门化。
- 虽然我们不允许订单处理直接更改库存或合同，但是，当他们创建和填写订单时，商品和合同余额会自动更改。以后这将会成为安全性问题吗?
- 销售及市场人员涉及企业的所有部分和每个应用程序。他们设置商品的价格和描述。尽管会计设置信用限制，但他们可以设置新的客户。他们负责设置所有合同条款和价格。

决定用户组应该有哪些用户。如果需要“用户组标识”表单帮助您作出决定，则填写该表单。

将用户添加至“用户组标识”表单之后，您可以计划组概要文件。

计划组概要文件

一旦标识用户组，就随时可以计划每个组的概要文件。所作的许多决定会影响安全性和定制。例如，当指定初始菜单时，可能将用户仅限制于该菜单。但也确保用户在注册之后看到正确的菜单。

作为示例，为一个用户组准备用户组描述表单。在完成了第一个表单之后，返回并完成所需要的其它组的表单。

iSeries 中的安全性和定制设计得很灵活。本主题中的计划方法提供一种很好的方式来设计组概要文件和作业描述，但程序员或应用程序供应商可能会建议另一种方法。

命名组概要文件

因为组概要文件充当一种特殊类型的用户概要文件，所以您可能要在列表和显示中方便地标识组概要文件。您需要给它们指定特殊名称。要在列表中一起显示，组概要文件应该以相同的字符开始，如 GRP（对于组）或 DPT（对于部门）。当命名用户组时，使用以下准则:

- 用户组名称最长可以为 10 个字符。

- 名称可以包括字母、数字和特殊字符: # 符号、$ 符号、下划线和 @ 符号。
- 名称不能以数字开始。

注: 对于每个组概要文件，系统指定一个组标识号（*组标识*）。通常，可以让系统生成*组标识*。如果在网络中使用系统，则可能需要为组概要文件指定特定的组标识。与网络管理员一起检查来验证是否需要指定组标识。

应该在“命名约定表单”中的适当字段中添加对于组概要文件的命名系统。例如，Sharon Jones 选择 DPT 作为组概要文件的命名约定。她填写“命名约定表单”的适当部分。

表 20. JKL Toy 公司的“命名约定表单”： “组概要文件”示例

对象类型	命名约定
组概要文件	使用字符 DPT 后跟部门缩写。组概要文件的文本描述应该是部门名称。

确定用户组需要哪些应用程序和库

如果尚未这样做，则将用户组添加至先前绘制的应用程序图表和库。此可视图像将帮助您决定每个组的资源和应用程序需要。

在“用户组描述表单”的“第一部分”中指示组的主应用程序，该程序是他们最常用的应用程序。列示组需要的其它应用程序。

检查“应用程序描述表单”和应用程序图表来查看每个组需要的库。与您的程序员或应用程序供应商一起检查来找出用于提供对这些库的访问的最好方法。大多数应用程序使用以下技术之一:

- 应用程序将这些库包括在用户的初始库列表中。
- 应用程序运行设置程序，该程序将库放在用户的库列表中。
- 库不必位于库列表中。应用程序始终指定库。

当运行应用程序时，系统使用库列表来查找您需要的文件和程序。**库列表**是系统进行搜索以获取用户所需要的对象的库的列表。库列表有两部分:

1. **系统部分**: 在 QSYSLIBL 系统值中指定它，系统部分用于 OS/400 库。不需要更改此系统值的缺省值。
2. **用户部分**: QUSRLIBL 系统值提供库列表的用户部分。用户的作业描述指定初始库列表，或在注册用户之后控制。如果您具有初始库列表，则它覆盖 QUSRLIBL 系统值。应用程序库应该包括在库列表的用户部分中。

使用作业描述

当用户注册到系统中时，用户的作业描述定义作业的许多特征（包括作业如何打印，批处理作业如何运行）和初始库列表。系统附带了一个作业描述（称为 QDFTJOBD），当创建组概要文件时可以使用该作业描述。然而，QDFTJOBD 指定 QUSRLIBL 系统值作为初始库列表。如果想要不同的用户组在注册时对不同的库具有访问权，则应该为每个组创建唯一的作业描述。

在“用户组描述表单”中列示组所需要的每个库。如果应该在组的作业描述中的初始库列表中包括库，则在表单中标记每个库名称。

在开始选择影响注册的值之前，可能要查看关于 Sharon Jones 如何描述在 JKL Toy 公司的用户组的示例。

示例: JKL Toy 公司的用户组描述表单

第一个表显示 Sharon Jones 为“销售及市场”部门准备的“用户组描述”表单的“第一部分”。注意，她未在组的初始库列表中包括库 CONTRACTS 和 CPPGMLIB。应用程序自动将它们添加到库列表中，而不是将它们包括在 DPTSM 初始库列表上。当用户退出应用程序时，系统从库列表中除去这些库。这为那些库提供了附加安全性，因为您仅能通过应用程序访问它们。

表 21. JKL Toy 公司“用户组描述”表单: 描述性信息示例

“用户组描述”表单	第一部分（共两部分）
准备人: Sharon Jones	日期: 99/5/9
组概要文件名称: DPTSM 组的描述: 销售及市场部门	
组的主要应用程序: 合同及定价 列示组所需要的其它应用程序: 库存（用于输入商品描述和价格）和客户订单	
列示组所需要的每个库。标记（✓）应该在组的初始库列表中的每个库: • ✓CUSTLIB • ✓ITEMLIB • ✓COPGMLIB • ✓ICPGMLIB • CPPGMLIB • CONTRACTS	

另外，Sharon 也为“仓库部门”开始了“用户组描述”表单。

表 22. “用户组描述”表单: 描述性信息

“用户组描述”表单	第一部分（共两部分）
准备人: Sharon Jones	日期: 99/5/9
组概要文件名称: DPTWH 组的描述: 仓库部门	
组的主要应用程序: 库存控制 列示组所需要的其它应用程序: 无	
列示组所需要的每个库。将一个选择标记（✓）放置在应该在组的初始库列表中的每个库前面: • ✓ITEMLIB • ✓ICPGMLIB	

在完成“用户组描述”表单的“第一部分”之后，可以开始选择影响注册的值。

选择影响注册的值

在系统上计划组概要文件之后，需要选择影响注册的系统值。在“用户组描述”表单的“第二部分”中输入您的选择。记住，您选择的值将会被复制，以便为组的成员创建单个概要文件。通过输入您选择的组概要文件名称和组的简短描述（文本）开始。

如果正确定制了系统，则用户只须在“注册”屏幕中输入他们的用户标识和密码。其用户概要文件提供其它注册值。

密码

将组概要文件的密码设置为 *NONE。这可防止任何人使用组概要文件注册。稍后，当您复制组概要文件来创建单个用户概要文件时，应为每个用户设置一个密码。

初始程序和初始过程

用户的初始程序（也称为**注册程序**）在系统显示第一个菜单之前运行。即使库是初始库列表的一部分，也将程序及其库的名称都放在组概要文件中。通过指定这两者，确保系统运行正确的程序，且不必担心库列表更改。

使用初始程序或过程是由于以下原因之一:

- 某些应用程序使用初始程序来设置应用程序环境。
- 您想要一个用户仅运行一个程序且从不会看到菜单。例如，在 JKL Toy 公司，在装运码头上使用工作站的人只能运行用于接收库存的程序。这可防止在公共位置中的工作站上的安全性暴露。

将用户的**限制能力**字段设置为 *YES 或 *PARTIAL 防止用户在“注册”屏幕上更改初始程序。

与程序员一起检查以查看应用程序是否需要初始程序或过程。

初始菜单和初始菜单库

初始菜单（也称为**第一个菜单**）是用户在注册之后看到的第一个菜单。初始程序在显示初始菜单之前运行。如果初始程序显示任何屏幕，则在系统显示初始菜单之前用户会看到那些屏幕。

通常，组的初始菜单应该是组的主应用程序的主菜单。同时指定菜单名称及其库。

如果将用户的**限制能力**字段设置为 *YES，则不允许用户在“注册”屏幕上更改初始菜单。如果将用户的*限制能力*字段设置为 *PARTIAL，则允许用户在“注册”屏幕上更改初始菜单。

当前库

当前库也称为**缺省库**。当为用户指定当前库时，发生几种情况:

- 如果用户创建任何对象（如查询程序），则除非用户指定另一个库，否则系统将那些对象放在当前库中。
- 系统自动将当前库添加至库列表的用户部分。可以在作业描述中的初始库列表上包括当前库，但不必这样做。
- 当前库成为库列表的用户部分中第一个库。系统在搜索用户库列表中的库之前搜索当前库以找到文件和程序。

- 如果不为用户指定当前库，则系统指定 QGPL（一般用途）库。

建议

如果计划使用“IBM Query iSeries 版”许可程序或另一个类似程序，则当前库特别重要。使用以下方法之一:

- 创建组中的每个人共享的库。将组的所有查询程序和文件放在该库中。给予它与组概要文件相同的名称并使之成为组的当前库。
- 给予计划使用“查询”的每个用户一个个人库。给予库与用户概要文件相同的名称。在组成员的单个概要文件中而不是在组概要文件中将该库指定为当前库,

在“用户描述”表单的“第二部分”中，填写对于影响注册的字段的选择。

在选择影响注册的值之后，可以选择限制用户可以执行什么操作的值。

选择限制用户可以执行什么操作的值

在“用户组描述表单”的“第二部分”中输入对于影响注册的值的选择之后，应该考虑限制用户在系统上可以执行什么操作。由于以下几个原因，您可能要限制用户可以执行什么操作:

- 防止人们使用 CL 命令。他们可能会受到诱惑去试验并无意地破坏某些事情。
- 将用户限制于特定应用程序和功能。
- 提供简单的环境，用户在其中不会由于不必要的选项而感到困惑。

许多因素确定用户可以执行操作的范围:

- 应用程序设计
- 系统值
- 资源安全性
- 组概要文件
- 用户概要文件
- 作业描述

在组或用户概要文件中的两个字段: **限制能力**和**用户类**，确定用户可以覆盖多少您作出的决定。

限制能力

限制能力字段称为**受限制的命令行使用**。可以限制用户是否可以更改“注册”屏幕中的值、输入命令以及更改其“辅助操作请求键处理”程序。可以选择严格限制（*YES）、一般限制（*PARTIAL）或无限制（*NO）。下表显示这些值中的每个值所允许的功能:

表 23. 限制能力值所允许的功能

限制能力值	更改初始程序	更改初始菜单	更改当前库	更改辅助操作请求程序	输入命令
*YES	否	否	否	否	一些[1]
*PARTIAL	否	是	否	否	是
*NO	是	是	是	是	是

表 23. 限制能力值所允许的功能 (续)

限制能力值	更改初始程序	更改初始菜单	更改当前库	更改辅助操作请求程序	输入命令
1	允许以下命令：SIGNOFF、SNDMSG、DSPMSG、DSPJOB、DSPJOBLOG 和 STRPCO。用户不能使用 F9 键从任何“操作辅助”菜单或屏幕来显示命令行。				

用户类

用户类（也称为**用户类型**）确定用户在“操作辅助”和系统菜单中看到什么选项。除非在**特权**字段中列示权限，否则用户类还确定允许用户执行什么系统功能。

对于受限制能力和用户类的建议

大多数用户不需要或不想访问 CL 命令或系统功能。“操作辅助”屏幕给予用户有关其自身的工作的足够信息和控制。这些建议允许用户仅访问他们完成任务所需要的那些系统资源:

- 在每个组概要文件中，将**限制能力**字段设置为 *YES。将*用户类*字段设置为 *USER。
- 为需要系统功能的单个用户覆盖这些规范。
- 确保您的菜单提供一种方法在应用程序之间移动（如果用户需要这样做）。

在“用户组描述”表单的“第二部分”中输入对用户类和限制能力的选择之后，可以选择设置用户环境的值。

选择设置用户环境的值

在“用户组描述”表单的“第二部分”中输入对于限制用户在系统上可以执行什么操作的选择之后，可以选择值来确定用户的操作环境。用户概要文件中的许多字段确定用户的操作环境：使用什么打印机、在哪里发送消息以及作业应该按什么优先级运行。对于这些字段中的许多字段，建议使用缺省设置。以下段落中描述了一些字段。

- **作业描述和作业描述库**：概要文件中的这些字段告诉系统当用户注册时使用什么作业描述。作业描述包含初始库列表。每个用户组都应该具有一个其名称与组概要文件相同的作业描述。通常将作业描述放在 QGPL 库中。
- **打印机设备和输出队列**：用户创建的任何打印机输出转至概要文件中所列示的打印机设备（除非特定打印作业将它发送至另一个打印机）。用户组的成员通常在一起并共享同一打印机。可以在组概要文件中指定该打印机并将其复制到每个单个的用户概要文件。用户的打印机设备也称为**缺省打印机**。

  在打印之前，输出队列包含打印机输出。通常，每个打印机设备有其自己的同名输出队列。可以为输出队列指定 *DEV 来告诉系统使用打印机设备的输出队列。

  在“用户组描述”表单中填写作业描述及其库的名称以及缺省打印机和输出队列字段。
- **设置“操作辅助”界面**：当交付系统时，“操作辅助”菜单是用于每个用户的“辅助操作请求键处理”程序。当用户按“辅助操作请求”键时，他们会看到“操作辅助”（ASSIST）菜单。如果您的应用程序已经使用不同的“辅助操作请求键处理”程序，则应该为用户提供另一种方法来到达“操作辅助”菜单:
  - 通过使用 `GO ASSIST` 或 `CALL QEZAST`，从主应用程序菜单将“操作辅助”菜单添加为一个选项。
  - 让用户从命令行输入 `GO ASSIST`。

如果在用户概要文件中将**限制能力**字段设置为 *YES，则用户不能使用 GO 命令来显示菜单。需要提供一种方法以便“操作辅助”用户访问 ASSIST 菜单。

您可能要查看 Sharon Jones 为 JKL Toy 公司的“用户组描述”表单选择了什么值的示例。

要完成这些计划步骤，应该:

- 为公司中的每个组完成一个“用户组描述”表单。
- 在“命名约定”表单中描述如何命名用户组。
- 将用户组添加至应用程序和库的图表。

在完成了这些任务之后，可以开始计划单个用户概要文件。

示例: JKL Toy 公司的用户组描述表单 — 第二部分

当 Sharon Jones 准备“销售及市场”人员的“用户组描述”表单时，她记下了有关“销售及市场”和“仓库”部门的一些内容。

- 销售及市场人员将是“IBM Query iSeries 版”的主要用户。每个用户都应具有专用库。仓库可以具有一组库。
- 在装运码头工作的仓库人员将需要初始程序，而不是需要初始菜单。

Sharon 为两个部门准备了“用户组描述”表单的“第二部分”。

表 24. JKL Toy 公司的“用户组描述”表单: “销售及市场”部门示例

字段名称	建议值	您的选择
组概要文件名称（用户）		DSTSM
密码	*NONE	*NONE
用户类（用户类型）	*USER	*USER
当前库（缺省库）	*与组概要文件名称相同*	（在组中留下空白，对单个概要文件填写）
要调用的初始程序（注册程序）		
初始程序库		
初始菜单（第一个菜单）		CPMAIN
初始菜单库		CPMAINLIB
限制能力（限制命令行使用）	*YES	*PARTIAL
文本（用户描述）		销售及市场
作业描述	*与组概要文件名称相同*	DPTSM
作业描述库		QGPL
组概要文件名称（用户组）	*NONE[1]	*NONE
打印设备（缺省打印机）		PRT03
输出队列	*DEV	*DEV

表 25. JKL Toy 公司的“用户组描述”表单: 仓库部门示例

字段名称	建议值	您的选择
组概要文件名称（用户）		DPTWH
密码	*NONE	*NONE

表 25. JKL Toy 公司的“用户组描述”表单: 仓库部门示例 (续)

字段名称	建议值	您的选择
用户类（用户类型）	*USER	*USER
特殊环境		
当前库（缺省库）	*与组概要文件名称相同*	DPTWH
要调用的初始程序（注册程序）		
初始程序库		
初始菜单（第一个菜单）		ICMAIN
初始菜单库		ICPGMLIB
限制能力（限制命令行使用）	*YES	*YES
文本（用户描述）		仓库部门
作业描述	*与组概要文件名称相同*	DPTWH
作业描述库		QGPL
组概要文件名称（用户组）	*NONE[1]	*NONE
打印设备（缺省打印机）		PRT04
输出队列	*DEV	*DEV
1 对于组概要文件，组概要文件名称必须是 *NONE。组概要文件不能是其它组的成员。		

现在，您可以开始计划单个用户概要文件。

计划单个用户概要文件

既然在整体安全性策略中已作出决定且已计划用户组，您就随时可以计划单个用户概要文件。

需要什么表单?

使用以下表单来计划单个用户概要文件:

- “单个用户概要文件”表单
- “系统责任”表单

还将需要使用以下已完成的表单中的信息:

- “用户组定义”表单
- “命名约定”表单
- 应用程序图表

命名用户概要文件

您的用户概要文件名称是如何对系统标识您。应在“注册”屏幕的**用户标识**字段中输入您的用户概要文件名称。您所做任何工作和创建的打印机输出与您的用户概要文件名称关联。

当决定如何命名用户概要文件时，考虑以下事项:

- 用户概要文件名称最长可以为 10 个字符。一些通信方法将用户标识限制为 8 个字符。

- 用户概要文件名称可以包括字母、数字和特殊字符: # 符号、$ 符号、下划线和 @ 符号。它不可以数字或下划线（_）开始。
- 系统不区分用户概要文件名称中的大写和小写字母。如果输入小写字母字符，则系统将它们转换为大写字符。
- 用来管理用户概要文件的屏幕和列表按用户概要文件名称的字母顺序显示用户概要文件。
- IBM 提供的所有概要文件以字母 Q 开始。要将您的概要文件与 IBM 提供的概要文件区分开，避免指定以字母 Q 开始的用户概要文件名称。

建议

指定用户概要文件名称的一种技术是使用姓的前 7 个字符并后跟名字的第一个字符。以下是 Sharon 在 JKL Toy 公司用于用户概要文件的命名约定:

表 26. JKL Toy 公司的“命名约定”表单: “用户概要文件”示例

用户名	用户概要文件名称
Anderson, George	ANDERSOG
Anderson, Roger	ANDERSOR
Jones, Sharon	JONESS

此方法使用户概要文件名称容易记住。而且，按姓的字母顺序排序列表和屏幕。

例如，JKL Toy 公司的 Sharon Jones 计划使用此命名技术。她填写了“命名约定”表单的适当部分。

表 27. JKL Toy 公司的“命名约定”表单: “用户概要文件”示例

对象类型	命名约定
用户概要文件	使用用户姓的前 7 个字符，并后跟用户名字的第一个字符。用户概要文件的描述将是“姓，名字”。

描述如何计划在“命名约定”表单中命名用户概要文件，然后您可以确定谁应该负责系统功能并为每个用户选择值。

确定谁应该负责系统功能

当计划单个用户概要文件时，必须首先确定系统上个人的责任。要保持系统有效操作，需要人们定期执行各种管理和维护功能。执行这些任务的人需要运行命令并执行系统功能的权限。

选择限制用户可以执行什么操作的值讨论了**用户类**和**限制能力**字段如何控制用户可以访问的系统功能。通常，不应该允许大多数用户执行系统功能（将用户类设置为 *USER 并将限制能力设置为 *PARTIAL 或 *YES）。然而，某些用户需要附加权限来保持系统有效操作。

下表列示一些重要的系统管理任务。它还指示可以为具有那些责任的人指定的用户类和特权。此列表帮助您确定系统上的哪些用户需要特权。然而，它并不打算作为一个完整的计划工具用于操作和维护系统。此表提供使用大多数系统的用户类和特权。您可能需要根据您的系统指定不同的权限。

当在概要文件中指定 *USER 以外的用户类时，用户自动接收一组确定的特权来执行系统功能。可以给用户指定不同于您在用户类字段中指定的那些特权的特权，但这可能是不必要的。

表 28. 系统责任、用户类和特权

系统功能[1]	描述	所需用户类 [2]	所需特权 [3]
系统操作	管理打印机输出、响应系统消息、监控正常操作和执行初始程序装入（IPL）。	*SYSOPR	*JOBCTL
系统内务处理	执行系统内务处理功能，如建立自动清除调度和监控磁盘使用情况。	*SYSOPR	*JOBCTL
系统备份	定期保存应用程序库、系统库和安全性信息。有关这些功能的详细信息，参见“信息中心”的备份与恢复主题。	*SYSOPR	*SAVSYS
概要文件管理	添加新的用户概要文件，维护现有的概要文件。	*SECADM	*SECADM
资源安全性管理	维护系统上的对象的权限。	*SECOFR	*ALLOBJ
程序维护	对 IBM 提供的库应用定期程序更改（PTF）。对应用程序库进行更改。	*SECOFR	*ALLOBJ
安全性审计	设置安全性审计功能。确定应该审计哪些事件、用户和对象。		*AUDIT [4]
系统配置	从系统添加、更改和除去设备。		*IOSYSCFG[5]

1 对于具有这些责任的用户，将“限制能力”字段设置为 *NO。

2 这是需要的最小用户类。用户类提供权限以使用执行功能所必需的命令和菜单选项。取决于资源安全性，还可能需要附加对象权限。

3 此特定的特权对于作业责任是必需的。用户类可给出附加特权。

4 *AUDIT 特权不具有对应的用户类。*SECOFR 用户类包括 *AUDIT 特权。然而，审计员可能不需要 *SECOFR 用户类的其它能力。应该为需要在系统上控制审计的每一单个用户指定 *AUDIT 特权。

5 *IOSYSCFG 特权不具有对应的用户类。*SECOFR 用户类包括 *IOSYSCFG 特权。只应该为需要配置系统的个人指定 *IOSYSCFG 特权。个人可以创建线路、控制器和设备或配置 TCP/IP。然而，配置系统的用户可能不需要 *SECOFR 用户类的其它能力。

建议

使用以上表来计划谁应该执行系统功能。至少应该指定两个人来管理系统安全性，而指定另外两个人来管理操作和备份。

使用“系统责任”表单作为管理和审计系统的工具。跟踪系统中具有特权的每个人以及他们需要该特权的原因。

在您为每个用户选择值之前，可能要查看 Sharon Jones 如何确定用户责任的示例。

示例: JKL Toy 公司的系统责任表单

以下是 Sharon Jones 完成的“系统责任表单”的示例:

表 29. JKL Toy 公司的“系统责任表单”：示例

谁是您的主要安全主管？Sharon Jones 谁是您的后备安全主管？Ken Harrison			
概要文件名称	用户名称	类	注释
JONESS	Sharon Jones	*SECOFR	Sharon 是主要安全主管和系统管理员。
HARRISOK	Ken Harrison	*SECOFR	Ken 是 Sharon 作为整个系统管理员的后备人员。
JOHNSONS	Sandy Johnson	*SYSOPR	Sandy 对系统操作和备份负主要责任。
ROGERSK	Karen Rogers	*SYSOPR	Karen 将帮助 Sandy 执行操作和系统备份。
WILLISR	Rose Willis	*SYSOPR	第二次换班期间，Rose 将操作系统。

在完成“系统责任”表单之后，可以开始为每个用户选择值。

为每个用户选择值

在确定了系统上用户的责任之后，可以开始为每个用户选择值。通过计划组概要文件作为单个用户概要文件的模式，已完成了大部分工作。使用“单个用户概要文件”表单来将每个用户指定给正确组并定义用户如何与组中的其它用户不同。您应该为一个用户组完成“单个用户概要文件”表单作为一个示例，然后返回并为任何附加用户组准备“单个用户概要文件”表单。

在“单个用户概要文件”表单的顶部填写组概要文件名称和其它描述性信息。

示例：JKL Toy 公司的“单个用户概要文件”表单的描述性信息

此处是 Sharon Jones 如何填写“单个用户概要文件”表单的顶部。

表 30. JKL Toy 公司的“单个用户概要文件”表单：“描述性信息”示例

“单个用户概要文件”表单		
准备人：Sharon Jones		日期：99/5/9
组概要文件名称：DPTOP		
创建的对象的所有者：	对创建的对象的组权限：	
组权限类型：		

确定组成员的值

在“单个用户概要文件”表单中写下概要文件名称和组的每个成员的描述（用户名称）。以下段落描述如何确定每个组成员的其它值。

记住，组概要文件是单个用户概要文件的模式。在“单个用户概要文件”表单中，只需要指定与组不同的内容。

- **指定密码**：为用户指定初始密码最容易的方法是使密码与概要文件名称相同。然后可以通过将密码设置为到期来要求用户在首次注册时更改密码。在主题将密码设置为到期中，了解当复制组概要文件时如何自动执行此操作。如果计划这样做，则不需要在“单个用户概要文件”表单中列示密码。

- **用户类和限制能力**: 检查“系统责任”表单来查看每个组的哪些成员对**用户类**和**限制能力**字段需要不同的值。对于需要不同于组概要文件的值的任何人，在“单个用户概要文件”表单中填写适当的信息。
- **指定其它值**: 检查特定用户是否需要不同于在组的“用户组描述”表单中指定的值。在“用户组描述”表单中，在顶部列示**用户类**和**限制能力**字段，因为对于组的某些成员它们的值可能会经常不同。列示对于正在使用的组的成员改变的任何其它字段。

要完成此计划步骤，确保:

- 完成“系统值选择”表单。
- 描述如何在“命名约定”表单中计划命名用户概要文件。
- 为公司中的每个用户组准备“单个用户概要文件”表单。

在计划资源安全性之前，您可能要查看 Sharon 用于单个用户的信息的示例

示例: JKL Toy 公司的单个用户概要文件表单

在 JKL Toy 公司，在装运码头工作的人仅可以运行一个程序。Sharon 将这些用户限制于少数几个功能，因为他们在公众可以轻易地访问其工作站的区域工作。“仓库”部门的这些成员具有初始程序但不具有初始菜单。“订单处理”部门具有两个本地打印机和一个远程销售办公室的打印机。因此，Sharon 对某些用户指定与组不相同的打印机。

以下是 Sharon Jones 为 JKL Toy 公司的“仓库和订单处理部门”完成的“单个用户概要文件”表单。注意，仅当字段与组概要文件中设置的值不同时，她才填写字段。

表 31. JKL Toy 公司的“单个用户概要文件”表单: “仓库部门”示例

组概要文件名称: DPTWH					
对组的每个成员生成一项:					
用户概要文件	**文本（描述）**	**用户类**	**限制能力**	**初始程序 / 库**	**初始菜单 / 库**
WILLISR	Willis, Rose	*SYSOPR	*NO		
WAGNERR	Wagner, Ray			ICRCPT/ICPGMLIB	无
AMESJ	Ames, Janice			ICRCPT/ICPGMLIB	无
FOSSJ	Foss, Julie				
WOODBURC	Woodburt, Carol				

表 32. “单个用户概要文件”表单: “订单处理部门”示例

组概要文件名称: DPTOP				
对组的每个成员生成一项:				
用户概要文件	**文本（描述）**	**用户类**	**限制能力**	**打印设备**
HARRISOK	Harrison, Ken	*SECOFR	*NO	PRT05
RICHARDK	Richards, Karen			
UNGERJ	Unger, Jeff			PRT04
BELLB	Bell, Brad			PRT04

下一步，可以开始计划资源安全性。

第 5 章 计划资源安全性

既然已完成了计划系统上用户的过程，就可以计划保护系统上对象的资源安全性。在“设置资源安全性”中，了解如何设置系统上的资源安全性。

系统值和用户概要文件控制谁对您的系统具有访问权并防止未授权用户注册。资源安全性控制已授权的系统用户在成功注册之后可以执行的操作。资源安全性支持您系统上的安全性的主要目标以保护下列各项:

- 信息的机密性
- 信息的准确性，以防止未授权更改
- 信息的可用性，以防止意外或故意损坏

可以不同方式计划资源安全性，这取决于是您的公司开发应用程序还是购买它们。对于开发的应用程序，在应用程序设计过程期间，应该将对信息的安全性的要求通知程序员。当购买应用程序时，需要确定您的安全性要求，并将那些要求与您的供应商设计您的应用程序的方式匹配。此处描述的技术应该在两种情况下帮助您。

本主题提供计划资源安全性的基本方法。它介绍主要技术并显示如何可以使用它们。此处所描述的方法将不必对每个公司和每个应用程序有效。当计划资源安全性时，咨询您的程序员或应用程序供应商。

查看这些主题以帮助您计划资源安全性:

- 确定您的资源安全性的目标
- 了解权限类型
- 计划应用程序库的安全性
- 确定库和对象的所有权
- 将对象分组
- 保护打印机输出
- 保护工作站
- 资源安全性建议摘要
- 计划您的应用程序安装

需要什么表单?

复制几份以下表单并在阅读本主题时填写它们。对一个应用程序完成整个过程，然后对每个附加应用程序重复该过程。

表 33. 计划资源安全性所需要的计划表单

表单名称	需要的份数
权限列表表单	几份
打印机输出和工作站安全性表单	一份

将信息添加至以下表单，先前您已使用它们:

表 34. 计划将要更改的表单

表单名称	准备
库描述表单	描述库信息
用户组描述表单	计划组概要文件

参考以下表单，先前已准备它们:

表 35. 计划完成资源安全性所需要的表单

表单名称	准备:
“库描述”表单	绘制应用程序图和标识用户组
应用程序描述表单	描述应用程序信息
单个用户概要文件表单	为每个用户选择值
用户组标识表单	标识用户组
系统责任表单	确定谁应该负责系统功能
物理安全性计划表单	计划物理安全性

确定您的资源安全性的目标

要开始计划资源安全性，您必须首先了解您的目标。iSeries 提供了灵活的资源安全性实现。它给予您以想要的方式来保护关键资源的能力。但是，资源安全性还对应用程序引入附加开销。 例如，无论何时应用程序需要一个对象时，系统必须检查用户对该对象的权限。您必须在性能成本和您的机密性需要之间进行权衡。当您作出资源安全性决定时，针对安全性的成本衡量安全性的值。

要防止资源安全性降低您的应用程序的性能，遵循以下准则。

- 使您的资源安全性方案简单。
- 仅保护那些您需要保护的对象。
- 使用资源安全性来补充（而不是代替）其它工具以保护信息，如:
  - 将用户限制于特定菜单和应用程序。
  - 防止用户输入命令（在用户概要文件中的限制能力）。

通过定义您的目标来开始您的资源安全性计划。您可以在应用程序描述表单或库描述表单中定义您的安全性目标。

您使用的表单取决于在库中如何组织您的信息。

在查看您可以用于资源安全性的权限类型之前，您可能要查看 JKL Toy 公司的安全性目标的示例。

示例: JKL Toy 公司的安全性目标

JKL Toy 公司的 Sharon Jones 使用“库描述”表单来描述“客户记录库”（CUSTLIB）的安全性需求。

表 36. JKL Toy 公司的“库描述”表单: 安全性目标示例

“库描述”表单	第一部分（共两部分）

表 36. JKL Toy 公司的“库描述”表单: 安全性目标示例 (续)

为库定义安全性目标，如是否有信息是机密的:	现在，允许公司中的每个雇员查看客户信息和客户订单。要保护信息的准确性，应该控制允许更改它的人。

Sharon 对“合同及定价”应用程序使用了“应用程序描述”表单来描述整个应用程序的安全性目标。

表 37. JKL Toy 公司的“应用程序描述”表单: 安全性目标示例

“应用程序描述”表单	第一部分（共两部分）
为库定义安全性目标，如是否有信息是机密的:	有关合同和特殊定价的信息是机密的。只有少数人才有权查看并更改它: • 销售及市场人员以及所有经理都需要创建、更改并分析合同。他们需要使用文件和程序。 • “订单处理”人员在输入和交付订单时可以间接更改合同和查看价格。除非在他们输入或更改订单时，否则不允许他们查看合同和价格。

在“应用程序描述”表单或“库描述”表单上编写应用程序的安全性目标。然后，您可以查看您可以用来计划资源安全性的权限类型。

了解权限类型

在您确定了资源安全性的目标并在“库描述”表单中记录了您的决定之后，就可以开始计划权限类型。资源安全性定义用户如何获取系统上的对象的访问权。

权限指授权某人如何使用对象。例如，您可以具有在系统上查看信息或更改信息的权限。系统提供几种不同的权限类型。IBM 将这些权限类型分组为几个类别（称为**系统定义的权限**），它们满足大多数人的需要。下表列示这些类别并说明如何应用它们来保护文件和程序。

注: 当您计划权限时，参考下面的表。

表 38. 系统定义的权限

权限名称	允许对文件执行的操作	不允许对文件执行的操作	允许对程序执行的操作	不允许对程序执行的操作
*USE	查看文件中的信息。	更改或删除文件中的任何信息。删除文件。	运行程序。	更改或删除程序。
*CHANGE	查看、更改和删除文件中的记录。	删除或清除整个文件。	更改程序的描述。	更改或删除程序。
*ALL	创建和删除文件。添加、更改和删除文件中的记录。授权其他人使用文件。	无	创建、更改和删除程序。授权其他人使用程序。	更改程序的所有者（如果程序沿用权限）。
*EXCLUDE[1]	无	对文件的任何访问。	无	对程序的任何访问。

表 38. 系统定义的权限 (续)

权限名称	允许对文件执行的操作	不允许对文件执行的操作	允许对程序执行的操作	不允许对程序执行的操作
1 *EXCLUDE 覆盖您对公众授予的或通过组概要文件授予的任何权限。				

了解对象权限和库权限如何一起工作

要设计简单的资源安全性，尝试计划整个库的安全性。为此，需要了解如何将系统定义的权限应用于库，如下表所示:

表 39. 库的系统定义权限

权限名称	允许的操作	不允许的操作
*USE	• 对于库中的对象，对于特定对象该权限允许的任何操作。 • 对于库，查看描述信息。	• 将新对象添加至库。 • 更改库描述。 • 删除库。
*CHANGE	• 对于库中的对象，对于特定对象该权限允许的任何操作。 • 将新对象添加至库。 • 更改库描述。	• 删除库。
*ALL	• 对于更改允许的所有操作。 • 删除库。 • 授权其他人使用库。	• 无

您还需要了解库和对象权限如何一起工作。下表给出对于对象和库都是必需的权限的示例:

表 40. 库权限和对象权限如何一起工作

对象类型	操作	需要的对象权限	需要的库权限
文件	更改数据	*CHANGE	*USE
文件	删除文件	*ALL	*USE
文件	创建文件	*ALL	*CHANGE
程序	运行程序	*USE	*USE
程序	更改（重新编译）程序	*ALL	*CHANGE
程序	删除程序	*ALL	*USE

目录权限与库权限类似。需要对象的路径名称中所有目录的权限才能访问该对象。

现在您随时可以计划应用程序库的安全性。

计划应用程序库的安全性

在您确定了资源安全性的目标之后，就可以开始计划应用程序库的安全性。当您执行此处所描述的过程时，选择要使用的应用程序库之一。如果系统将文件和程序存储在单独的库中，则选择包含文件的库。当您完成该主题时，对其余的应用程序库重复这些步骤。

查看您收集的关于应用程序和库的信息:

- “应用程序描述”表单
- “库描述”表单
- 需要库的任何组的“用户组描述”表单
- 应用程序、库和用户组的图表

考虑库中哪些组需要该信息，它们为什么需要它以及要用它作什么。

确定库的内容

应用程序库包含重要的应用程序文件。它们还包含其它对象，其中大多数是使应用程序正确工作的编程工具，如:

- 工作文件
- 数据区域和消息队列
- 程序
- 消息文件
- 命令
- 输出队列

除文件和输出队列以外的大多数对象不表示安全性暴露。它们通常包含少量应用程序数据，经常以在程序外不易于理解的格式表示。通过使用“显示库”命令可以列示库中所有对象的名称和描述。例如，要列示 CONTRACTS 库的内容: `DSPLIB LIB(CONTRACTS) OUTPUT(*PRINT)`

接着，需要决定您想对应用程序库和程序库具有哪种公共权限。

决定对应用程序库的公共权限

为了资源安全性，**公众**指您授权注册至您系统的任何人。如果用户不具有任何其它更具体的访问权，则**公共权限**允许用户访问对象。除了决定已在库中的对象的公共权限外，还可以指定以后添加至库的任何新对象的公共权限。为此，使用**创建权限（CRTAUT）**参数。通常，库对象的公共权限和新对象的库创建权限应该相同。

QCRTAUT（创建权限）系统值确定新对象的系统范围内的公共权限。IBM 用 *CHANGE 交付 QCRTAUT 系统值。避免更改 QCRTAUT，因为许多系统功能使用它。如果为应用程序库的“创建权限”（CRTAUT）指定 *SYSVAL，则它使用 QCRTAUT 系统值（*CHANGE）。

为了简单化和更好的性能，尽可能多使用公共权限。要确定库的公共权限应该是什么权限，询问以下问题:

- 公司中的每个人应该具有对此库中大部分信息的访问权吗？
- 人们应该具有对此库中大部分信息的哪种访问权？

集中作出对于大多数人和大部分信息的决定。稍后，您将了解如何处理例外情况。计划资源安全性经常是一个循环过程。您可能会发现，在考虑特定对象的需求之后需要对公共权限作出更改。尝试对象和库的公共和专用权限的几种组合之后，然后才选择满足您的安全性和性能需要的一种组合。

确保足够的权限

对于大多数应用程序功能，对对象的 *CHANGE 权限和对库的 *USE 权限是足够的。然而，您需要询问您的程序员或应用程序供应商某些问题，以确定某些应用程序功能是否需要更多权限:

- 在处理期间删除库中的任何文件或其它对象吗？清除任何文件吗？将成员添加至任何文件吗？删除对象、清除文件或添加文件成员需要对象的 *ALL 权限。
- 在处理期间在库中创建任何文件或其它对象吗？创建对象需要库的 *CHANGE 权限。

在决定程序库的公共权限之前，您可能要查看 Sharon 对于对象的权限所作出的选择的示例。

示例: JKL Toy 公司的库描述表单

Sharon Jones 查看“客户记录”库的安全性目标以及关于使用客户信息的应用程序和部门的信息。她记下了她的结论:

- 除仓库和制造部门以外的每个部门都需要更改客户信息。
- 仓库和制造部门中的所有用户都拥有具有“限制能力”（是）的用户概要文件，他们被限于某些菜单或程序。他们的菜单允许他们查看客户信息，但不能更改信息。
- “客户记录”库中对象的公共权限可以设置为 *CHANGE。菜单限制防止未授权的人员更改客户信息。然而，如果稍后将其它部门添加到系统，则应该再次评估此信息。

这是获取信息的不严格方法的示例。在此情况下，通过用户概要文件而不是使用权限限制来处理异常。Sharon 填写“客户记录”库（CUSTLIB）的“库描述”表单的公共权限部分。

表 41. JKL Toy 公司“库描述”表单 — 第一部分: “客户记录”示例

库名称: CUSTLIB	描述性名称（文本）: 客户记录
库的公共权限:	*USE
库中对象的公共权限:	*CHANGE
新对象的公共权限（CRTAUT）:	*CHANGE

Sharon Jones 发现，在“应收帐款”应用程序的月底处理期间，清除了“客户记录”库中的某些临时文件。她选择单独地处理这些文件的权限，而不是冒可能意外地删除库中其它对象的风险。对于所有其它处理活动，*CHANGE 权限是足够的。

即使仅少数人员运行月底处理，Sharon 也认为临时文件不会造成任何安全性风险。她决定给公众授予对这些文件的 *ALL 权限，而不是仅将该权限授予运行月底处理的人。下表显示“客户记录”库的“库描述”表单的“第二部分”:

表 42. JKL Toy 公司的“库描述”表单 — 第二部分: “客户记录”示例

列示库对象的特定权限

表 42. JKL Toy 公司的“库描述”表单 — 第二部分: “客户记录”示例 (续)

组概要文件或用户概要文件	对象名称	对象类型	所需权限	权限列表
PUBLIC	ARFILE01	*FILE	*ALL	
PUBLIC	ARFILE02	*FILE	*ALL	
PUBLIC	ARFILE03	*FILE	*ALL	

现在可以决定对您需要的程序库的公共权限。

决定对程序库的公共权限

通常，将应用程序保存在与文件和其它对象不同的单独的库中。不要求您对应用程序使用单独的库，但许多程序员在他们设计应用程序时使用此技术。如果您的应用程序具有单独的程序库，则您需要决定那些库的公共权限。您可以同时使用库和库中程序的 *USE 权限来充分运行程序，但程序库可能具有需要附加权限的其它对象。询问您的程序员几个问题:

- 应用程序使用数据区域或消息队列在程序之间通信吗？它们在程序库中吗？对象的 *CHANGE 权限对于处理数据区域和消息队列是必需的。
- 在处理期间删除程序库中的任何对象（如数据区域）吗？需要对象的 *ALL 权限以删除该对象。
- 在处理期间创建程序库中的任何对象（如数据区域）吗？需要对象的 *CHANGE 权限以在库中创建任何新对象。

在“库描述”表单的两部分中填写所有资源安全性信息，而库所有者和权限列表栏除外。然后可以确定库和对象的所有权。

您可能要查看 Sharon Jones 如何确定对程序库的权限的以下两个示例。在第一个示例中，Sharon 决定非限制性的方法很适合“客户订单”程序库。第二个示例显示 Sharon 用于“应收帐款”程序库的更具限制性的方法。

示例: JKL Toy 公司的库描述表单 — 非限制方法

Sharon Jones 调查了“客户订单程序”库，并记下了以下内容:

- 一个消息队列（COMSGQ01）用于在程序之间通信。
- 已清除该消息队列，但从不删除它。对该消息队列的 *CHANGE 权限是足够的。

Sharon 决定将 *USE 权限授予程序库中的所有对象，并单独定义 COMSGQ01 消息队列。以下两个表显示用于 COPGMLIB 库的“库描述”表单。

表 43. JKL Toy 公司的“库描述”表单: 程序库示例

“库描述”表单	**第一部分（共两部分）**
库名称: COPGMLIB	描述性名称（文本）: 客户订单程序库
库的公共权限: *USE 库中对象的公共权限: *USE 新对象的公共权限（CRTAUT）: *USE 库所有者:	

表 44. JKL Toy 公司的“库描述”表单: 程序库示例

“库描述”表单				第二部分（共两部分）
列示库中单个对象的权限				
组概要文件或用户概要文件	对象名称	对象类型	所需权限	权限列表
PUBLIC	COMSGQ01	*MSGQ	*CHANGE	

使用对程序的权限来控制访问

尽管允许 JKL Toy 公司的大多数人更改客户信息，但仅允许少数人设置客户的信用限制。信用限制存储在客户主文件（CUSTMAS）中，但使用 ARPGMLIB 中称为 ARPGM12 的单独程序更改它们。Sharon 可以限制该程序以防止未授权的人更改信用限制。下表显示 ARPGMLIB 的“库描述”表单:

表 45. JKL Toy 公司的“库描述”表单: 单个权限示例

“库描述”表单	第一部分（共两部分）
库名称: ARPGMLIB	描述性名称（文本）: 应收帐款程序库
库的公共权限: *USE 库中对象的公共权限: *USE 新对象的公共权限（CRTAUT）: *USE 库所有者:	

表 46. JKL Toy 公司的“库描述”表单: 单个权限示例

“库描述”表单				第二部分（共两部分）
列示库中单个对象的权限				
组概要文件或用户概要文件	对象名称	对象类型	所需权限	权限列表
PUBLIC	ARPGM12	*PGM	*EXCLUDE	
JACOBS	ARPGM12	*PGM	*USE	
DAVISP	ARPGM12	*PGM	*USE	
SMITHJ	ARPGM12	*PGM	*USE	

在开始确定库和对象的所有权之前，您可能要查看使用沿用权限的限制性示例。

示例: JKL Toy 公司的库描述表单 — 限制方法

示例迄今为止显示了不严格的安全性方法，在这种方法中，大多数人可以访问库中的信息。JKL Toy 公司的合同及定价信息被认为是机密的，需要限制方法。幸运地，此信息全部存储在一个单独的库中。更新合同及定价的程序也在一个特殊库中。

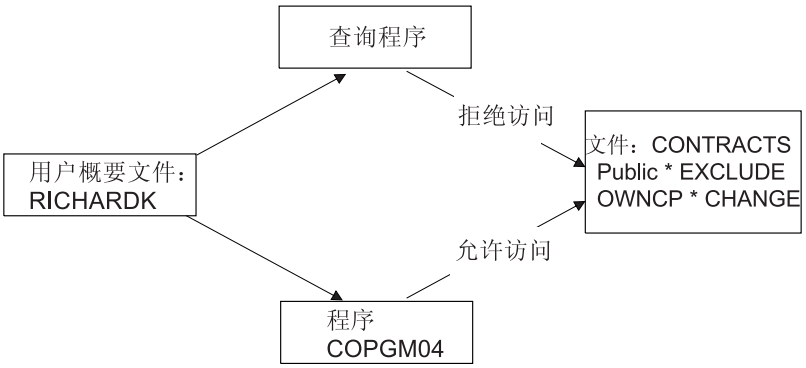
Sharon 查看“合同及定价”应用程序的安全性目标（参见确定资源安全性的目标）。她也查看了“应用程序描述”表单和“库描述”表单。Sharon 感到要达到应用程序的安全性目标将比较困难。她记下了一些内容并与应用程序供应商讨论了该问题:

- “销售及市场”人员和经理需要创建和更改合同。他们需要使用文件和程序。

- “订单处理”人员在输入和交付订单时间接更改合同并查看价格，但不允许他们以任何其它方式查看合同和价格。然而，他们将使用“查询”来创建自己的有关客户和订单的报表。如果他们被授予对“合同及定价”文件的权限，他们可以创建“查询”程序来查看或打印这些文件。

JKL Toy 公司的应用程序供应商建议使用安全性的沿用权限功能部件来解决此问题。**沿用权限**允许用户在程序运行时沿用程序所有者的权限。用户不需要对对象的权限。

以下图表显示沿用权限如何工作的示例。在“订单处理”部门中的 Karen Richards（RICHARDK）通常无权使用“合同”文件。然而，当她输入订单时，她必须检查并更新合同余额。使用合同余额的订单输入程序（COPGM04）沿用 OWNCP 概要文件的权限。当 Karen 运行 COPGM04 程序时，她有权使用合同文件:



OWNCP 的沿用权限

有关对象所有权的详细信息，参见主题“确定库和对象的所有权”。应用程序供应商或程序员可以指定当创建（编绎）程序时程序沿用所有者的权限，或程序员可以使用“更改程序”（CHGPGM）命令指定程序的沿用权限。使用此技术之前，确保了解程序的所有功能。

Sharon 决定使用沿用权限功能来授予“销售及市场”部门外面的人对“合同及定价”文件的访问权。她也确定对于由“合同及定价”应用程序使用的所有对象，*CHANGE 访问权是足够的。下表显示“合同”库的“库描述”表单:

表 47. JKL Toy 公司的“库描述”表单: 限制性权限示例

“库描述”表单	**第一部分（共两部分）**
库名称: CONTRACTS	描述性名称（文本）: 合同及定价库
库的公共权限: *EXCLUDE 库中对象的公共权限: *CHANGE 新对象的公共权限（CRTAUT）: *CHANGE 库所有者:	

表 48. JKL Toy 公司的“库描述”表单: 限制性权限示例

“库描述”表单	**第二部分（共两部分）**
列示库中单个对象的权限	

表 48. JKL Toy 公司的“库描述”表单: 限制性权限示例 (续)

组概要文件或用户概要文件	对象名称	对象类型	所需权限	权限列表
DPTSM	CONTRACTS	*LIB	*USE	
DPTMG	CONTRACTS	*LIB	*USE	

您不需要限制库中对象的权限，因为您限制了对库本身的访问。同样，Sharon 对经理和“销售及市场”部门授予了权限。她使用组权限，而不是对部门中的每个单个用户授予权限。

注: 具有对库的访问权的有经验的程序员可能能够保留对库中对象的访问权，即使在您取消了库的权限之后也是如此。如果库包含具有较高安全性需求的对象，则限制对象和库以进行完整保护。

在开始确定库和对象的所有权之前，您可能要查看非限制的示例。

确定库和对象的所有权

在您计划应用程序库的安全性之后，您可以决定库和对象的所有权。创建时，指定每个对象一个所有者。对象的所有者自动具有对象的所有权限，这包括授权其他人使用对象、更改对象和删除对象。安全主管可以对系统上的任何对象执行这些功能。

系统使用对象所有者的概要文件来跟踪谁对于对象具有权限。系统在内部完成此功能。这可能不会直接影响用户概要文件。然而，如果您不正确计划对象所有权，某些用户概要文件会变得很大。

当系统保存对象时，系统也与它一起保存拥有的概要文件的名称。如果系统恢复对象，则系统使用此信息。如果恢复的对象拥有的概要文件不在系统上，则系统将所有权转移至 IBM 提供的称为 QDFTOWN 的概要文件。

建议

以下建议在许多（但不是所有）情况下都适用。查看建议之后，与您的程序员或应用程序供应商讨论您对于对象所有权的意见。如果您购买应用程序，则您可能不能控制什么概要文件拥有库和对象。应用程序可能设计成防止更改所有权。

- 避免将 IBM 提供的概要文件（如 QSECOFR 或 QPGMR）用作应用程序所有者。这些概要文件拥有 IBM 提供的库中的许多对象且已经很大。
- 通常，组概要文件不应该拥有应用程序。组中的每个成员与组概要文件具有相同的权限，除非您明确指定较低的权限。实际上，您将会给予组中每个成员对于应用程序的全部权限。
- 如果您计划将控制应用程序的责任委派给各部门的管理员，则那些管理员可以是所有应用程序对象的所有者。然而，应用程序的管理员可以更改责任。如果是这样，则您应将所有应用程序对象的所有权转移给新的管理员。
- 许多人使用将密码设置为 *NONE 为每个应用程序创建特殊所有者概要文件的技术。系统使用所有的概要文件来管理应用程序的权限。安全主管（或具有该权限的某个人）执行应用程序的实际管理或将它委派给对特定应用程序具有 *ALL 权限的管理员。

决定哪些概要文件应该拥有您的应用程序。在每个“库描述”表单中输入所有者概要文件信息。

在您开始决定用户库的所有权和访问权之前，您可能要查看 JKL Toy 公司如何确定应用程序所有权的示例。

示例: JKL Toy 公司的应用程序所有权

Sharon Jones 决定为每个应用程序创建一个特殊的所有者概要文件。她和 Ken Harrison（后备安全主管）将负责管理应用程序安全性。以后，如果公司安全性需求变得更复杂，Sharon 可以指定部门经理管理权限。

Sharon 将新项添加到她的“命名约定”表单:

表 49. JKL Toy 公司的“命名约定”表单: 所有者概要文件示例

对象类型	“命名”约定
所有者概要文件	将对每个应用程序创建所有者概要文件。它将拥有其中所有应用程序库和这些库中的对象。所有者概要文件将命名为 OWN 加上应用程序缩写。“库存控制”所有者概要文件将为 OWNIC。

Sharon 决定以 OWN 为所有者概要文件名称的开头，以便全部所有者概要文件一起出现在显示器和列表上。

Sharon 对所有应用程序库指定了所有者，并在“命名约定”表单上输入该信息。唯一具有多个可能应用程序所有者的库是“客户记录”库。因为“应收帐款”应用程序用于创建新客户和设置信用限制，Sharon 决定它应该拥有客户文件。她指定了以下所有者:

库名称	所有者名称
ICPGMLIB	OWNIC
ITEMLIB	OWNIC
CONTRACTS	OWNCP
CPPGMLIB	OWNCP
COPGMLIB	OWNCO
CUSTLIB	OWNAR
ARPGMLIB	OWNAR

您现在可以决定您的用户库的所有权和访问权。

决定用户库的所有权和访问权

如果您的系统具有“IBM Query iSeries 版”许可程序或另一个决定支持程序，则用户需要一个库，以用于存储他们创建的查询程序。通常，此库是用户概要文件中的**当前库**。有关为每个用户创建当前库的更多信息，参见“选择影响注册的值”。Sharon Jones 计划将当前库用于“销售及市场”部门而将组库用于其它部门:

- “销售及市场”人员将是“查询”的主要用户。每个用户都应具有专用库。否则，他们将不得不担心如何命名其查询，且他们可能会意外删除彼此的程序。
- 要启动，其它部门将具有组库。如果他们创建了许多“查询”程序，我们可以考虑单个的库。

如果用户属于一个组，则您可使用用户概要文件中的字段来指定是用户还是组拥有用户所创建的任何对象。如果用户拥有这些对象，则您可以指定组成员具有使用这些对象的什么权限。还可以指定组的权限是主组权限还是专用权限。主组权限可能会提供更好的系统性能。Sharon 记下一些关于用户库的附加内容:

- “销售及市场”人员应该拥有他们创建的对象，而不是让组拥有他们。他们不需要更改彼此的查询程序。
- 组中的每个人应能够运行彼此的“查询”程序，这意味着组获取对于组成员所创建的任何对象的 *USE 权限。
- 组的权限应该是主组权限。
- 公众不应该具有对这些库的访问权。“销售及市场”人员可以具有来自其查询的输出文件。那些文件可能包含机密数据。
- 对于其它部门，组将拥有组库以及库中创建的任何内容。这意味着组的任何成员可以更改或删除库中的任何内容。如果这会导致问题，则可能必须尝试另一方法。

下表显示使用用户拥有的对象的“销售及市场”部门的“单个用户概要文件表单”：

表 50. JKL Toy 公司的“单个用户概要文件表单”： “用户拥有的对象”示例

组概要文件名称: DPTSM	
创建的对象的所有者: *USRPRF	对创建的对象的组权限: *USE
组权限类型: *PGP	

下表显示具有组所拥有的对象的部门的“单个用户概要文件表单”：

表 51. JKL Toy 公司的“单个用户概要文件表单”： “组拥有的对象”示例

组概要文件名称: DPTxx	
创建的对象的所有者: *GRPPRF	对创建的对象的组权限:

如果创建的对象的所有者是组，则不使用**对创建的对象的组权限**字段。组成员对创建的任何对象自动具有 *ALL 权限。

决定谁应该拥有并可以访问用户库。在“单个用户概要文件”表单上的**创建的对象的所有者**和**对于对象的组权限**字段中输入您的选择。现在您随时可以开始将对象分组。

将对象分组

在确定了库和对象的关系之后，可以开始将系统上的对象分组。要简化管理权限，使用权限列表将具有相同需求的对象分组。然后可以将公共、组概要文件和用户概要文件权限给予权限列表而不是给予列表中的单个对象。系统将由权限列表保护的每个对象看作是相同的，但您可以对不同用户授予对整个列表的不同权限。

权限列表使得易于在恢复对象时重新建立权限。如果用权限列表保护对象，则恢复进程自动将对象链接至列表。

可以对组或用户授予管理权限列表的权限（*AUTLMGT）。权限列表管理允许用户从列表添加和除去其它用户以及更改那些用户的权限。

建议

- 对需要安全性保护并具有类似安全性需求的对象使用权限列表。使用权限列表促使您考虑权限的类别而不是单个权限。权限列表还使得易于在系统上恢复对象和审计权限。
- 避免使用将权限列表、组权限和单个权限组合在一起的复杂方案。选择最符合要求的方法，而不是同时使用所有方法。

还需要将权限列表的命名约定添加至“命名约定”表单。

一旦准备了“权限列表”表单，就返回并将该信息添加至“库描述”表单。程序员或应用程序供应商可能已经创建了权限列表。确保与他们一起检查。

在计划打印机和打印机输出的安全性之前，您会发现查看 JKL Toy 公司的 Sharon Jones 如何计划权限列表的示例很有用。

示例: JKL Toy 公司的权限列表表单

Sharon 查看“客户记录”库的“库描述”，并决定为每个月底清除的文件创建权限列表。即使仅清除三个文件，Sharon 仍决定使用权限列表来简化对权限的管理。如果稍后将其它文件添加到月底进程，她就可以简单地用权限列表来保护这些文件。Sharon 决定排除文件的公共权限来避免在月底处理期间发生无意的问题。她仅对运行处理的用户授予 *ALL 权限。Rose Willis 是晚间系统操作员，可能需要查看有关文件的信息来检查月底处理。她需要 *USE 权限。

下表显示 Sharon 用于权限列表的命名约定:

表 52. JKL Toy 公司的“命名约定”表单: “权限列表”示例

“命名约定”表单	
准备人: Sharon Jones	日期: 99/5/9
对象类型	**命名约定**
权限列表	对于保护来自一个库的对象的列表，使用库名的一部分加上 LST 和一个数字。CUSTLIB 中对象的列表是 CUSTLST1。对于保护来自多个库的对象的列表，使用应用程序缩写，如果可能的话，使用 ARLST1。如果列表应用于多个应用程序，选择任何有意义的名称。列表描述应表明它的主要目的。

下表显示 CUSTLIB 库的“权限列表”表单。Sharon 使用来自“库描述”表单的信息准备此表单:

表 53. JKL Toy 公司的权限列表计划: 示例

“权限列表”表单					
权限列表名称: CUSTLST1					
描述: 月底处理期间清除的文件。					
列示列表所保护的对象					
对象名称	对象类型	对象库	对象名称	对象类型	对象库
ARFILE01	*FILE	CUSTLIB	ARFFILE02	*FILE	CUSTLIB
ARFILE03	*FILE	CUSTLIB			
列示可以访问该列表的组和用户					
组或用户	允许的访问类型	列表管理？	组或用户	允许的访问类型	列表管理？
PUBLIC	*EXCLUDE	否	ROSSG	*ALL	否

表 53. JKL Toy 公司的权限列表计划: 示例 (续)

SMITHJ	*ALL	否	JONESS	*ALL	是
WILLISR	*USE	否			

Sharon 也将权限列表信息添加到 CUSTLIB 库的“库描述”表单:

“库描述”表单				第二部分（共两部分）
准备人: Sharon Jones			日期: 9/9/99	
库名称: CUSTLIB				
列示库对象的特定权限				
组概要文件或用户概要文件	对象名称	对象类型	所需权限	权限列表
PUBLIC	ARFILE01	*FILE	*AUTL	CUSTLST1
PUBLIC	ARFILE02	*FILE	*AUTL	CUSTLST1
PUBLIC	ARFILE03	*FILE	*AUTL	CUSTLST1

注意，必须将每个文件的公共权限更改为 *AUTL，以便系统使用权限列表来确定公共权限。

查看“库描述”表单上的组和单个权限。决定使用权限列表是否合适。如果合适，则准备“权限列表”表单并用权限列表信息更新“库描述”表单。然后，可以计划打印机和打印机输出的安全性。

计划打印机和打印机输出的安全性

在将对象分组之后，需要计划如何保护打印机输出。您已制订保护系统上存储的信息的计划。您还需要一个计划在机密信息正在打印或正等待打印时保护机密信息。检查公司用于机密输出的打印机的“物理安全性计划”。

当运行打印报表的程序时，报表通常不直接转至打印机。程序创建报表的副本，称为**假脱机文件**或**打印机输出**。在打印机可用之前，系统将假脱机文件存储在称为**输出队列**的对象中。当输出队列包含打印机输出时，您可以在您的工作站上查看报表。也可以保留它或将它定向至特定打印机。

假脱机使得更易于调度打印作业和共享打印机。假脱机还帮助您保护机密输出。可以创建一个或多个保留机密输出的特殊输出队列并限制谁可以查看和管理那些输出队列。还可以控制何时将机密输出从队列发送至打印机。

当阅读完本主题时，完成“打印机输出和工作站安全性”表单。

当创建特殊输出队列时，可以指定几个与安全性有关的参数:

- **显示数据（DSPDTA）参数**: 输出队列的 DSPDTA 参数确定用户是否可以查看、发送或复制另一个用户拥有的假脱机文件。
- **检查权限（AUTCHK）参数**: 输出队列的 AUTCHK 参数确定用户是否可以更改或删除另一个用户拥有的假脱机文件。
- **操作员控制（OPRCTL）参数**: 输出队列的 OPRCTL 参数确定是否允许具有 *JOBCTL 特权（*SYSOPR 用户类）的用户控制输出队列。

输出队列参数、用户对输出队列的权限和用户的特权一起来确定用户对输出队列中的假脱机文件可以执行的功能。下表显示什么组合允许用户执行不同功能:

打印功能	输出队列参数			输出队列权限	特权
	DSPDTA	AUTCHK	OPRCTL		
将假脱机文件添加至队列 [1]	任何	任何	任何	*READ	无
	任何	任何	*Yes	任何	*JOBCTL
查看假脱机文件列表（WRKOUTQ 命令）[2]	任何	任何	任何	*READ	无
	任何	任何	*Yes	任何	*JOBCTL
显示、复制或发送假脱机文件（DSPSPLF、CPYSPFL、SNDNETSPLF 和 SNTCPSPLF）[2]	*YES	任何	任何	*READ	无
	*NO	*DTAAUT	任何	*CHANGE	无
	*NO	*OWNER	任何	所有者 [3]	无
	*YES	任何	*Yes	任何	*JOBCTL
	*NO	任何	*Yes	任何	*JOBCTL
	*OWNER[5]	任何	任何	任何	任何
更改、删除、保留、释放假脱机文件（CHGSPLFA、DLTSPLF、HLDSPLF 和 RLSSPLF）[2]	任何	*DTAAUT	任何	*CHANGE	无
	任何	*OWNER	任何	所有者 [3]	无
更改、清除、保留和释放输出队列（CHGOUTQ、CLROUTO、HLDOUTQ 和 RLSOUT）[2]	任何	*DTAAUT	任何	*CHANGE	无
	任何	*OWNER	任何	所有者 [3]	无
	任何	任何	*YES	任何	*JOBCTL
启动队列的写程序（STRPRTWTR 和 STRRMTWTR）[2]	任何	*DTAAUT	*Any	*CHANGE[4]	无
	任何	任何	*YES	任何[4]	*JOBCTL

1 这是将输出定向至输出队列所需要的权限。

2 从屏幕使用这些命令或相当选项。

3 您必须是输出队列的所有者。

4 也需要对打印机设备描述的 *USE 权限。

5 要使用此命令，您必须是假脱机文件的所有者或具有 *SPLCTL 特权。

查看“物理安全性计划”的打印机部分。当阅读完本主题时，填写“打印机输出和工作站安全性”表单的输出队列部分。

在计划工作站的资源安全性之前，您会发现查看 JKL Toy 公司的 Sharon Jones 如何确定这些输出队列参数的值的示例很有用。

示例: JKL Toy 公司的输出队列和工作站安全性表单 — 输出队列部分

JKL Toy 公司的“销售及市场部门”对机密打印有两个要求:

- 在计划价格更改时，打印初步价格列表。“销售及市场部门”外的任何人（公司经理除外）都不能查看此信息。

- 当协商合同时，合同是机密的。仅协商合同的人员才能查看合同的草稿，而“销售及市场部门”的其它成员则不能查看。

Sharon 决定创建两个特殊输出队列:

PRICEQ

将用于初步价格列表。“销售及市场部门”的任何人都可以对此输出队列执行任何功能。该部门以外的任何人都不可以使用此输出队列，包括系统操作员。PRICEQ 在 CONTRACTS 库中。

NEWCP

将用于打印正在协商的合同。“销售及市场部门”的成员共享该输出队列，但仅在输出队列上创建假脱机文件的人员才可以控制该文件。NEWCP 在 CONTRACTS 库中。

下表显示 Sharon 为这些输出队列准备的“输出队列和工作站安全性”表单:

表 54. JKL Toy 公司的“输出队列和工作站安全性”表单: “打印机输出队列”示例

列示受限制的输出队列的参数:				
输出队列名称	输出队列库	显示任何文件（DSPDTA）	检查权限（AUTCHK）	操作员控制（OPRCTL）
PRICEQ	CONTRACTS	*YES	*DTAAUT	*NO
NEWCP	CONTRACTS	*NO	*OWNER	*NO

主题决定对程序库的公共权限包含一个示例，该示例显示 JKL Toy 公司的 CONTRACTS 库的权限。仅经理和“销售及市场部门”的成员可以访问该库。库中对象（包括这些输出队列）的公共权限是 *CHANGE。

因为 NEWCP 输出队列上的 AUTCHK 参数是 *OWNER，所以仅假脱机文件的所有者才可以使用该文件（参见以上“执行打印功能所必需的权限”表）。这可以防止“销售及市场部门”的成员互相打印他们新合同或在输出队列中查看它们。

在计划打印机输出队列安全性之后，可以计划工作站的安全性。

计划工作站的安全性

在计划打印机和打印机输出的资源安全性之后，可以开始计划工作站安全性。在“物理安全性计划”中，您列示了由于其位置而产生安全性风险的工作站。使用此信息来确定需要限制哪些工作站。

可以促使使用这些工作站的人特别意识到安全性。无论何时离开工作站，他们都应该注销。对于安全性策略中易受攻击的工作站，您可能要记录关于注销过程的决定。还可以限制在那些工作站上可以执行哪些功能来最小化风险。

在工作站上限制功能的最容易的方法是将该功能限制于具有限制功能的用户概要文件。Sharon Jones 对 JKL Toy 公司的“仓库部门”使用了此技术。Sharon 允许在装运码头工作的 Ray Wagner 和 Janice Ames 仅运行库存接收程序。并且 Sharon 使他们成为允许注册到装运码头上的工作站的唯一用户。

可以选择防止具有安全主管或服务权限的用户在每个工作站注册。如果使用 QLMTSECOFR 系统值执行此操作，则具有安全主管权限的人只能在特定授权的工作站上注册。

准备“输出队列和工作站安全性”表单的工作站部分

当准备“输出队列和工作站安全性”表单的工作站部分时，可能要查看关于 Sharon 如何计划工作站的安全性的示例。还应该查看资源安全性建议列表，以确保资源安全性计划简单且完整。在查看示例和建议之后，可以开始计划应用程序安装。

示例: JKL Toy 公司的输出队列和工作站安全性表单 — 工作站部分

Sharon Jones 查看她的“物理安全性计划”来确定哪个工作站造成了安全性风险。例如，在 JKL Toy 公司，公司外部的人可以容易地访问装运码头和远程营业部上的工作站。Sharon 在“物理安全性计划”中指示这些工作站会造成潜在的安全性风险。

工作站上限制功能的最容易的方法是将该功能限制于具有限制功能的用户概要文件。Sharon Jones 对 JKL Toy 公司的“仓库部门”使用了此技术。Sharon 允许在装运码头工作的 Ray Wagner 和 Janice Ames 仅运行库存接收程序。并且 Sharon 使他们成为允许注册到装运码头上的工作站的唯一用户。

Sharon 重新评估她对 QLMTSECOFR 系统值的选择。她决定将它设置为 1（是）作为装运码头和远程营业部上的易受攻击的工作站的附加保护。

下表显示 Sharon 准备的“输出队列和工作站安全性”表单的工作站部分。

表 55. JKL Toy 公司的“输出队列和工作站安全性”表单: “工作站”示例

安全主管工作站: 如果您将安全主管限制于特定工作站（系统值 QLMTSECOFR 为是），则以下列示对安全主管和任何具有 *ALLOBJ 权限的人授权的工作站: 除以下所列示的以外的所有工作站。	
以下列示受限制的工作站的权限:	
工作站名称	授权（*CHANGE 权限）的组或用户
DSP10	AMESJ, WAGNERR
DSP11	AMESJ, WAGNERR
RMT01	UNGERJ, BELLB
RMT02	UNGERJ, BELLB

在计划应用程序安装之前，您可能要查看资源安全性建议的摘要。

资源安全性建议摘要

完成计划工作站安全性之后，可以查看下列资源安全性建议。iSeries 系统提供用于保护系统上的信息的许多选项。这就给了您为公司设计最好的资源安全性计划的灵活性。但大量的选项也可以使您混乱。

使用 JKL Toy 公司作为一个示例，本主题已尝试演示使用以下准则的计划资源安全性的基本方法:

- 从一般到特定:
  - 计划库的安全性。仅在必要时处理单个对象。
  - 首先计划公共权限，然后计划组权限和单个权限。

- 要提高性能并简化备份和恢复，仅定义使用公共权限不能满足其安全性需求的对象的特定安全性。
- 使库中新对象的公共权限（CRTAUT）与为库中大多数现有对象定义的公共权限相同。
- 尝试不要对组或个人授予比公众具有的权限少的权限。这会降低性能，以后会导致错误并使审计困难。如果知道每个人至少对对象具有公众具有的相同权限，则它使得更易于计划和审计安全性。
- 使用权限列表来将具有相同安全性需求的对象分组。权限列表比单个权限管理简单且有助于恢复安全性信息。
- 创建特殊用户概要文件作为应用程序所有者。将所有者密码设置为 *NONE。
- 避免 IBM 提供的概要文件（如 QSECOFR 或 QPGMR）拥有应用程序。
- 对于机密报表，使用特殊输出队列。将输出队列放在与机密信息相同的库中。
- 限制具有安全主管权限的人数。
- 当授予对对象或库的 *ALL 权限时，要小心。具有 *ALL 权限的人可以意外删除某些内容。

要确保已成功计划设置资源安全性，您应该收集了下列信息:

- 填写所有应用程序库的“库描述”表单的“第一部分”和“第二部分”。
- 在“单个用户概要文件”表单中，填写**创建的对象的所有者**和**对于创建的对象的组权限**字段。
- 在“命名约定”表单中描述如何计划命名权限列表。
- 准备“权限列表”表单。
- 将权限列表信息添加至“库描述”表单。
- 准备“输出队列和工作站安全性”表单。

现在可以准备计划应用程序安装。

计划您的应用程序安装

要完成计划资源安全性，需要准备应用程序安装。以下主题将帮助您在安装您的应用程序之后计划对您的应用程序的所有权和权限。此处描述的方法可能并非对所有应用程序都有效。咨询您的程序员或应用程序供应商以获取制订好的安装计划的帮助。

如果计划从应用程序供应商获取应用程序，则使用此信息来计划在装入应用程序库前后需要执行的安全性活动。

如果计划安装程序员在您自己的系统上开发的应用程序，则使用此信息来计划将应用程序从测试移动到生产状态所需要的安全性活动。

对一个应用程序完成这些步骤。然后返回并为任何附加应用程序准备“应用程序安装”表单。

需要哪些表单?

复制下列表单并在完成本主题时填写它:

表 56. 计划应用程序安装所需要的计划表单

表单名称	需要的份数
“应用程序安装”表单	每个应用程序一份

使用这些表单（先前已完成的）来收集用于计划应用程序安装的信息:

表单名称	准备:
“库描述”表单	描述库信息
“权限列表”表单	将对象分组

在主题装入应用程序中，您了解到如何执行安装应用程序所需要的步骤。

要计划应用程序安装，参见以下主题:

- 确定应用程序的用户概要文件和安装值
- 更改安装值。

确定应用程序的用户概要文件和安装值

当计划应用程序安装时，必须首先决定每个应用程序的用户概要文件和安装值。在另一个系统上安装已创建的应用程序之前，可能需要创建一个或多个用户概要文件。在系统上装入应用程序库之前，拥有应用程序库和对象的用户概要文件应该存在于系统上。在“应用程序安装”表单中记录需要为每个库创建的概要文件以及概要文件需要的参数。

要确定必要的安装值，询问您的程序员或应用程序供应商以下问题并在“应用程序安装”表单中记录他们的回答:

- 哪个概要文件拥有应用程序库？
- 哪个概要文件拥有库中的对象？
- 什么是库的公共权限（AUT）？
- 什么是新对象的公共权限（CRTAUT）？
- 什么是库中对象的公共权限？
- 哪些程序（如果有的话）沿用所有者的权限？

查明您的程序员或应用程序供应商是否创建了应用程序的任何权限列表。为每个已创建的权限列表准备“权限列表”表单或询问您的程序员有关该列表的信息。

可以确定是否应该更改任何安装值。

更改应用程序的安装值

将“应用程序安装”表单中的信息与“库描述”表单中的库的资源安全性计划比较。如果它们不同，则需要决定安装应用程序之后要做的更改。

更改应用程序所有权

如果您的程序员或应用程序供应商已创建拥有应用程序库和对象的特殊概要文件，则即使该概要文件与您的命名约定不匹配，也考虑使用该概要文件。转移对象的所有权会花费较长时间，应该避免。

如果 IBM 提供的组概要文件之一（如 QSECOFR 或 QPGMR）拥有应用程序，则在安装应用程序之后，应该将所有权转移到另一个概要文件。

有时，程序员设计应用程序来防止对象所有权的更改。尝试在限制范围内工作而仍满足您自己管理安全性的要求。然而，如果 IBM 提供的概要文件（如 QSECOFR）拥有应用程序，则您和您的程序员或应用程序供应商需要制订更改所有权的计划。理想情况下，您应该在安装应用程序之前更改所有权。

更改公共权限

当保存对象时，也将其公共权限与它们保存在一起。当将应用程序库恢复到系统时，库及其所有对象都将具有保存它们时所具有的相同公共权限。即使在另一个系统上保存库也同样如此。

库的 CRTAUT 值（新对象的公共权限）不影响恢复的对象。用已保存的公共权限恢复它们，而不管库的 CRTAUT。

应该更改库和对象的公共权限以便与“库描述”表单中的计划匹配。

当计划您的应用程序安装时，您可能要查看显示 JKL Toy 公司的 Sharon Jones 如何计划应用程序安装的示例。

要确保已完全计划您的应用程序安装，您应该:

- 完成填写您的初始“应用程序安装”表单。然后返回并为每个附加应用程序准备表单。
- 查看所有表单并确保它们完整。在安装了您的系统和许可程序之前，复制表单并将它们保存在安全位置。

完成这些计划任务之后，可以随时设置用户安全性。

示例: JKL Toy 公司应用程序安装表单

JKL Toy 公司从应用程序供应商购买了他们的“客户订单和应收帐款”应用程序。他们雇佣了一个外面的程序员来开发他们的“合同及定价”应用程序，并将该程序链接到“客户订单”应用程序。

Sharon Jones 使用她的“库描述”表单中的信息来准备“应用程序安装”表单。下表显示 Sharon 的 CUSTLIB“库描述”表单的副本: （参见主题“描述库信息。”）

表 57. JKL Toy 公司的“库描述”表单: 示例

“库描述”表单	第一部分（共两部分）
准备人: Sharon Jones	日期: 9/9/99
库名称: CUSTLIB	描述名称（文本）: 客户记录库
简要描述此库的功能: 容纳所有客户文件，包括订单和帐户。	
为库定义安全性目标，如是否有信息是机密的: 现在，允许公司的每个人查看客户订单。要保护信息的准确性，应该限制允许更改它的人。	

表 57. JKL Toy 公司的“库描述”表单: 示例 (续)

库的公共权限: *USE
库中对象的公共权限: *CHANGE
新对象的公共权限（CRTAUT）: *CHANGE
库所有者: OWNAR

下表显示 Sharon 为“客户订单”应用程序准备的“应用程序安装”表单。注意，Sharon 决定使用由应用程序供应商创建的所有者概要文件。概要文件 COWNER 将拥有文件和程序库。

在安装应用程序之后，Sharon 应执行下列操作:

- 将库的公共权限更改为与她的“库描述”表单上的资源安全性计划匹配。
- 将 COWNER 概要文件的用户类更改为 *USER，并除去任何特权。
- 将 COWNER 概要文件的密码更改为 *NONE。

表 58. JKL Toy 公司的“应用程序安装”表单: 示例

应用程序名称: 客户订单（CO）		描述: 输入、跟踪和交付订单。
列示并解释安装应用程序必须创建的任何概要文件: 称为 COWNER 的概要文件拥有包含文件的库。QPGMR 拥有程序库。		
库名称: CUSTLIB		
	安装之前	**安装之后**
库所有者	COWNER	COWNER
对象所有者	COWNER	COWNER
库公共权限	*EXCLUDE	*USE
对象公共权限	*ALL	*CHANGE
新对象的公共权限	*CHANGE	*CHANGE
库名称: COPGMLIB		
	安装之前	**安装之后**
库所有者	QPGMR	COWNER
对象所有者	QPGMR	COWNER
库公共权限	*EXCLUDE	*USE
对象公共权限	*ALL	*CHANGE
新对象的公共权限	*CHANGE	*CHANGE

既然您已完成计划任务，下一步准备设置用户安全性。

第 6 章 设置用户安全性

通过使用命令行界面，本主题指导您完成设置系统上的用户安全性所需要的任务。如果正在设置新的系统，则应该按顺序完成这些步骤。当继续执行下一步骤时，系统使用每个步骤的信息。要设置基本系统安全性，需要完成两组任务。必须首先定义用户安全性，然后，其次必须保护系统上的资源。以下两个表突出显示设置用户和资源安全性必须配置的每个步骤。

注：在开始设置资源安全性之前，**必须**首先完成设置用户安全性的所有步骤。

表 59. 设置用户安全性的步骤

步骤	在此步骤中执行的操作	使用的表单
设置整体环境	设置初始系统值和网络属性。创建安全主管用户概要文件。	“系统值选择”表单
设置安全性的系统值	设置附加系统值。	“系统值选择”表单
准备用于装入应用程序的基本安全性步骤	创建所有者概要文件。装入应用程序。完成其余步骤之前，应用程序库和对象应该位于系统上。	“应用程序安装”表单
设置用户组	创建作业描述、组库和组概要文件。	“用户组描述”表单
设置单个用户	创建单个库和用户概要文件。	“单个用户概要文件”表单

表 60. 设置资源安全性的步骤

步骤	在此步骤中执行的操作	使用的表单
设置所有权和公共权限	建立库和对象的所有权和公共权限。	“应用程序安装”表单
创建权限列表	创建权限列表。	“权限列表”表单
设置特定权限	设置对库和单个对象的访问权。	“库描述”表单
保护打印机输出	通过创建输出队列并指定输出来保护打印机输出。	“输出队列和工作站安全性”表单
保护工作站	保护工作站。	“输出队列和工作站安全性”表单

除上表中所列示的主题外，参见用于管理系统安全性的下列主题:

- 测试安全性。
- 更改安全性信息。
- 保存安全性信息。
- 监控安全性。

在开始之前

如果正在安装新系统，则在开始设置安全性之前，执行以下操作:

- 确保系统部件和设备安装和工作正常。如果不计划对您的设备使用 iSeries 命名，则等待到更改了确定如何命名设备的系统值（QDEVNAMING）之后连接您的工作站和打印机。应用新的系统值告诉您何时连接设备。
- 装入计划使用的任何许可程序。

设置整体环境

要开始设置用户安全性，需要为用户设置整体环境。在本主题中，使用“设置”菜单来设置系统值，并创建您自己的用户概要文件。还将更改“专用服务工具”（DST）概要文件的用户标识和密码。

在以下过程中，您将会找到说明这些步骤的示例命令行屏幕。然而，它们并不显示整个屏幕。它们仅显示完成任务所需要的信息。

需要哪些表单?

输入在“计划整体安全性策略”中准备的“系统值选择”表单中的信息。

要设置整体环境，需要完成下列任务:

1. 注册到系统。
2. 选择正确的辅助级别。
3. 防止其它用户注册。
4. 输入安全性的系统值。
5. 应用新的系统值。
6. 创建安全主管概要文件

完成以上步骤之后，必须更改“服务工具”密码，以防止某些人不正确地使用它们。有关详细信息，参见服务工具。

注册到系统

要开始设置系统环境，需要注册到系统。

1. 在控制台上，作为安全主管（QSECOFR）注册。如果您是第一次注册，则使用密码 QSECOFR。因为系统将此密码交付为已到期，所以系统将提示您更改此密码。必须更改此密码才能成功地注册。
2. 在“注册”屏幕上的*菜单*字段中输入 SETUP。

注: “设置”菜单称为“定制您的系统、用户和设备”菜单。本文本全部将它称为“设置”菜单。

```
                    注册
                                  系统  . . . . . .
                                  子系统  . . . . .
                                  屏幕  . . . . . .

用户  . . . . . . . . . . . . . .  QSECOFR
密码  . . . . . . . . . . . . . .  __________
程序 / 过程  . . . . . . . . . . .  __________
菜单  . . . . . . . . . . . . . .  SETUP
当前库  . . . . . . . . . . . . .  __________
```

在注册到系统上之后，必须选择适当的辅助级别。

选择正确的辅助级别

在注册到系统之后，可以为用户选择适当的辅助级别。**辅助级别**确定您看到屏幕的哪个版本。许多系统屏幕有两个不同的版本:

- 基本辅助级别版本，它包含较少信息并且不使用技术术语。
- 中间辅助级别版本，它显示更多信息并使用技术术语。

某些字段或功能仅在特定版本的屏幕上可用。指示信息告诉您使用哪个版本。要从一个辅助级别更改为另一个，使用 **F21**（选择辅助级别）。**F21** 并非从所有屏幕都可用。

选择辅助级别之后，必须在您设置安全性时防止其它用户注册到系统上。

防止其它用户注册

在选择正确的辅助级别之后，必须防止别的任何用户注册到系统上。如果担心人们在您有机会保护系统之前干预系统，则可以防止任何用户在其它工作站注册。这是可选的。仅当您感觉到临时安全性有必要时，才执行此操作:

1. 从“设置”菜单中，按 **F9** 来显示命令行。
2. 在命令行中，输入 GO DEVICESTS。
3. 屏幕显示“设备状态任务”菜单。如果看到“使用配置状态”菜单，使用 **F21**（选择辅助级别）来更改为基本辅助级别。
4. 选择选项 **1**（使用显示设备）。
5. 在“使用显示设备”屏幕中，使除正使用的工作站以外的所有工作站不可用。通过在每个工作站名称前面输入 **2** 并按**执行**键来完成此操作。
6. 通过按 **F3**（退出）两次返回到“设置”菜单。
7. 按 **F12**（取消）除去命令行。

```
                              使用显示设备

输入以下选项，然后按执行键。
  1=使可用              2=使不可用            5=显示
  7=显示消息            8=使用控制器和线路
  13=更改描述

Opt  设备         类型     状态
__   DSP01        3196     QSECOFR
2_   DSP02        3196     可使用
2_   DSP03        3196     可使用
2_   DSP04        3196     可使用
```

当使设备不可用时，即使打开它，它也不具有“注册”屏幕。仅当停止并再次启动系统之后，工作站才可用。可能需要重复此步骤。

在防止别的任何用户注册到系统上之后，可以输入安全性的系统值。

输入安全性的系统值

在已防止其它用户注册之后，需要将系统值输入到系统中。

使用以下过程来输入“系统值选择”表单的“第一部分”中的信息:

1. 从“设置”菜单，选择 **1**（更改系统选项）。
2. 在“更改系统选项”屏幕上输入“系统值选择”中的信息。如果不想更改屏幕上的选项之一，可以使用 Tab 键跳过它。
3. 如果启动系统时未设置日期与时间，则在此屏幕上输入正确的日期与时间。

4. 在此页面上输入信息之后，向下翻页到下一页。屏幕右下角的*尚有...* 指屏幕至少多于一页。

```
                              更改系统选项
系统:
输入以下选项，然后按执行键。
系统名称 . . . . . .  JKLTOY      名称

日期与时间选项:
  系统日期  . . . . . .  09/21/99     MM/DD/YY
  系统时间  . . . . . .  10:52:57     HH:MM:SS
  日期分隔符  . . . . . .  1          1=/
                                      2=-
                                      3=.
                                      4=,
                                      5=空白
  日期格式  . . . . . .  MDY          YMD、MDY、DMY 和 JUL
  时间分隔符  . . . . . .  1          1=:
                                      2=.
                                      3=,
                                      4=空白


                                                          尚有...
F1=帮助    F3=退出    F5=刷新    F12=取消
```

5. 在屏幕的第二页输入您的选择并向下翻页。

```
                              更改系统选项

输入以下选项，然后按执行键。
安全性选项:
  安全级别  . . . . . .  40
    :
  允许安全主管
    注册到任何
    显示站  . . . . . .  N
```

6. 在屏幕的第三页上输入您的选择并按**执行**键。

```
                              更改系统选项

输入以下选项，然后按执行键。
设备选项:
  新设备的设备
    命名格式  . . . . . .  1


    缺省系统打印机  . . . . . .  PRT01

附加选项:
  注册时使用户处于
    S/36 环境中 . . . . . .  N
  保存有关已完成的
    打印机输出的
    作业记帐信息  . . . . . .  Y
```

7. 应该再次看到“设置”菜单。注意屏幕底部的消息: **已成功更改系统选项。需要进行 IPL**。

   注: 仅当更改了安全级别时，系统才需要进行 IPL。

在大多数系统任务主题末尾，将会发现一个描述可能的错误和恢复步骤的表。如果您的结果与所描述的那些结果不同，则使用这些表以获取辅助。这些表不可能预料到每个问题。表的用途是指导您解决问题，并使您更轻松地使用系统。

可能的错误	恢复
显示了“主”菜单。	您按了 **F3**（退出）或 **F12**（取消）。输入 GO SETUP 并再试。
看到另一个屏幕，如“更改清除选项”屏幕。	从“设置”菜单选择了错误的选项。按 **F3**（退出）返回到菜单并再试。
按**执行**键之后，再次显示“更改系统选项”屏幕。	查找屏幕底部的错误消息。可能输入了不允许的值。如果需要更多信息，记住使用 **F1**（帮助）。如果要系统将所有值恢复到您开始输入之前的值，使用 **F5**（刷新）。重试。
在屏幕上输入所有您的选择之前，按了**执行**键。	可以按需要多次使用此屏幕来更改系统值。从“设置”菜单选择选项 **1** 并输入第一次丢失的值。**注意：一旦系统可操作，如果不咨询程序员，就不要更改安全级别。并且，如果正在使用 iSeries Access 或正在与另一个计算机通信，则不要更改系统名称。**
按了**执行**键，而不是向下翻页。	再次从“设置”菜单选择选项 **1** 并向下翻页来显示第二个页面。输入您的选择并按**执行**键。

输入系统值之后，必须应用新的系统值。

应用新的系统值

在输入系统值之后，需要应用这些值的其中一些值。对系统值的大多数更改立即生效。然而，当更改系统上的安全级别时，在停止系统并再次启动它之后更改才生效。验证在“更改系统选项”屏幕上正确输入了所有值之后，可随时应用新的值。

注: 如果尚未将工作站连接到系统，则现在连接。当启动系统时，它自动使用在“更改系统选项”屏幕中选择的命名格式来配置那些设备。

使用下列过程停止系统并再次启动它。当系统启动时，在“更改系统选项”屏幕中输入的值生效。

1. 确保您已在控制台上注册且没有注册其它工作站。
2. 确保处理器部件上的密钥锁开关处于“正常”位置。
3. 从“设置”菜单，选择“打开和关闭任务”的选项。
4. 选择“立即关闭系统然后打开”选项。按**执行**键。
5. 系统显示要求您确认关机请求的屏幕。按 **F16**（确认）。

这使系统停止，然后再次自动启动。屏幕变为空白几分钟。然后应该再次看到“注册”屏幕。

应用新的系统值之后，必须在系统上为自己创建安全主管概要文件。

创建安全主管概要文件

系统上的**安全主管**是具有 *SECOFR 用户类或 *ALLOBJ 和 *SECADM 特权的任何用户。

从“更改系统选项”屏幕应用系统值之后，为您自己和备用安全主管创建用户概要文件。将来，当执行安全主管功能时，使用您的概要文件而不是使用 QSECOFR 概要文件。

1. 作为 QSECOFR 注册到系统并请求“设置”菜单。

   注意，所选择的系统名称出现在“注册”屏幕的右上角。

```
                    注册
                                   系统  . . . . . .
                                   子系统  . . . . .
                                   屏幕  . . . . . .

用户  . . . . . . . . . . . . . .  QSECOFR
密码  . . . . . . . . . . . . . .  _________
程序/过程  . . . . . . . . . . .  _________
菜单  . . . . . . . . . . . . . .  SETUP
当前库  . . . . . . . . . . . . .  _________
```

2. 从“设置”菜单，选择*使用用户登记*选项。“使用用户登记”屏幕列示当前在系统上的概要文件。

   注: 如果看到“使用用户概要文件”屏幕，按 **F21**（选择辅助级别）并更改为基本辅助级别。

3. 要创建新的概要文件，在 *Opt*（选项）列中输入 **1**（添加），在*用户*列中输入概要文件的名称。按**执行**键。

```
                          使用用户登记

输入以下选项，然后按执行键。
  1=添加    2=更改    3=复制    4=除去    5=显示

Opt      用户              描述
1        JONESS
         QDOC              文档用户概要文件
         QSECOFR           安全主管用户概要文件
```

4. 在“添加用户”屏幕上，给您自己指定一个密码。
5. 用您自己的适当信息填写样本屏幕中所显示的字段。
6. 向下翻页到屏幕的下一页。

```
                              添加用户

输入以下选项，然后按执行键。
用户  . . . . . .  JONESS
用户描述  . . . . . .  Jones, Sharon
密码  . . . . . .  secret
用户类型  . . . . . .  *SECOFR
用户组  . . . . . .  *NONE

限制命令行使用  _____
缺省库  . . . . . .
缺省打印机  . . . . . .  *WRKSTN
注册系统  . . . . . .  *NONE
库  . . . . . .

第一个菜单  . . . . . .
库  . . . . . .
```

7. 填写屏幕的第二页，并按**执行**键。
8. 检查“使用用户登记”屏幕底部的确认消息。
9. 按 **F3**（退出）返回到“设置”菜单。

```
                              添加用户

输入以下选项，然后按执行键。
辅助操作请求键程序  . . .  *SYSVAL
  库  . . . . . .
```

可能的错误	恢复
在输入所有字段的值之前，按了**执行**键。	从“使用用户登记”屏幕使用*更改*选项来更改刚才创建的概要文件。如果概要文件未出现在列表中，则按 **F5**（刷新）并向下翻页来查找它。

在为您自己创建安全主管概要文件之后，需要更改“服务工具”用户的用户标识和密码。参见“信息中心”中的服务工具主题。

设置安全性的系统值

在本主题中，使用“使用系统值”（WRKSYSVAL）命令来更改并显示系统值。

需要什么表单?

输入在“计划整体安全性策略”中准备的“系统值选择”表单中的信息。

要设置系统值，完成下列任务:

1. 更改安全性系统值。
2. 更改单个系统值。

注册到命令行界面

使用以下信息来注册到系统:

概要文件

您自己的概要文件（需要 *SECADM 和 *ALLOBJ 权限）

菜单 主菜单

注册后，可以开始更改安全性系统值。

更改安全性系统值

注册到系统之后，使用下列过程来输入出现在“系统值选择”表单的“第二部分”上的安全性系统值。

1. 在命令行上，输入 WRKSYSVAL *SEC 并按**执行**键。命令名称后面的 *SEC 意味着您仅要查看与安全性相关的系统值。
2. 在“使用系统值”屏幕上，在要更改的系统值的前面的*选项*列中，输入 **2**（更改）。如果要更改的系统值未出现在屏幕上，则向下翻页，直到找到它。

```
                          使用系统值

定位至 . . . . . .                  开始字符
按类型划分子集 . . . . .  *SEC       F4 显示列表

输入选项，按执行键。
  2=更改    5=显示

        系统
选项    值          类型        描述
        QINACTMSGQ  *SEC        不活动的作业消息队列
2       QLMTDEVSSN  *SEC        限制设备会话
        QLMTSECOFR  *SEC        限制安全主管设备
        QMAXSGNACN  *SEC        要对失败执行的操作
  ⋮
```

3. 输入您对系统值的选择，并按**执行**键。屏幕再次显示“使用系统值”屏幕。

```
                          更改系统值
系统值 . . . . . :    QLMTDEVSSN
描述 . . . . . :     限制设备会话


输入选项，按执行键。
  限制设备会话 . . . . . .  0          0=不限制
                                       1=限制
```

4. 检查屏幕底部的确认消息。

可能的错误	恢复
您看到的系统值与“使用系统值”屏幕的示例上显示的值不同。	忘记输入 *SEC。将屏幕顶部的*按类型划分子集*字段与样本屏幕进行比较。将光标移动到*按类型划分子集*字段。输入 *SEC 并按**执行**键。
系统未处理您的命令。您仍可以看到菜单。	检查屏幕底部的错误消息。可能输入了不正确的命令名称。重试。如果消息指出您未授权，则注销并使用具有安全主管权限的概要文件再次注册。

可能的错误	恢复
按**执行**键之后，“更改系统值”屏幕再次出现。	检查屏幕底部以获取错误消息。可能错误地输入了您的选择或选择了超出允许范围的值。使用 **F1**（帮助）以获取附加信息。
您看到菜单而不是看到“使用系统值”屏幕。	可能按了两次**执行**键。输入 WRKSYSVAL *SEC。
选择了您不要更改的系统值。	按 **F12**（取消）来返回到“使用系统值”屏幕。

*（星号）的含义?

您可能注意到，某些值在它们前面有星号（*）。系统使用星号来区分特殊值和常规值。例如，当您指定在用户概要文件上的密码是 *NONE 时，这意味着系统将不允许任何人使用该概要文件注册。如果将该密码指定为 NONE，则用户必须输入字符 NONE 作为密码。

在系统上设置安全性时，确保注意指示信息和表单上星号的使用。

更改安全性系统值之后，可以更改单个系统值。

更改单个系统值

在更改安全性系统值之后，可以更改单个系统值。

例如，“断开连接的作业超时时间间隔”（QDSCJOBITV）系统值没有被包括为安全性系统值。它没有出现在“使用系统值”屏幕的 *SEC 子集上。使用以下过程来更改 QDSCJOBITV 系统值或任何单个系统值:

1. 输入 WRKSYSVAL QDSCJOBITV 并按**执行**键。
2. 在“使用系统值”屏幕上，在 QDSCJOBITV 前面的*选项*列中，输入 **2**（更改）。
3. 输入对 QDSCJOBITV 的选择。
4. 检查确认消息。

```
                              更改系统值
系统值 . . . . . . . . . :   QDSCJOBITV
描述 . . . . . . . . . . :   断开连接的作业超时时间间隔


输入选项，按执行键。
  断开连接的作业超时时间间隔 ..... 300
```

列示安全性值

在输入“系统值选择”表单中的所有信息之后，可以打印所有安全性系统值的列表。输入 WRKSYSVAL *SEC OUTPUT(*PRINT)。用“系统值选择”表单归档列表的副本。无论何时更改安全性系统值，都要重新打印该列表。

在输入“系统值选择”表单中系统值的所有选择后，可以准备装入您的应用程序。

执行用于装入应用程序的安全性步骤

在设置系统值之后，可以准备装入应用程序。本主题包括将应用程序库装入系统的必要安全性步骤。在创建概要文件和其它安全性对象之后，“设置所有权和公共权限”和“设置资源安全性”显示如何建立应用程序的所有权和权限。

如果可能，在设置用户组和单个概要文件之前，应将应用程序库装入到系统。当创建作业描述和概要文件时，需要引用应用程序对象。

如果创建组和单个概要文件之前无法装入应用程序，则可能会接收到警告消息，如下所示:

- 当创建作业描述时，系统未找到初始库。
- 当创建概要文件时，系统未找到初始程序或菜单。

必须装入应用程序库之后，才能成功测试作业描述和概要文件。

使用您在“计划应用程序安装”中准备的“应用程序安装”表单。

要装入每个应用程序，完成下列任务:

1. 创建所有者概要文件。
2. 装入应用程序。

注册到系统

- 要创建所有者概要文件:

  概要文件

  您自己的概要文件（需要 *SECADM 权限）

  菜单 主菜单

- 要装入应用程序库:

  与应用程序供应商一起检查，以查看当装入应用程序库时，您应该以安全主管还是以应用程序所有者身份注册。

注册之后，可以为应用程序创建所有者概要文件。

创建所有者概要文件

在注册到系统之后，检查您的“应用程序安装计划”来查看是否需要在装入应用程序之前创建任何概要文件。要创建概要文件:

1. 输入 CRTUSRPRF（创建用户概要文件）并按 **F4**（提示）。
2. 在“创建用户概要文件”屏幕上，按程序员或应用程序供应商的指示填写字段。
3. 使用 **F10**（其余字段）并向下翻页来显示附加字段。

```
                        创建用户概要文件（CRTUSRPRF）

输入选项，按执行键。
用户概要文件 . . . . . >
用户密码 . . . . . .   *USRPRF
将密码设置为到期 . . . . . .   *NO
状态 . . . . . .   *ENABLED
用户类 . . . . . .   *USER
辅助级别 . . . . . .   *SYSVAL
当前库 . . . . . .   *CRTDFT
要调用的初始程序 . . . . . .   *NONE
  库 . . . . . .
初始菜单 . . . . . .   MAIN
  库 . . . . . .     *LIBL
限制能力 . . . . . .   *NO
文本‘描述’ . . . . . .   xxxxxx 的所有者
```

4. 检查屏幕底部以获取消息。

注: 创建组概要文件更详细地讨论了如何创建概要文件。

创建应用程序的所有者之后，可以开始装入应用程序。

装入应用程序

遵循应用程序供应商的指示信息以装入应用程序库。在“设置所有权和公共权限”中，了解设置应用程序的所有权和公共权限。

装入所有应用程序之后，可以设置用户组。

设置用户组

在执行用于装入应用程序的安全性步骤之后，可以设置用户组。将创建组库、作业描述和组概要文件。对一个用户组完成整个主题，然后返回，并对任何附加组重复步骤。样本屏幕显示 JKL Toy 公司的“销售及市场部门”和“仓库部门”的“用户组描述”表单中的信息。

使用在“计划用户组”中准备的“用户组描述”表单。

完成以下任务来设置用户组:

1. 为用户组创建库。
2. 创建作业描述。
3. 创建组概要文件。

注册到系统

概要文件
    您自己的概要文件（需要 *SECADM 权限）

菜单 主菜单

在注册后，可以为用户组创建库。

为组创建库

在注册到系统之后，您需要为用户组创建库。如果计划使组共享他们创建的对象（如“查询”程序）的库，则在创建组概要文件之前创建库:

1. 输入 CRTLIB（创建库）并按 **F4**（提示）。
2. 填写屏幕。库名称应该是组概要文件名称。
3. 按 **F10**（附加参数）。
4. 填写库和在库中创建的新对象的公共权限。
5. 按**执行**键。检查确认消息。

```
                              创建库

输入选项，按执行键。
库 . . . . . . . . . . . . . . . .   DPTWH
库类型 . . . . . . . . . . . . . .   *PROD
文本‘描述’ . . . . . . . . . . . .   仓库库

                           附加参数

权限 . . . . . . . . . . . . . . .   *USE
辅助存储池标识 . . . . . . . . . .   1
创建权限 . . . . . . . . . . . . .   *CHANGE
创建对象审计 . . . . . . . . . . .   *SYSVAL
```

可能的错误	恢复
输入库的描述之前，按了**执行**键。	输入 **CHGLIB** 并按 **F4**（提示）。在提示屏幕上输入库名称并按**执行**键。在“更改库”屏幕上输入描述。
给予库一个错误名称。	使用“重命名对象”（RNMOBJ）命令。

为组创建库之后，可以创建作业描述。

创建作业描述

在为组创建库之后，可以为每个组创建作业描述。

如果初始库列表所需要的库尚未在系统上，则当创建作业描述时，会接收到警告消息。

1. 输入 **CRTJOBD**（创建作业描述）并按 **F4**（提示）。
2. 填写以下字段:

   作业描述:
   与组概要文件名称相同。

   库名称:
   QGPL

   文本: 组描述
3. 按 **F10**（附加参数）。
4. 向下翻页到*初始库列表*字段。

```
                    创建作业描述

输入选项，按执行键。
作业描述 . . . . . . . . . . . . .   DPTSM
  库 . . . . . . . . . . . . . . .   QGPL
作业队列 . . . . . . . . . . . . .   QBATCH
  库 . . . . . . . . . . . . . . .     *LIBL
作业优先级（JOBQ 上）. . . . . . .   5
输出优先级（OUTQ 上）. . . . . . .   5
打印设备 . . . . . . . . . . . . .   *USRPRF
输出队列 . . . . . . . . . . . . .   *USRPRF
  库 . . . . . . . . . . . . . . .
文本‘描述’ . . . . . . . . . . .   销售及市场
```

5. 在*初始库列表*字段中的 *SYSVAL 上输入 **+**（加）来指定要输入值的列表。按**执行**键。

```
记帐代码 . . . . . . . . . . . . .   *USRPRF
   :
CL 语法检查 . . . . . . . . . . .   *NOCHK
初始库列表 . . . . . . . . . . . .   +
             + 以获取更多值
```

6. 在*初始库列表*字段中，输入“用户组描述”表单中已标记（✓）的库名称:
   - 每行放置一个库名称。
   - 包括 QGPL 和 QTEMP。每个作业都使用称为 QTEMP 的库来存储临时对象。**所有初始库列表必须具有 QTEMP 库**。对于多数应用程序，QGPL 库也应该在初始库列表上。
   - 您不必在库列表上包括当前（缺省）库。系统在注册时自动添加该库。
7. 按**执行**键。检查消息。（向下翻页来查看所有消息。）

```
指定更多值

输入选项，按执行键。
初始库列表 . . . . . . . . . . .   CUSTLIB
                                   ITEMLIB
                                   COPGMLIB
                                   ICPGMLIB
                                   QGPL
                                   QTEMP
```

可能的错误	恢复
按了**执行**键而不是 **F10**。	要将正确的库放置到初始库列表中，输入 **CHGJOBD**（更改作业描述）并按 **F4**。
当尝试创建作业描述时，获取了错误消息。	当尝试包括未在系统上的库时，会出现最常见的错误消息。这是警告消息。仍然对初始库列表中的库创建作业描述。直到库在系统上之后，您才能用指定该作业描述的概要文件注册。 如果库在系统上，您可能输入了不正确的名称。验证库名称并重试。

创建作业描述之后，可以创建组概要文件。

创建组概要文件

在创建作业描述之后，可以创建组概要文件。为此，使用“用户组描述”表单的“第二部分”中的信息。

1. 使用“使用用户概要文件”命令。输入 WRKUSRPRF *ALL。最初，屏幕列示由 IBM 提供的概要文件。

   注: 如果看到“使用用户登记”屏幕，则按 **F21** 来更改为中间辅助级别。

2. 要创建新的概要文件，在 *Opt*（选项）列中输入 **1**，在*用户概要文件*列中输入概要文件名称。按**执行**键。

```
                          使用用户概要文件

输入选项，按执行键。
  1=创建    2=更改    3=复制    4=删除    5=显示
  12=按所有者使用对象

      用户
Opt   概要文件     文本
1     DPTSM
      QDOC         文档用户概要文件
      QSECOFR      安全主管用户概要文件
```

3. 将“用户组描述”表单中的信息输入到适当字段。
4. 使用 **Tab** 键跳过要使用缺省值的任何字段。
5. 按 **F10**（附加参数）。
6. 向下翻页。

```
                    创建用户概要文件（CRTUSRPRF）

输入选项，按执行键。
用户概要文件 . . . . . > DPTSM
用户密码 . . . . . .   *none
将密码设置为到期 . . . . . .   *NO
状态 . . . . . .   *ENABLED
用户类 . . . . . .   *USER
辅助级别 . . . . . .   *SYSVAL
当前库 . . . . . .   *CRTDFT
要调用的初始程序 . . . . . .   cpsetup
  库 . . . . . .   cppgmlib
初始菜单 . . . . . .   cpmain
  库 . . . . . .   cppgmlib
限制能力 . . . . . .   *yes
文本 '描述' . . . . . .   销售及市场
```

7. 将“用户组描述”表单的剩余字段输入屏幕的附加页面上，并按**执行**键。

```
                        创建用户概要文件

                        附加参数

特权 . . . . . . . . . . . . . . .   *USRCLS

   :
作业描述 . . . . . . . . . . . . .   DPTSM
  库 . . . . . . . . . . . . . . .   QGPL
```

```
                        创建用户概要文件

组权限 . . . . . . . . . . . . . .   *NONE

   :
打印设备 . . . . . . . . . . . . .   PRT03
```

8. 检查消息。

记住

组概要文件只是一种特殊类型的用户概要文件。许多消息和屏幕将组概要文件称为用户或用户概要文件。仅当您将成员添加到组概要文件或对它指定组标识号（gid），系统才知道您创建了组概要文件。

可能的错误	恢复
在输入组概要文件的所有值之前，按**执行**键。	按 **F5**（刷新）来将创建的概要文件添加到“使用用户概要文件”屏幕。使用选项 **2**（更改）来更正概要文件。
用错误的名称创建了概要文件。	不能更改概要文件的名称。使用复制选项（**3**）来创建具有正确名称的新概要文件。然后删除（选项 **4**）具有错误名称的概要文件。
“用户组描述”表单的某些字段未出现在屏幕上。	确保正在使用中间辅助级别。“创建用户概要文件”的基本辅助级别版本称为“添加用户”屏幕。要更改辅助级别，按 **F12**（取消）返回到“使用用户登记”屏幕。使用 **F21** 来更改辅助级别。参见“选择正确的辅助级别”。
意外地从“创建用户概要文件”屏幕擦除了一些缺省信息。	如果使字段保持为空白，则当创建用户概要文件时，系统使用缺省值。如果要查看缺省值，按 **F5**（刷新）来恢复整个屏幕。重新输入信息。

列示结果

通过使用“显示已授权的用户”（DSPAUTUSR）命令，列示系统上所有概要文件的名称和描述。输入 DSPAUTUSR OUTPUT(*PRINT)。检查以确保所有组概要文件具有密码 *NONE。

在设置单个用户之前，完成下列操作:

- 为每个用户组创建作业描述。
- 可选择为每个组创建库。
- 为每个用户组创建组概要文件。

设置单个用户

当设置用户组时，已完成创建组概要文件的步骤。现在，为组的每个成员创建单个概要文件。

对一个用户组的成员完成整个主题，然后返回，并对任何附加组重复步骤。样本屏幕显示 Sharon Jones 为 JKL Toy 公司的“销售及市场部门”和“仓库部门”准备的“单个用户概要文件表单”中的用户。可以在“计划单个用户概要文件”中找到这些表单的副本。

使用在“计划单个用户概要文件”中准备的“单个用户概要文件”表单。

要为组的成员创建单个概要文件，完成下列任务:

1. 创建个人库。（可选）
2. 复制组概要文件。
3. 将密码设置为到期。
4. 创建附加用户。（可选）

   注: 重复创建个人库和创建附加用户，直到每个组成员都具有一个用户概要文件。
5. 如果有必要，更改关于用户的信息。
6. 显示结果。

注册到系统

概要文件

您自己的概要文件（需要 *SECADM 权限）

菜单 设置

创建个人库

要开始设置单个用户，您可能需要为对象（如“查询”程序）的每个成员创建个人库。在创建单个用户概要文件之前，创建个人库。

1. 输入 **CRTLIB** 并按 **F4**（提示）。
2. 给予库与用户概要文件相同的名称。
3. 按 **F10**（附加参数）。
4. 填写库和在库中创建的新对象的公共权限。
5. 按**执行**键。检查确认消息。

```
                              创建库

输入选项，按执行键。
库 . . . . . .  DPTSM
库类型 . . . . . .  *PROD
文本 '描述' . . . . . .  仓库库

                           附加参数

权限 . . . . . .  *EXCLUDE
辅助存储池标识 . . . . . .  1
创建权限 . . . . . .  *CHANGE
创建对象审计 . . . . . .  *SYSVAL
```

创建个人库之后，可以通过复制组概要文件来创建单个概要文件。

复制组概要文件

组概要文件有两个作用:

1. 系统使用它来确定组成员是否有权使用对象。
2. 可以将它作为模式来为单个组成员创建用户概要文件。

当您设置用户组时，已创建了组概要文件。现在，可以复制组概要文件来创建单个概要文件，并复制单个概要文件来创建组中其它的概要文件。

1. 从“设置”菜单选择“使用用户登记”选项。

   注: 如果看到“使用用户概要文件”屏幕，使用 **F21**（选择辅助级别）来更改为基本辅助级别。

2. 在用户组前面的 *Opt* 列中，输入 **3**（复制）。屏幕显示“复制用户”屏幕。（如果要复制的用户组未在屏幕上，则向下翻页，直到找到为止。）系统使用户名保持为空白，并根据您复制的组概要文件填写剩余字段。

```
                          使用用户登记

输入以下选项，然后按执行键。
  1=添加    2=更改    3=复制    4=除去    5=显示

Opt      用户          描述

         DPTSM         销售及市场部门
3        DPTWH         仓库部门
```

3. 输入正在创建的用户概要文件的名称和描述。
4. 让密码保持为空白。系统自动使密码与新用户概要文件名称相同。
5. 将组概要文件名称输入到*用户组*字段中。
6. 检查“单个用户概要文件”表单来查看此用户是否具有与组不同的其它值。输入这些值。
7. 向下翻页。

```
                                复制用户

从用户复制  . . . . . :   DPTWH

输入以下选项，然后按执行键。
用户  . . . . . .  .   WILLISR
用户描述. . . . . .  .   Willis, Rose
密码  . . . . . .  .
用户类型  . . . . . .   *SYSOPR
用户组  . . . . . .  .   DPTWH

限制命令行使用             N

缺省库  . . . . . .  .   DPTWH
缺省打印机  . . . . . .   PRT04
注册程序. . . . . .  .   *NONE
  库  . . . . . .  .
第一个菜单  . . . . . .   ICMAIN
  库  . . . . . .  .      ICPGMLIB
```

8. 在屏幕的下一页面上进行必要的更改，并按**执行**键。
9. 检查“使用用户登记”屏幕底部的确认消息。

```
                                复制用户

从用户复制  . . . . . :   DPTWH

输入以下选项，然后按执行键。
辅助操作请求键程序  . . .   *SYSVAL
  库  . . . . . .  .
```

可能的错误	恢复
您看到“创建用户概要文件”屏幕而不是“复制用户”屏幕。	使用 **F12**（取消）来返回到“使用用户概要文件”屏幕。使用 **F21** 来更改为基本辅助级别。再次启动复制操作。
您选择的用户概要文件名称将在用户提示中容纳不下。	尽管用户概要文件名称最多可以为 10 个字符，但“复制用户”和“添加用户”屏幕只支持少于 8 个字符的名称。选择更短的用户名称或使用中间辅助级别来创建单个用户概要文件。

测试用户概要文件

当在组中创建第一个单个概要文件时，您应该通过用该概要文件注册来测试它。验证您是否看到正确的第一个菜单和注册程序是否运行。

如果您用该概要文件无法成功注册，系统可能无法找到在概要文件中指定的某些内容。它可能是注册程序、作业描述或初始库列表中的一个库。使用“使用打印机输出”屏幕来查找当尝试注册时写入的作业记录。该作业记录会告诉您所发生的错误。

有关当进行安全性更改时测试和诊断问题的信息，参见“测试安全性”。

在测试用户概要文件之后，可以将密码设置为到期。

将密码设置为到期

将单个概要文件设置为要求用户在第一次注册时更改他们的密码。*将密码设置为到期*字段未出现在“复制用户”屏幕的基本辅助级别版本上。您需要在用复制功能创建用户概要文件之后，单独更改该字段。要更改*将密码设置为到期*字段，输入 CHGUSRPRF *profile-name* PWDEXP(*YES)。

注: 如果要通过用用户概要文件注册来测试用户概要文件，在将密码设置为到期之*前*执行测试。

可能的错误	恢复
测试了概要文件，并被强制更改密码。	输入 **CHGUSRPRF** *profile-name* 并按 **F4**（提示）。将密码重新设置为用户概要文件的名称。（将用户概要文件名称输入密码字段。）在*将密码设置为到期*字段中，输入 ***YES**。需要中间辅助级别才能执行此操作。

创建第一个单个用户概要文件之后，可以创建附加用户。

创建附加用户

在复制组概要文件来创建第一个单个概要文件之后，可以创建附加用户。复制第一个单个用户概要文件来创建组中的附加成员。当用复制方法创建单个概要文件时，仔细查看每个单个概要文件。检查“单个用户概要文件”表单并确保您更改的任何字段对于新用户概要文件是唯一的。

1. 在“使用用户登记”屏幕上，在您要复制的用户概要文件的前面输入 **3**（复制）。
2. 在“复制用户”屏幕上，输入概要文件名称和描述。
3. 将信息输入到对于新用户是唯一的任何字段中。

```
                          使用用户登记

输入以下选项，然后按执行键。
  1=添加    2=更改    3=复制    4=除去    5=显示

Opt      用户           描述

         DPTSM          销售及市场部门
         DPTWH          仓库部门
3        WILLISR        Willis, Rose
```

可能的错误	恢复
您要复制的概要文件未出现在“使用用户登记”屏幕上。	按 **F5**（刷新）。向上翻页和向下翻页。列表是按概要文件名称的字母顺序排列的。

如果要改变关于用户的信息，参见更改关于用户的信息。

更改关于用户的信息

对于某些用户，您可能需要设置未出现在“复制用户”屏幕上的值。例如，某些用户可以属于多个组概要文件。在通过使用复制方法创建用户概要文件之后，可以更改它。

1. 在“使用用户登记”屏幕上，按 **F21** 来更改为中间辅助级别。
2. 在“使用用户概要文件”屏幕上，在要更改的概要文件旁边的 *Opt*（选项）列中输入 **2**（更改）。按**执行**键。

```
                          使用用户概要文件

输入选项，按执行键。
  1=创建    2=更改    3=复制    4=删除    5=显示
  12=按所有者使用对象

     用户
Opt  概要文件    文本
2    AMESJ       Ames, Janice
     DPTSM       销售及市场部门
     QDOC        文档用户概要文件
     QSECOFR     安全主管用户概要文件
     WAGNERR     Wagner, Ray
     WILLISR     Willis, Rose
```

3. 在“更改用户概要文件”屏幕上，按 **F10**（附加参数）。
4. 往下翻页直到找到要更改的字段。例如，如果要使用户成为附加组概要文件的成员，向下翻页，直到找到*补充组*字段。
5. 输入您需要的值，并按**执行**键。接收确认消息，并再次看到“使用用户概要文件”屏幕。

```
                      更改用户概要文件（CHGUSRPRF）

输入选项，按执行键。
允许的最大存储量 . . . . . .   *NOMAX
最高调度优先级 . . . . . .   3
作业描述 . . . . . .   DPTWH
  库 . . . . . .     QGPL
组概要文件 . . . . . .   DPTWH
所有者 . . . . . .   *GRPPRF
组权限 . . . . . .   *USEE
组权限类型 . . . . . .   *PGP
补充组 . . . . . .   DPTIC
             + 以获取更多值
```

一旦更改了用户信息，可以显示结果来检查概要文件。

显示用户概要文件

有几种方法可用来显示您创建的概要文件。

显示一个概要文件

从“使用用户登记”屏幕或“使用用户概要文件”屏幕中使用选项 **5**（显示）。

列示一个概要文件

使用“显示用户概要文件”命令：DSPUSRPRF *profile-name* DETAIL(*BASIC) OUTPUT(*PRINT)。

显示组成员

输入 DSPUSRPRF *group-profile-name* *GRPMBR。可以使用 OUTPUT(*PRINT) 来打印列表。

列示所有概要文件

要按组排序列示所有概要文件的名称和描述，使用“显示已授权用户”命令：DSPAUTUSR SEQ(*GRPPRF) OUTPUT(*PRINT)。

在设置所有权和公共权限之前，确保完成以下任务：

- 完成创建所有单个用户概要文件。
- 对每个概要文件将密码设置为到期。
- 打印按组排序的所有概要文件的列表，并用“用户组描述”表单保存。当添加新用户时，再次打印该列表。

第 7 章 设置资源安全性

在本主题中，建立对象的所有权和公共权限，并指定对应用程序的特定权限。还要设置工作站和打印机的资源安全性。对一个库完成整个主题，然后返回并对由应用程序使用的任何附加库重复这些步骤。当完成设置一个应用程序的资源安全性时，对其它应用程序重复这些步骤。

无论何时在系统上安装新应用程序或当为现有的应用程序设置资源安全性时，使用这些过程。

本主题中的样本屏幕显示 JKL Toy 公司的“权限列表”表单、“库描述”表单和“输出队列和工作站安全性”表单。可以在“设置所有权和公共权限”中找到这些表单的示例。

需要什么表单?

- 在“计划应用程序安装”中准备的“应用程序安装”表单。
- 在“将对象分组”中准备的“权限列表”表单。
- 在“确定库和对象的所有权”中准备的“库描述”表单。
- 在“保护打印机输出”和“保护工作站”中准备的“输出队列和工作站安全性”表单。
- 在“计划整体安全性策略”中准备的“系统责任”表单。

可以以几种方法设置资源安全性。本主题中步骤的顺序与“应用程序安装”表单、“权限列表”表单和“库描述”表单上的信息的顺序匹配。

1. 设置所有权和公共权限。
2. 创建权限列表。
3. 用权限列表保护对象。
4. 将用户添加到权限列表。
5. 设置任何特定权限。
6. 保护打印机输出。
7. 保护工作站。
8. 限制对系统操作员消息队列的访问。

设置所有权和公共权限

在本主题中，建立应用程序库、组库和个人库的所有权和公共权限。对一个应用程序完成整个主题，然后返回，并对任何附加应用程序重复这些步骤。样本屏幕显示 Sharon Jones 为“计划应用程序安装”中的“客户订单”应用程序准备的“应用程序安装”表单。

无论何时在系统上安装新应用程序或设置现有的应用程序安全性时，都使用本主题中的过程。

使用您在“计划应用程序安装”中准备的“应用程序安装”表单。

要设置所有权和公共权限，完成以下任务:

1. 创建所有者概要文件。
2. 更改库所有权。
3. 设置应用程序对象的所有权。
4. 设置对库的公共访问权。
5. 设置库中所有对象的公共权限。
6. 设置新对象的公共权限。
7. 使用组和个人库。

注册到系统

概要文件
您自己的概要文件（需要 *ALLOBJ 权限）

菜单 主菜单

创建所有者概要文件

如果所有者概要文件尚未存在，执行下列操作:

- 使用 CRTUSRPRF（创建用户概要文件）命令来创建它。将密码设置为 *NONE。

如果所有者概要文件已存在，执行下列操作:

- 使用 CHGUSRPRF（更改用户概要文件）命令来将密码设置为 *NONE。

在创建所有者概要文件之后，可以更改库所有权。

更改库所有权

此步骤更改库的所有权而不是库中对象的所有权。

注意: 在更改任何应用程序对象的所有权之前，确保与应用程序供应商一起检查。某些应用程序使用依赖特定对象所有权的功能。

1. 输入 CHGOBJOWN（更改对象所有权）并按 **F4**（提示）。
2. 填写库名称、对象名称（*LIB）和新所有者。
3. 检查确认消息。

```
                    更改对象所有者（CHGOBJOWN）

输入选项，按执行键。
对象 . . . . . > COPGMLIB
  库 . . . . . >   *LIBL       名称，
对象类型 . . . . . > *LIB
新所有者 . . . . . .   COWNER
当前所有者权限 . . . . . .   *REVOKE
```

可能的错误	恢复
接收到错误消息。	最常见的消息是未找到库或未找到新所有者概要文件。检查输入是否有错误，并重试。

在更改库所有权之后，可以设置应用程序对象的所有权。

设置应用程序对象的所有权

更改应用程序对象的所有权是一个较麻烦的任务，因为您必须单独地更改每个对象。如果有可能，请求程序员或应用程序供应商为您建立所有权。

列示库中的对象

在更改所有权之前，使用“显示库”命令打印库中所有对象的列表。可以将它用作核对表。输入 DSPLIB *library-name* *PRINT。

选择最佳方法

选择下列两种方法之一来更改应用程序库中对象的所有权:

表 61. 更改对象所有权的方法

方法	它的作用	何时使用它
按所有者使用对象命令	显示列示概要文件拥有的所有对象的屏幕。使用屏幕上的一个选项来更改对象的所有者。	此方法易于使用。然而，如果 QPGMR 或 QSECOFR 拥有对象，IBM 建议不要使用此方法。这些概要文件拥有许多对象，您的列表屏幕将很大。
更改对象所有权命令	要求对每个对象使用单独的命令。然而，可以使用*检索*（**F9**）来重复先前命令并减少所需的输入量。	如果 QPGMR 或 QSECOFR 拥有对象，则此方法更快。

使用“按所有者使用对象”（WRKOBJOWN）命令

如果 IBM 提供的概要文件（如 QPGMR 或 QSECOFR）*未*拥有这些对象，则使用此方法来更改库中对象的所有权:

1. 输入 WRKOBJOWN *owner-profile-name*。屏幕显示用户概要文件拥有的所有对象的列表。
2. 在您正在使用的库中的每个对象前面输入 **9**（更改所有者）。
3. 在屏幕底部的*参数或命令*行上，输入 NEWOWN(*owner-profile-name*) 并按**执行**键。
4. 系统将您指示的每个对象的所有者更改为您在底部输入的新所有者。您会在屏幕的底部接收到确认消息。对象不再显示在屏幕上，因为概要文件不再拥有他们。
5. 重复步骤 2 和 4，直到更改库中所有对象的所有权为止。

```
                          按所有者使用对象

用户概要文件 . . . . . :   OLDOWNER

输入选项，按执行键。
  2=编辑权限     4=删除    5=显示程序设计者
  8=显示描述     9=更改所有者

Opt  对象          库            类型         属性
     COPGMMSG      COPGMLIB      *MSGQ
9    CUSTMAS       CUSTLIB       *FILE
9    CUSTMSGQ      CUSTLIB       *MSGQ
     ITEMMSGQ      ITEMLIB       *MSGQ


  ⋮

参数或命令
===> NEWOWN(COWNER)
F3=退出    F4=提示     F5=刷新    F9=检索
F18=底部
```

可能的错误	恢复
看到“更改对象所有者”屏幕。	如果指定选项 **9**（更改所有者）且未在“按所有者使用对象”屏幕的底部输入任何参数，则会看到此屏幕。如果输入不正确的参数，也会看到此屏幕。按 **F12**（取消）来返回到“按所有者使用对象”屏幕。重试。确保输入如示例中所示的参数。

可以使用更改对象所有者命令来更改由 QPGMR 或 QSECOFR 拥有的对象的所有权。

使用更改对象所有者命令

如果 QPGMR 或 QSECOFR *的确*拥有这些对象，则使用此方法来更改库中对象的所有者。

1. 输入 CHGOBJOWN 并按 **F4**（提示）。
2. 对于列表上的第一个对象，在屏幕上填写信息，并按**执行**键。

```
                    更改对象所有者（CHGOBJOWN）

输入选项，按执行键。
对象 . . . . . > CUSTMAS
  库 . . . . . >   CUSTLIB
对象类型 . . . . . > *FILE
新所有者 . . . . . .  COWNER
当前所有者权限 . . . . .  *REVOKE
```

3. 您会接收到已更改对象所有权的确认消息。核对您的列表上的项。
4. 按 **F9**（检索）来检索输入的命令。
5. 按 **F4**（提示）。在“更改对象所有者”屏幕上，输入库中下一个对象的信息，并按**执行**键。
6. 对库中的每个对象重复步骤 4 或 5。

检查工作

要确保已更改库中所有对象的所有权，使用“按所有者使用对象”命令。输入 WRKOBJOWN *new-owner-profile*。将屏幕与库中对象的列表进行比较。

在更改库中对象的所有权之后，可以设置对库的公共访问权。

设置对库的公共访问权

在设置应用程序对象的所有权之后，可以使用“编辑对象权限”（EDTOBJAUT）命令来更改库的公共权限:

1. 输入 EDTOBJAUT *library-name* *LIB。
2. 将光标下移到显示 **PUBLIC* 的行。
3. 输入您希望公众对库具有的权限，并按**执行**键。

```
                          编辑对象权限

对象 . . . . . :   CUSTLIB         所有者 . . . . . :   COWNER
  库 . . . . . :     QSYS             主组 . . . . . :   *NONE
对象类型 . . . . . :   *LIB

输入对当前权限的更改，按执行键。
  由权限列表保护的对象  . . . . . .   *NONE

                        对象
用户        组          权限
COWNER                  *ALL
*PUBLIC                 *CHANGE
```

4. 屏幕显示新权限。

现在可以设置库中所有对象的公共权限。

设置库中所有对象的公共权限

使用“取消对象权限”（RVKOBJAUT）命令来除去库中对象的当前公共权限。使用“授予对象权限”（GRTOBJAUT）命令来设置库中所有对象的公共权限:

1. 输入 RVKOBJAUT 并按 **F4**（提示）。
2. 填写显示的屏幕，替换上您的应用程序库的名称，并按**执行**键。

```
                  取消对象权限（RVKOBJAUT）

输入选项，按执行键。
对象 . . . . . .   *all
  库 . . . . . .     custlib
对象类型 . . . . . .   *all
用户 . . . . . .   *public
            + 以获取更多值
权限 . . . . . .   *all
```

注: 如果库具有大量对象，则系统可能要花几分钟来处理您的请求。

3. 输入 GRTOBJAUT 并按 **F4**（提示）。
4. 填写显示的屏幕，替换上您的应用程序库的名称和需要的权限，并按**执行**键。

```
                    授予对象权限（GRTOBJAUT）

输入选项，按执行键。
对象 . . . . . .  *all
  库 . . . . . .    custlib
对象类型 . . . . . .  *all
用户 . . . . . .  *public
            + 以获取更多值
权限 . . . . . .  *use
```

注：如果库具有大量对象，则系统可能要花几分钟来处理您的请求。

在设置完库中所有对象的公共权限之后，下一步您可以使用作业记录来检查您的工作。

使用作业记录来检查您的工作

当使用 GRTOBJAUT 命令对权限进行多次更改时，查看作业记录来验证所作的更改。

1. 输入 DSPJOBLOG（显示作业记录）。
2. 按 **F10**（显示详细消息）。
3. 您应该会获得一条有关库中每个对象的权限更改的消息。当查看消息时，核对列表上的对象。

```
                          显示所有消息
    系统:     RCHASxxx
作业 . . :   QPADEV0010    用户 . . :   JCHEIDEL      编号 . . . :   025457

7 > GRTOBJAUT OBJ(CUSTLIB/*ALL) OBJTYPE(*ALL) USER(*PUBLIC) AUT(*USE)
  授予用户 *PUBLIC 对 CUSTLIB 中对象类型为 *FILE 的对象 CUSTMAS 的权限。
  授予用户 *PUBLIC 对 CUSTLIB 中对象类型为 *MSGQ 的对象 CUSTMSGQ 的权限。
  授予对 2 个对象的权限，未授予对 0 个对象的权限，部分地授予对 0 个对象的权限。
  已授予对象权限。
7>> dspjoblog
```

可能的错误	恢复
作业记录指示未更改库中某些对象的权限。	使用“帮助”（**F1**）来获取有关消息的更多信息。使用 EDTOBJAUT 来单独设置这些对象的权限。

现在可以设置新对象的公共权限。

设置新对象的公共权限

库描述具有称为创建权限（CRTAUT）的参数，它确定在库中创建的新对象的公共权限。创建对象的命令使用对象库的 CRTAUT 权限作为缺省值。您应该使库的 CRTAUT 权限与库中大多数现有对象的公共权限相同。

1. 输入 CHGLIB *library-name* 并按 **F4**（提示）。
2. 按 **F10**（附加参数）。
3. 在*创建权限*字段中输入您的选择。

```
                    更改库（CHGLIB）

输入选项，按执行键。
库 . . . . . . . . . . . . . . . > CUSTLIB
库类型 . . . . . . . . . . . . .   *PROD
文本‘描述’ . . . . . . . . . .    ‘客户记录’


                    附加参数

创建权限 . . . . . . . . . . .   *CHANGE
创建对象审计 . . . . . . . . .   *SYSVAL
```

如果将 CRTAUT 设置为 *SYSVAL，则当在库中创建新对象时，系统对 QCRTAUT 系统值使用当前设置。对每个库设置特定 CRTAUT 权限可以保护 QCRTAUT 系统值在以后不受更改。

您现在可以使用组和个人库。

使用组和个人库

概要文件拥有您在设置用户组和单个用户时创建的组和个人库。

使用刚才描述的过程来将组库的所有权更改为组概要文件，并将个人库的所有权更改为单个用户概要文件。使用 EDTOBJAUT 命令。

为每个组和个人库设置“创建权限”参数，以确定这些库中任何新对象的公共权限。使用 CHGLIB 命令。

在开始创建权限列表之前，完成下列任务:

- 使用“应用程序安装”表单和“库描述”表单来确保已建立所有应用程序库的所有权和公共权限。
- 为您所创建的所有组和个人库设置所有权并创建权限。

注: 通过输入 DSPOBJD *ALL *LIB *PRINT，可以获取系统上所有库的列表。

创建权限列表

在设置所有权和公共权限之后，准备设置权限列表。通过使用“权限列表”表单中的信息，创建保护库所必需的任何权限列表。使用“创建权限列表”（CRTAUTL）命令:

1. 输入 CRTAUTL 并按 **F4**（提示）。
2. 填写“权限列表”表单中的信息。
3. 按 **F10**（附加参数）。
4. 使用权限参数来指定对由列表保护的对象的公共权限。
5. 检查确认消息。

```
                    创建权限列表（CRTAUTL）

输入选项，按执行键。
权限列表 . . . . . .   custlst1
文本‘描述’ . . . . .   清除文件的时间

                       附加参数

权限 . . . . . . . . .  *ALL
```

可能的错误	恢复
输入了不正确的列表名称。	系统一旦创建列表，您就不能更改列表的名称。删除列表（DLTAUTL）并重试。
忘记为列表指定公共权限。	使用“编辑权限列表”（EDTAUTL）命令。

可以立即用权限列表保护对象。

用权限列表保护对象

您一旦创建权限列表，就使用“编辑对象权限”（EDTOBJAUT）命令来保护“权限列表”表单上列示的项:

1. 输入 EDTOBJAUT 并按 **F4**（提示）。
2. 填写提示屏幕，并按**执行**键。
3. 在“编辑对象权限”屏幕上，输入权限列表名称。
4. 如果对象的公共权限来自权限列表，则将公共权限更改为 *AUTL。
5. 对“权限列表”表单上的每个对象重复这些步骤。

```
                        编辑对象权限

对象 . . . . . :   ARFILE01       所有者 . . . . . :   OWNAR
  库 . . . . . :     CUSTLIB      主组 . . . . . :   *NONE
对象类型 . . . . . :   *FILE

输入对当前权限的更改，按执行键。
  由权限列表保护的对象  . . . . . .   CUSTLST1

                        对象
用户        组          权限
OWNER                   *ALL
*PUBLIC                 *AUTL
```

可以立即将用户添加到权限列表。

将用户添加到权限列表

一旦用权限列表保护对象，就使用“编辑权限列表”（EDTAUTL）命令来添加“权限列表”表单上列示的用户:

1. 输入 EDTAUTL *authorization-list-name*。
2. 在“编辑权限列表”屏幕上，按 **F6**（添加新用户）。

3. 输入用户或组的名称和他们对列表上的项应该具有的权限，并按**执行**键。
4. 新用户应出现在列表上。

```
                              添加新用户

对象 . . . . . :   WSLST1          所有者   . .
  库 . . . . . :     QSYS

输入新用户，按执行键。
                对象     列表
用户            权限     管理
QSECOFR         *CHANGE
```

可能的错误	恢复
给用户或组授予了对列表的错误权限。	可以在“编辑权限列表”屏幕上更改权限。
将错误的用户或组添加到列表。	可以使用“除去权限列表项”（RMVAUTLE）命令除去用户或组，也可以在“编辑权限列表”屏幕上的用户权限上输入空白。

检查工作

使用“显示权限列表”（DSPAUTL）命令来列示对权限列表的所有用户权限。使用屏幕中的 **F15** 来列示由权限列表保护的所有对象。

在设置特定权限之前，完成下列任务:

- 使用 CRTAUTL 命令来为应用程序创建您需要的任何权限列表。
- 通过使用 EDTOBJAUT 命令用权限列表保护对象。
- 通过 EDTAUTL 命令将用户添加到权限列表。

设置特定权限

在“设置所有权和公共权限”中，您了解了如何使用 GRTOBJAUT 命令来基于“库描述”表单的“第一部分”中的信息设置库中所有对象的公共权限。现在，可以使用“编辑对象权限”（EDTOBJAUT）命令来基于“库描述”表单的“第二部分”中的信息设置库和库中对象的特定权限。

参见下列主题来设置特定权限:

- 设置库的特定权限。
- 设置对象的特定权限。
- 同时设置多个对象的权限。

设置库的特定权限

库实际上是一种特殊类型的对象。通过 EDTOBJAUT 命令，象设置任何其它对象的权限一样设置库的权限。所有库都驻留在由 IBM 提供的称为 QSYS 的库中。以下示例中的屏幕使用 JKL Toy 公司的 CONTRACTS 库的“库描述”表单的“第二部分”:

列示库对象的特定权限

组概要文件或用户概要文件	对象名称	对象类型	所需权限	权限列表
DPTSM	CONTRACTS	*LIB	*USE	
DPTMG	CONTRACTS	*LIB	*USE	

1. 输入 EDTOBJAUT 并按 **F4**（提示）。
2. 填写提示屏幕，并按**执行**键。

```
                    编辑对象权限（EDTOBJAUT）

输入选项，按执行键。
对象 . . . . . . . . . . . . . .   CONTRACTS
  库 . . . . . . . . . . . . . .     QSYS
对象类型 . . . . . . . . . . . .   *LIB
```

3. 在“编辑对象权限”屏幕上，按 **F6**（添加新用户）来将权限授予屏幕上未列示的用户。
4. 按**执行**键。

```
                          添加新用户

对象 . . . . . :   CONTRACTS       所有者 . . . . . :   OWNCP
  库 . . . . . :     QSYS            主组 . . . . . :   *NONE
对象类型 . . . . . :   *LIB


输入新用户，按执行键。
             对象
用户         权限
DPTSM        *USE
DPTMG        *USE
```

5. “编辑对象权限”屏幕应该与“库描述”表单的“第一部分”和“第一部分”上的信息匹配。

```
                          编辑对象权限

对象 . . . . . :   CONTRACTS       所有者 . . . . . :   OWNCP
  库 . . . . . :     QSYS            主组 . . . . . :   *NONE
对象类型 . . . . . :   *LIB

输入对当前权限的更改，按执行键。
  由权限列表保护的对象 . . . . . . . . . . . . . . . . . . . . .   *NONE

                       对象
用户         组        权限
OWNCP                  *ALL
DPTSM                  *USE
DPTMG                  *USE
*PUBLIC                *EXCLUDE
```

新对象的公共权限（CRTAUT）未出现在库的“编辑对象权限”屏幕上。使用“显示库”（DSPLIB）命令来查看库的 CRTAUT。

也可以使用此过程来设置对系统上对象的特定权限。

现在可以设置对象的特定权限。

设置对象的特定权限

设置应用程序库中对象的特定权限的过程与设置库的特定权限相同。示例使用 JKL Toy 公司的 COPGMLIB 库的“库描述”表单的“第二部分”：

表 62. JKL Toy 公司的“库描述”表单

组概要文件或用户概要文件	对象名称	对象类型	所需权限	权限列表
PUBLIC	COMSGQ01	*MSGQ	*CHANGE	

1. 输入 EDTOBJAUT 并按 **F4**（提示）。
2. 填写提示屏幕上的信息，并按**执行**键。
3. 填写“编辑对象权限”屏幕上的权限信息，并按**执行**键。

```
                              编辑对象权限

对象 . . . . . :   COMSGQ01        所有者 . . . . . :    OWNCO
  库 . . . . . :     COPGMLIB      主组 . . . . . :    *NONE
对象类型 . . . . . :   *MSGQ

输入对当前权限的更改，按执行键。
  由权限列表保护的对象  . . . . . .   *NONE

                          对象
用户        组            权限
OWNCO                     *ALL
*PUBLIC                   *CHANGE
```

现在可以同时设置多个对象的权限。

同时设置多个对象的权限

示例迄今为止已使用 EDTOBJAUT 命令来设置单个对象的特定权限。使用“授予权限”（GRTOBJAUT）命令来设置多个对象的安全性。输入 GRTOBJAUT 并按 **F4**（提示）。以下是对权限进行多次更改的一些示例。

- 在以下屏幕上输入的字段将 CUSTLIB 库中所有消息队列的公共权限设置为 *CHANGE。

```
                        授予对象权限（GRTOBJAUT）

输入选项，按执行键。
对象 . . . . . .   *all
  库 . . . . . .     custlib
对象类型 . . . . . .   *msgq
用户 . . . . . .   *public
               + 以获取更多值
权限 . . . . . .   *change
```

- 在以下屏幕上输入的字段将对 CUSTLIB 库中其名称以字符 WRK 开始的所有文件的 *ALL 权限授予用户 AMES。

```
                        授予对象权限

输入选项，按执行键。
对象 . . . . . . . . . . . . . .   WRK*
  库 . . . . . . . . . . . . . .     custlib
对象类型 . . . . . . . . . . . .   *file
用户 . . . . . . . . . . . . . .   AMES
               + 以获取更多值
权限 . . . . . . . . . . . . . .   *all
```

此示例使用称为**类属**命名的技术指定参数。许多命令允许您对参数指定头几个字符后跟一个星号（*）。系统对其名称以这些字符开始的每个对象执行操作。命令的联机信息告诉哪些参数允许类属名称。

- 您将需要遵循两个步骤，以使用称为 ARLST1 的权限列表来保护以字符 AR 开始的所有文件，并使文件从列表中获取它们的公共权限。这些屏幕显示需要的步骤。

```
                        授予对象权限

输入选项，按执行键。
对象 . . . . . . . . . . . . . .   AR*
  库 . . . . . . . . . . . . . .     CUSTLIB
对象类型 . . . . . . . . . . . .   *FILE

   ⋮
权限列表 . . . . . . . . . . . .   ARLST1
```

```
                        授予对象权限

输入选项，按执行键。
对象 . . . . . . . . . . . . . .   AR*
  库 . . . . . . . . . . . . . .     CUSTLIB
对象类型 . . . . . . . . . . . .   *FILE
用户 . . . . . . . . . . . . . .   *PUBLIC
               + 以获取更多值
权限 . . . . . . . . . . . . . .   *AUTL
               + 以获取更多值
```

如“使用作业记录来检查您的工作”中所述使用 DSPJOBLOG 命令来验证系统是否作出了所请求的权限更改。

转至“保护打印机输出”之前，使用 EDTOBJAUT 或 GRTOBJAUT 命令来在“库描述”表单的“第二部分”上设置特定权限。

保护打印机输出

设置特定权限之后，可以通过使用以下主题中的信息保护机密的打印机输出:

- 创建输出队列并控制谁可以管理它。
- 将特殊打印机输出指定到队列。

创建输出队列

1. 输入 CRTOUTQ（创建输出队列）并按 **F4**（提示）。
2. 填写输出队列和库的名称。
3. 按 **F10**（附加参数）。
4. 向下翻页来查找输出队列的安全性信息。

```
                        创建输出队列（CRTOUTQ）

输入选项，按执行键。
输出队列 . . . . . . . . . . . . >   NEWCP
  库 . . . . . . . . . . . . . .       CONTRACTS
最大假脱机文件大小:
  页数 , . . . . . . . . . . . .   *NONE          数字，*NONE
  启动时间  . . . . . . . . . .                   时间
  结束时间 . . . . . . . . . . .                  时间
              + 以获取更多值
队列上文件的顺序 . . . . . . . .   *FIFO
远程系统 . . . . . . . . . . . .   *NONE

   ⋮
文本‘描述’ . . . . . . . . . .   新合同队列
```

5. 填写“输出队列和工作站安全性”表单中的信息来控制谁可以使用并管理输出队列。
6. 按**执行**键，并检查确认消息。

```
                        创建输出队列（CRTOUTQ）

输入选项，按执行键。

附加参数

显示任何文件 . . . . . . . . . .   *NO
作业分隔符 . . . . . . . . . . .   0
受控制的操作员 . . . . . . . . .   *NO
数据队列 . . . . . . . . . . . .   *NONE
  库 . . . . . . . . . . . . . .
检查权限 . . . . . . . . . . . .   *OWNER
权限 . . . . . . . . . . . . . .   *LIBCRTAUT
```

可能的错误	恢复
按了**执行**键而不是按 **F10**。	使用“更改输出队列”（CHGOUTQ）命令来输入附加信息。
在错误的库中创建输出队列。	使用“移动对象”（MOVOBJ）命令来将它移动到正确的库。

您现在可以将打印机输出指定到输出队列。

将打印机输出指定到输出队列

在创建输出队列之后，可以将打印机输出指定到输出队列。打印机文件通常控制打印机输出的目的地。与应用程序供应商一起检查，以找出机密报表的打印机文件的名称和库。

如果您不能访问此信息，打印该报表并将它保留在输出队列中。从“使用假脱机文件”屏幕使用属性选项来找出打印机文件的名称。打印机文件显示在“使用假脱机文件属性”屏幕上的*设备文件*字段中。

要更改打印机文件的目的地（输出队列），使用“更改打印机文件”（CHGPRTF）命令:

```
CHGPRTF FILE(library-name/printer-file-name)
        OUTQ(library-name/output-queue-name)
```

无论何时有人再次请求该报表，该报表将转至新目的地。要更改已在输出队列的假脱机文件的目的地，从“使用假脱机文件”屏幕使用更改选项。

例如，JKL Toy 公司的 Sharon Jones 要将价格列表打印机文件 PRCLST1 指定到 PRICEQ 输出队列。她输入:

```
CHGPRTF FILE(CONTRACTS/PRCLST1) OUTQ(CONTRACTS/PRICEQ)
```

要将所有价格列表报表指定到 PRICEQ 输出队列，Sharon 可以使用类属打印机文件名:

```
CHGPRTF FILE(CONTRACTS/PRCLST*) OUTQ(CONTRACTS/PRICEQ)
```

要将所有新合同定向至 NEWCP 输出队列，Sharon 可以更改与用于创建合同的样本文档相关联的输出队列。

检查工作

检查机密打印机输出的保护策略的最好的方法是将它打印出来。检查打印机输出是否转至正确的输出队列。以系统操作员身份注册，并查看是否可以查看或处理队列上的文件。

在保护工作站之前，确保已执行下列操作:

- 通过使用 CRTOUTQ 命令，创建“输出队列和工作站安全性表单”上列示的任何输出队列。
- 通过使用 CHGPRTF 命令，将打印机输出指定到新的输出队列。

保护工作站

在保护打印机输出之后，应该保护您的工作站。象授权系统上的其它对象一样授权工作站。使用 EDTOBJAUT 命令来授予用户对工作站的权限。

用户必须具有 *CHANGE 权限才能在工作站上注册。如果 QLMTSECOFR 系统值为否（0），则安全主管或具有 *ALLOBJ 权限的任何人可以在任何工作站上注册。

如果 QLMTSECOFR 系统值为是（1），则使用下列准则来设置对工作站的权限:

允许在工作站上注册的用户	公共权限	QSECOFR 权限	单个用户权限
所有用户	*CHANGE	*CHANGE	不需要
仅选择的用户	*EXCLUDE	无权限	*CHANGE
选择的用户和具有对所有对象的权限的用户。	*EXCLUDE	*CHANGE	*CHANGE
除具有对所有对象的权限的用户以外的所有用户。	*CHANGE	无权限	不需要

在限制对系统操作员消息队列的访问之前，使用 EDTOBJAUT 命令基于“输出队列和工作站安全性”表单上的信息来保护工作站。

限制对系统操作员消息队列的访问

通过保护打印机输出、保护工作站和限制对系统操作员消息队列的访问，可以改进安全性。

ASSIST 菜单上用于处理消息的选项允许用户使用功能键来显示系统操作员（QSYSOPR）消息队列。对系统操作员消息的不正确响应可能在系统上导致问题。用户需要 *CHANGE 权限才能响应并删除消息队列中的消息。仅系统操作员应该具有此权限。查阅“系统责任”表单，以查看谁对系统操作员消息队列具有 *CHANGE 权限。

使用 EDTOBJAUT 命令:

1. 输入 EDTOBJAUT QSYSOPR *MSGQ 并按**执行**键。
2. 按 **F11** 来显示详细的对象权限信息。
3. 对公众授予 *OBJOPR 权限，如样本屏幕上所示，并按**执行**键。

```
                          编辑对象权限

对象 . . . . . :   QSYSOPR         所有者 . . . . . :   QSYS
  库 . . . . . :     QSYS             主组 . . . . . :   *NONE
对象类型 . . . . . :  *MSGQ

输入对当前权限的更改，按执行键。
  由权限列表保护的对象  . . . . . .   *NONE

                       对象     ----------对象-----------
用户        组         权限 操作员 管理  存在  改变  引用
*PUBLIC                USER DEF    X
```

4. 系统将*对象权限*列更改为 USER DEF（用户定义）。
5. 再次按 **F11** 来显示详细的数据权限信息。
6. 对公众授予 *ADD 权限，如样本屏幕上所示，并按**执行**键。

```
                          编辑对象权限

对象 . . . . . :   QSYSOPR         所有者 . . . . . :   QSYS
  库 . . . . . :     QSYS             主组 . . . . . :   *NONE
对象类型 . . . . . :  *MSGQ

输入对当前权限的更改，按执行键。
  由权限列表保护的对象  . . . . . .   *NONE

                       对象     ---------------数据---------------
用户        组         权限      读     添加  更新  删除  执行
*PUBLIC                USER DEF        X
```

7. 使用 **F6**（添加用户）来添加需要响应 QSYSOPR 消息的用户。对他们授予 *CHANGE 权限。

注意: 不要使公共权限成为 *EXCLUDE。所有作业（和用户）必须能够将消息添加到 QSYSOPR 消息队列。

要确保已设置完资源安全性，您应该:

- 使用“权限列表”表单和“库描述”表单来确保已建立所有应用程序库的安全性。

- 检查“输出队列和工作站安全性”表单，确保已保护工作站并创建任何特殊输出队列。
- 限制对系统操作员（QSYSOPR）消息队列的访问。
- 根据应用程序附带的指示信息，保存应用程序库。系统将所有权和公共权限信息与应用程序保存在一起。
- 使用“保存安全性数据”（SAVSECDTA）命令来保存已创建的安全性信息。有关如何保存安全性信息的更多信息，参见“保存安全性信息”。

您现在可以开始测试您的安全性设置。

第 8 章 测试安全性

本主题描述用于测试系统上已设置的安全性的技术。在此上下文中测试意味着确保您已以希望的方式设置工作。主题“监控安全性”讨论如何评估系统上安全性的有效性。

无论何时在系统上进行了较大的更改，都应测试安全性。这可能是添加新应用程序、设置现有应用程序的资源安全性、添加新用户组或更改安全级别。

当进行安全性更改时，查看以下主题以了解用于测试和诊断问题的方法:

- 测试用户概要文件。
- 测试资源安全性。

测试用户概要文件

要开始测试您的安全性，无论何时在系统上设置新组，都将要测试用户概要文件。测试从组概要文件复制的单个概要文件的其中一个。

- 是否能用用户概要文件成功注册？如果不能注册，则检查对未成功注册尝试写入的作业记录。从 ASSIST 菜单使用“使用打印机输出”选项来定位作业记录以获取更多信息。

  以下是最可能出现的问题:

  – 需要的对象的之一不存在，如初始菜单、当前库或初始程序。
  – 作业描述中指定的库列表导致错误。库不存在或忘记在库列表中包括 QGPL 和 QTEMP。
  – 用户对工作站没有权限。
- 当注册时，屏幕显示正确的初始菜单或程序吗？
- 如果在“注册”屏幕上输入初始菜单或当前库，会出现什么情况？如果用户概要文件是“受限制能力”（是），您应该会获取一条错误消息。
- 当按“辅助操作请求”键时，您是否获取正确的屏幕？
- 输出是否已转至正确的打印机？如果没有，从 ASSIST 菜单使用“使用打印机输出”选项来找出它转至的位置。检查用户概要文件和作业描述来确定输出为何会转至不同的打印机。
- 可以获取命令行吗？
- 可以执行需要的应用程序功能而不发生安全性错误吗？有关更多详细信息，参见“测试资源安全性”。
- 可以执行必要的系统任务，如管理打印机或保存库吗？

如果系统要求您在用概要文件注册时指定一个新密码，则在完成测试后，将密码设置回用户概要文件名称:

1. 用自己的概要文件（用安全主管权限）注册。
2. 输入 `CHGUSRPRF profile-name PASSWORD(profile-name) PWDEXP(*YES)`。

既然已测试用户概要文件，可以测试资源安全性。

测试资源安全性

在测试用户概要文件之后，您还应该测试资源安全性。当测试资源安全性时，查找下列各项:

- 没有足够权限来执行其作业的用户。
- 具有比您预期更多的权限的用户。

测试不足够的权限

测试交互式和批处理功能，以查看用户概要文件是否具有足够的权限。

交互式测试

要测试应用程序的资源安全性，可能需要用几个不同的用户概要文件注册。您的目标是测试样本用户来确保您已指定的权限是足够的。

- 测试需要不同级别权限的功能: 查看、更改和删除。
- 测试程序，而不只是菜单。选择菜单选项对于测试权限可能是不够的。有时，直到您实际上尝试执行操作（如删除记录）之后，系统才访问文件。当让系统打开文件时，发生权限检查。应用程序设计确定系统何时打开文件。
- 保持安全性错误的记录，并解决这些错误。如果发生安全性错误，您应该会在屏幕上看到一条消息，告诉您对该操作的权限不够以及您正在尝试使用的对象。

批处理测试

- 使用将提交作业的用户的概要文件，从应用程序运行样本批处理作业。
- 测试需要不同级别权限的批处理作业，如: 打印信息、更改信息或在月底清除文件。
- 检查 QSYSOPR 消息队列和 QHST 作业记录来查找安全性错误。使用 DSPLOG 命令来查看 QHST 作业记录。安全性消息的范围为: CPF2200、CPI2200、CPC2200、CPD2200、CPF4A00、CPI4A00、CPC4A00 和 CPD4A00。

  也可以使用安全性审计功能来记录权限故障和其它安全性相关的事件。

测试太多权限

如果设置资源安全性来保护机密信息，则测试样本用户概要文件来确保安全性起作用。用应该无法访问机密文件的用户的概要文件注册。

- 能够进入允许访问该文件的菜单吗？
- 如果选择使用该文件的菜单选项，会出现什么情况？
- 可以获取命令行吗？
- 可以运行命令（如 CPYF FROMFILE(*file-name*) TOFILE(QSYSPRT)）来列示该文件吗？
- 可以使用查询工具来查看该文件吗？

测试结果可能指示您需要更改安全性信息。

第 9 章 更改安全性信息

既然已计划系统的安全性，您需要确保在企业需要更改时您的计划保持有效。

本主题强调简单性是设计安全性的基本目标。已将用户组设计为单个用户的模式。已尝试使用除特定单个权限以外的公共权限、权限列表和库权限。当管理安全性时利用此方法:

- 当添加新用户组或新应用程序时，使用用于计划安全性的技术。
- 当需要对安全性进行更改时，尝试采用除创建异常以外的常规方法来解决特定问题。

主题安全性命令描述使用什么命令来显示、更改和删除安全性信息。

参见这些主题以获取处理不同类型的更改的建议:

- 将新用户添加到系统。
- 创建新用户组。
- 更改用户组。
- 添加新应用程序。
- 添加新的工作站。
- 更改用户责任。
- 从系统除去用户。

安全性命令

下表显示使用什么命令使用系统上的安全性对象。可以使用下列命令来执行这些任务:

- 查看并列示安全性信息。
- 更改安全性信息。
- 删除安全性信息。

表 63. 安全性命令

安全性对象	如何查看	如何更改	如何删除
系统值	WRKSYSVAL DSPSYSVAL	WRKSYSVAL CHGSYSVAL	不能删除
作业描述	WRKJOBD DSPJOBD	WRKJOBD CHGJOBD	DLTJOBD
组概要文件	WRKUSRPRF DSPUSRPRF DSPAUTUSR	WRKUSRPRF CHGUSRPRF	DLTUSRPRF[1],[2]
用户概要文件	WRKUSRPRF DSPUSRPRF DSPAUTUSR	WRKUSRPRF CHGUSRPRF CHGUSRAUD	DLTUSRPRF[1]

表 63. 安全性命令 (续)

安全性对象	如何查看	如何更改	如何删除
对象权限	DSPAUT DSPOBJAUT DSPUSRPRF TYPE(*OBJAUT)	CHGAUT EDTOBJAUT GRTOBJAUT WRKAUT	EDTOBJAUT RVKOBJAUT WRKAUT
对象所有权	WRKOBJOWN DSPOBJAUT DSPUSRPRF TYPE(*OBJOWN)	CHGOBJOWN CHGOWN	CHGOBJOWN CHGOWN 允许您取消先前所有者的权限。
主组	DSPOBJAUT WRKOBJPGP DSPUSRPRF TYPE(*OBJPGP)	CHGOBJPGP CHGPGP	CHGOBJPGP CHGPGP 将主组设置为 *NONE
对象审计	DSPOBJD	CHGOBJAUD CHGAUD	CHGOBJAUD（设置为 *NONE）CHGAUD
权限列表	DSPAUTL DSPAUTLOBJ	EDTAUTL（用户对列表的权限） EDTOBJAUT（由列表保护的对象） ADDAUTLE CHGAUTLE GRTOBJAUT	DLTAUTL（整个列表）[3] RMVAUTLE（除去用户对列表的权限）EDTOBJAUT（由列表保护的对象） RVKOBJAUT

1. IBM 建议使用“使用用户登记”屏幕中的除去选项来删除概要文件。使用此选项，可以删除由概要文件拥有的任何对象，或将它们重新分配给新的所有者。某些 DLTUSRPRF 命令参数允许您删除用户所拥有的所有对象或将它们全部分配给新的所有者。除非删除或重新指定拥有的对象，否则不能删除概要文件。也不能删除为任何对象的主组的概要文件。
2. 不能删除具有任何成员的组概要文件。使用 DSPUSRPRF 命令的 *GRPMBR 选项来列示组的成员。删除组概要文件之前，更改每个单个组概要文件中的*组概要文件*字段。
3. 不能删除用于保护对象的权限列表。使用 DSPAUTLOBJ 命令来列示由权限列表保护的对象。通过使用 EDTOBJAUT 命令来更改由权限列表保护的任何对象的权限。

查看与列示安全性信息

通过使用带打印（*PRINT）选项的显示（DSP）命令，可以列示安全性信息。例如，要显示称为 MYLIST 的权限列表，输入 `DSPAUTL MYLIST *PRINT`。

某些显示命令提供了用于不同类型的列表的选项。例如，当创建单个用户概要文件时，使用 DSPUSRPRF 命令的 *GRPMBR 选项来列示组概要文件的所有成员。使用提示（**F4**）和联机信息来查找什么列表可用于安全性对象。

可以使用“显示”命令来查看显示站上的安全性信息。也可以使用“使用...”（WRK）命令，该命令提供更多功能。“使用...”命令提供一个列表屏幕。可以使用此屏幕来更改、删除与查看信息。

也可以使用安全性命令来通过使用类属名称列示或查看信息。如果您输入 `WRKUSRPRF DPT*`，则“使用用户登记”屏幕或“使用用户概要文件”屏幕仅显示以字符 *DPT* 开始的概要文件。使用命令的联机信息来查找哪些参数允许类属名称。

更改安全性信息

通过使用“使用...”（WRK）或“编辑...”（EDT）命令，可以以交互方式更改安全性信息。可以查看信息，更改信息，以及在更改之后再次查看信息。

也可以通过使用“更改...”（CHG）或“授权...”（GRT）命令在进行更改之前和之后更改安全性信息，而不查看这些信息。此方法对一次更改多个对象特别有用。例如，使用 GRTOBJAUT 命令来设置库中所有对象的公共权限（参见第 103 页的『设置库中所有对象的公共权限』）。

删除安全性信息

通过使用“使用...”（WRK）或“编辑...”（EDT）命令，可以交互地删除或除去某些类型的安全性信息。也可以使用“删除...”（DLT）、“除去...”（RMV）和“取消...”（RVK）命令来删除安全性信息。通常，您必须符合某些条件，系统才允许您删除安全性信息。安全性命令中的注意事项描述了一些这样的条件。

将新用户添加到系统

当需要将新用户添加到系统时，使用下列过程:

1. 将人员指定到用户组。使用“用户组描述”表单以获取参考。
2. 决定新用户是否需要执行系统功能。如果需要，将该信息添加到“系统责任”表单。
3. 将人员添加到“单个用户概要文件”表单。
4. 查看“系统责任”表单和“用户组描述”表单，以确定新用户是否需要与组的对应值不同的值。
5. 通过复制组概要文件或组成员的概要文件来创建用户概要文件。确保将密码设置为到期。（参见“复制组概要文件”。）
6. 给新用户一份安全性备忘录的副本。

要了解如何创建新用户组，参见“创建新用户组”。

创建新用户组

因为下列几个原因，可能需要创建新用户组:

- 附加部门需要使用系统。
- 发现需要使用户组更具体才能满足资源安全性需要。
- 公司重新改组一些部门。

要创建新用户组，执行下列操作:

1. 通过遵循“计划用户组”中的下列指示信息来填写“用户组描述表单”。
2. 将用户组添加到您的应用程序、库和用户组的图表。
3. 评估任何组成员是否需要执行系统功能。更新“系统责任”表单。（参见“确定谁应该负责系统功能”。）
4. 使用“用户组描述”表单和“系统责任”表单中的信息来填写“单个用户概要文件”表单。
5. 创建组概要文件。

6. 创建组的作业描述。
7. 创建组概要文件。

   注: 有关执行步骤 5、6 和 7 的指示信息，参见“设置用户组”。
8. 为组成员创建单个用户概要文件。（参见“设置单个用户”。）
9. 评估组所需要的所有应用程序的“库描述”表单。通过使用“设置资源安全性”中描述的技术，执行任何必要的步骤来授予对应用程序对象的组访问权。
10. 给组的所有成员一份安全性备忘录的副本。

要了解如何更改用户组，参见“更改用户组”。

更改用户组

将需要以不同方式来处理对组的特征的不同类型更改。以下是更改的一些示例和如何处理它们:

更改组的权限

您可能会发现组需要在初始计划中未预期的对象权限。执行下列操作:

1. 使用“编辑对象权限”（EDTOBJAUT）命令来授予组对对象或对适当的权限列表的正确访问权。第 107 页的『设置特定权限』显示如何执行此操作的示例。当授予组权限时，组的每个成员都获取对对象的权限。
2. 如果授予组对机密资源的权限，您可能要验证组的当前成员。使用“显示用户概要文件”命令（DSPUSRPRF *group-profile-name* *GRPMBR）来列示组成员。

更改组的定制

可能需要更改为组的成员设置的用户环境。例如，如果某部门具有自己的打印机，您希望新打印机对于该部门的用户组的成员是缺省打印机。或者，当系统已安装新的应用程序时，用户组的成员在注册时，可能需要不同的初始菜单。

组概要文件提供一种模式，您可以复制该模式来创建组成员的单个概要文件。然而，创建单个用户概要文件之后，组概要文件中的定制值不会影响它们。例如，更改字段（如组概要文件中的*打印机设备*）不会影响组成员。您需要更改每个单个用户概要文件中的*打印机设备*字段。

可以使用“使用用户概要文件”屏幕来同时为多个用户更改参数。该示例显示更改组的所有成员的输出队列:

1. 输入 WRKUSRPRF *ALL 并按**执行**键。
2. 如果看到“使用用户登记”屏幕，则使用 **F21**（选择辅助级别）来更改为“使用用户概要文件”屏幕。

```
                          使用用户概要文件

输入选项，按执行键。
  1=创建    2=更改    3=复制    4=删除    5=显示
  12=按所有者使用对象

           用户
Opt        概要文件       文本

           HARRISOK       Harrison, Keith
2          HOGANR         Hogan, Richard
           JONESS         Jones, Sharon
2          WILLISR        Willis, Rose

   ⋮                                                              尚有...
选项 1、2、3、4 和 5 或命令的参数
===> PRTDEV(PRT02)
F3=退出    F5=刷新    F12=取消    F16=重复定位至    F17=定位至
F21=选择辅助级别     F24=其余键
```

3. 在要更改的每个概要文件的旁边输入 **2**（更改）。
4. 在屏幕底部的参数行，输入参数名称和新值。如果不知道参数名称，按 **F4**（提示）。
5. 按**执行**键。您会接收到对更改的每个概要文件的确认消息。

   尽管在组概要文件中更改定制字段不影响组成员，但它在以后可能有帮助。当稍后要将成员添加到组中时，组概要文件提供模式。它也是组的标准字段值的记录。

授予组对新应用程序的访问权

当用户组需要访问应用程序时，您需要分析有关组和应用程序的信息。以下是建议的方法:

1. 查看新应用程序的“应用程序描述”表单和您的应用程序、库和用户组的图表来查看应用程序使用哪些库。将这些库添加到“用户组描述”表单。
2. 更新您的应用程序、库和用户组的图表以显示用户组和应用程序之间的新关系。
3. 如果组的初始库列表应该包括库，则通过使用“更改作业描述”（CHGJOBD）命令来更改组的作业描述。如果需要帮助，则参见第 88 页的『创建作业描述』，以使用作业描述。

   注: 当将库添加到作业描述中的初始库列表时，不需要更改使用作业描述的用户概要文件。当用户下次注册时，他们的初始库列表自动添加这些库。
4. 评估您是否需要更改组的初始程序或初始菜单来提供对新应用程序的访问权。需要通过使用 CHGUSRPRF 命令来对每个用户概要文件的初始菜单或程序进行单独的更改。
5. 查看由应用程序使用的所有库的“库描述”表单。确定可用于库的公共访问权是否充分满足组的需要。如果不满足，您可能需要授予组对库、特定对象或权限列表的权限。使用“编辑对象权限”（EDTOBJAUT）和“编辑权限列表”（EDTAUTL）命令来执行此操作。（如果需要更多信息，参见“设置资源安全性”。）

要将应用程序添加到系统，参见“添加新应用程序”。

添加新应用程序

您应该和计划初始应用程序一样仔细地计划任何新应用程序的安全性。遵循相同过程:

1. 准备应用程序的“应用程序描述”表单和“库描述”表单。
2. 更新您的应用程序、库和用户组的图表。
3. 遵循“计划资源安全性”中的过程，以确定如何保护新应用程序。
4. 通过使用“计划您的应用程序安装”中描述的方法，准备“应用程序安装”表单。
5. 评估应用程序的任何打印机输出是否是机密的以及是否需要保护。如果有必要，更新“输出队列和工作站安全性”表单。
6. 遵循“设置所有权和公共权限”和“设置资源安全性”中描述的步骤来安装和保护应用程序。

要将工作站添加到系统，参见“添加新工作站”。

添加新工作站

当将新工作站添加到系统时，考虑安全性需求:

1. 新工作站的物理位置会造成任何安全性风险吗？（参见“计划物理安全性”来恢复您的记忆。）
2. 如果工作站会造成风险，则更新“输出队列和工作站安全性”表单。
3. 您通常应该创建具有公共权限 *CHANGE 的新工作站。如果这样不符合工作站的安全性需求，则使用 EDTOBJAUT 命令来指定不同权限。

要更改用户在系统上的责任，参见“更改用户的责任”。

更改用户的责任

当系统用户获得公司的新作业或一组新责任时，您需要评估这会如何影响用户概要文件。

1. 该用户应该属于不同用户组吗？可以使用 CHGUSRPRF 命令来更改用户组。
2. 您需要更改概要文件中的任何定制值（如打印机或初始菜单）吗？您也可以使用 CHGUSRPRF 命令来更改这些值。
3. 对于此用户，新用户组的应用程序权限足够吗？
   - 使用“显示用户概要文件”（DSPUSRPRF）命令来查看旧的和新的组概要文件的权限。
   - 还要查看单个用户概要文件的权限。
   - 通过使用 EDTOBJAUT 命令进行必要的更改。
4. 用户拥有任何对象吗？您应该更改这些对象的所有权吗？使用“按所有者使用对象”（WRKOBJOWN）命令。
5. 用户执行系统功能吗？用户需要为新作业执行系统功能吗？如果有必要，更新“系统责任”表单，并更改用户概要文件。

要了解如何从系统除去用户，参见“从系统除去用户”。

从系统除去用户

如果某人离开公司，应该立即从系统除去其用户概要文件。必须先删除或转移由用户概要文件拥有的任何对象的所有权，才可以删除该用户概要文件。可以使用 WRKOBJOWN 命令来执行此操作，也可以从“使用用户登记”屏幕使用选项 **4**（除去）。

当从“使用用户登记”屏幕对概要文件选择选项 **4**（除去）时，您会看到允许您处理用户拥有的任何对象的附加屏幕。可以选择将所有对象给予新所有者，或单独处理对象:

```
                                除去用户

用户 . . . . . . . . . . . :   HOGANR
用户描述 . . . . . . . . . :   销售及市场部门

要除去此用户，输入以下选项，然后按执行键。
    1. 将此用户拥有的所有对象给予新所有者
    2. 删除或更改由此用户拥有的特定对象的所有者。
```

如果选择单独地处理对象（选项**2**），屏幕显示用户拥有的所有对象的列表:

```
                                除去用户

用户 . . . . . . . . . . . :   HOGANR
用户描述 . . . . . . . . . :   销售及市场部门

新所有者 . . . . . . . . . .                    名称，F4 显示列表

要除去此用户，删除或更改所有对象的所有者。
输入以下选项并按执行键。
  2=更改为新所有者    4=删除    5=显示详细信息

Opt  对象          库            描述
 4   HOGANR        QUSRSYS       Hogan, Richard 消息队列
 4   QUERY1        DPTWH         库存查询
```

如果选择删除对象，会看到“确认删除”屏幕。一旦系统删除对象，就可以除去用户概要文件。然后您会再次看到“使用用户登记”屏幕，并且有一条消息告诉您系统已除去用户。

第 10 章 保存安全性信息

本主题概述如何保存与恢复安全性信息。当计划系统的备份与恢复时，您需要考虑信息的安全性和信息本身。参见“信息中心”主题备份、恢复和可用性来帮助您设计完整的备份与恢复计划。

下列主题描述如何备份与恢复在设置安全性时创建的安全性信息:

- 保存系统值。
- 保存组和用户概要文件。
- 保存作业描述。
- 保存资源安全性信息。
- 使用缺省所有者概要文件（QDFTOWN）。
- 从已损坏的权限列表恢复。

保存系统值

系统值存储在系统库 QSYS 中。当执行下列操作时，保存 QSYS 库:

- 使用“保存系统”（SAVSYS）命令。
- 从“保存”菜单使用保存整个系统的选项。
- 从“保存”菜单使用保存系统信息的选项。
- 从“运行备份”（RUNBCKUP）菜单使用备份整个系统的选项。

如果需要恢复整个系统，当恢复操作系统时自动恢复系统值。

下一步，参见“保存组和用户概要文件”。

保存组和用户概要文件

组和用户概要文件存储在 QSYS 库。当使用“保存系统”（SAVSYS）命令或选择保存整个系统的菜单选项时，保存这些概要文件。

也可以通过使用“保存安全性数据”（SAVSECDTA）命令保存组和用户概要文件。

通过使用“恢复用户概要文件”（RSTUSRPRF）命令恢复用户概要文件。正常顺序如下:

1. 恢复操作系统，这将恢复库 QSYS。
2. 恢复用户概要文件。
3. 恢复剩余的库。
4. 使用“恢复权限”（RSTAUT）命令来恢复对象的权限。

下一步，参见“保存作业描述”。

保存作业描述

当创建作业描述时，指定它应驻留的库。IBM 建议将作业描述创建到 QGPL 库。

可以通过保存作业描述所驻留的库来保存作业描述。使用“保存库”（SAVLIB）命令来执行此操作。也可以通过使用“保存对象”（SAVOBJ）命令来保存作业描述。

可以通过使用“恢复库”（RSTLIB）命令来恢复库的内容。可以通过使用“恢复对象”（RSTOBJ）命令来恢复单个作业描述。

下一步，参见“保存资源安全性信息”。

保存资源安全性信息

资源安全性定义用户可以如何使用对象，它由存储在几个不同位置的一些不同类型的信息组成:

表 64. 保存与恢复资源安全性信息

信息类型	存储它的位置	如何保存它	如何恢复它
公共权限	与对象一起	SAVxxx 命令[1]	RSTxxx 命令[2]
对象审计值	与对象一起	SAVxxx 命令[1]	RSTxxx 命令[2]
对象所有权	与对象一起	SAVxxx 命令[1]	RSTxxx 命令[2]
主组	与对象一起	SAVxxx 命令[1]	RSTxxx 命令[2]
权限列表	QSYS 库	SAVSYS 或 SAVSECDTA	RSTUSRPRF USRPRF(*ALL)
对象和权限列表之间的链接	与对象一起	SAVxxx 命令[1]	RSTxxx 命令[2]
专用权限	与用户概要文件一起	SAVSYS 或 SAVSECDTA	RSTAUT

1. 通过使用 SAVOBJ 或 SAVLIB 命令，可以保存大多数对象类型。某些对象类型（如配置）具有特殊保存命令。
2. 可以通过使用 RSTOBJ 或 RSTLIB 命令来恢复大多数对象类型。某些对象类型（如配置）具有特殊恢复命令。

当需要恢复应用程序或整个系统时，需要细心地计划步骤，包括恢复对象的权限。以下是恢复应用程序的资源安全性信息所必需的基本步骤:

1. 如果有必要，恢复用户概要文件，包括拥有应用程序的概要文件。可以用 RSTUSRPRF 命令恢复特定概要文件或所有概要文件。
2. 恢复由应用程序使用的任何权限列表。当使用 RSTUSRPRF USRPRF(*ALL) 时，恢复权限列表。

   注: 这将从备份媒体恢复所有用户概要文件值，包括密码。
3. 通过使用 RSTLIB 或 RSTOBJ 命令来恢复应用程序库。这将恢复对象所有者、公共权限和对象和权限列表之间的链接。
4. 通过使用 RSTAUT 命令来恢复对象的专用权限。RSTAUT 命令也恢复用户对权限列表的权限。您可以恢复特定用户或所有用户的权限。

有关恢复不在系统上的对象和所有者概要文件的信息，参见“使用缺省所有者概要文件（QDFTOWN）”。

使用缺省所有者概要文件（QDFTOWN）

如果恢复不在系统上的对象和所有者概要文件，则系统将对象的所有者转移到称为 QDFTOWN 的缺省概要文件。一旦恢复所有者概要文件或再次创建它，可以通过使用“按所有者使用对象”（WRKOBJOWN）命令来将所有者权转移回来。

有关权限列表恢复的信息，参见“从已损坏的权限列表恢复”。

从已损坏的权限列表恢复

当权限列表保护某个对象，而权限列表损坏时，则仅具有所有对象（*ALLOBJ）特权的用户才可以访问该对象。

从已损坏的权限列表恢复需要两个步骤:

1. 恢复用户和他们在权限列表上的权限。
2. 恢复权限列表与对象的关联。

具有 *ALLOBJ 特权的用户可以完成这些步骤。

步骤1: 恢复权限列表

如果知道用户对权限列表的权限，则删除权限列表，再次创建它，并对其添加用户。

如果并不知道用户对权限列表的所有权限，则通过使用以下步骤从最后一个 SAVSYS 或 SAVSECDTA 磁带恢复权限列表。

1. 删除已损坏的权限列表:

   ```
   DLTAUTL AUTL(authorization-list-name)
   ```

2. 恢复权限列表:

   ```
   RSTUSRPRF USRPRF(*ALL)
   ```

3. 通过使用“恢复权限”（RSTAUT）命令，将用户添加到列表。

步骤 2: 恢复对象与权限列表的关联

当已恢复权限列表或再次创建它时，需要建立列表和由列表保护的对象之间的链接。

1. 使用“回收存储器”（RCLSTG）命令。RCLSTG 将由已损坏或丢失的权限列表保护的对象指定到称为 QRCLAUTL 的缺省值列表。
2. 列示由 QRCLAUTL 权限列表保护的对象:

   ```
   DSPAUTLOBJ AUTL(QRCLAUTL)
   ```

3. 使用 GRTOBJAUT 命令来保护具有正确权限列表的对象。例如，要用权限列表 ARLST01 保护 CUSTLIB 库中的 ARWRK01 文件，输入

   ```
   GRTOBJAUT OBJ(CUSTLIB/ARWRK01) OBJTYPE(*FILE) +
             AUTL(ARLST01)
   ```

第 11 章 监控安全性

本主题提供关于监控系统上安全性保护装置的有效性的基本建议。

监控安全性一般具有两个基本目标:

- 确保充分地保护公司资源。
- 检测对您的系统和公司信息的未授权访问尝试。

当决定要定期执行哪些监控任务时，查看安全性策略声明和用户安全性备忘录。

参见下列主题以获取有关监控安全性的更多信息:

- 监控安全性的核对表。
- 安全性审计

用于监控安全性的核对表

以下是用于查看系统上安全性不同方面的核对表。使用它们来制订您的计划。

监控物理安全性

- 保护备份媒体不受损坏和窃取。
- 限制对公共区域中工作站的访问。使用 DSPOBJAUT 命令来查看对工作站具有 *CHANGE 权限的人员。

监控系统值

- 验证设置是否与“系统值选择”表单匹配。使用“打印系统安全性属性”（PRTSYSSECA）命令。
- 查看有关系统值的决定，特别是在安装新应用程序时。

监控组概要文件

- 验证组概要文件是否不具有密码。使用 DSPAUTUSR 命令来验证是否所有组概要文件具有密码 *NONE。
- 验证正确的人是组的成员。使用具有 *GRPMBR 选项的 DSPUSRPRF 命令来列示组的成员。
- 检查每个组概要文件的特权。使用 DSPUSRPRF 命令。如果正在以安全级别 30、40 或 50 运行，则组概要文件应该不具有 *ALLOBJ 权限。

监控用户概要文件

- 验证系统上的用户概要文件是否属于以下类别的其中一类:
  - 当前雇员的用户概要文件
  - 组概要文件
  - 应用程序所有者概要文件
  - IBM 提供的概要文件（以 Q 开头）
- 当公司调动用户或当用户离开公司时，除去他们的用户概要文件。使用“更改到期调度项”（CHGEXPSCDE）命令在用户一离开就自动删除或禁用概要文件。

- 查找不活动的概要文件并除去它们。使用“分析概要文件活动”（ANZPRFACT）命令来在概要文件不活动一定时间后自动禁用概要文件。
- 确定哪些用户具有与其用户概要文件名称相同的密码。使用“分析缺省密码”（ANZDFTPWD）命令。使用此命令的该选项来强制用户在下次注册到系统时更改他们的密码。

  注意: 不要从系统除去任何 IBM 提供的概要文件。IBM 提供的概要文件以字符 Q 开头。
- 知道谁具有除 *USER 以外的用户类以及为什么具有。使用“打印用户概要文件”（PRTUSRPRF）命令来获取所有用户、其用户类和特权的列表。使此信息与“系统责任”表单匹配。
- 控制哪些用户概要文件具有设置为 *NO 的*限制能力*字段。

监控关键对象

- 查看可以访问关键对象的用户。使用“打印专用权限”（PRTPVTAUT）命令和“打印公共授权对象”（PRTPUBAUT）命令来监控对象。如果组具有访问权，则使用 DSPUSRPRF 命令的 *GRPMBR 选项来验证组的成员。
- 验证谁可以使用通过另一安全性方法（如沿用权限）来提供对对象的访问权的应用程序。使用“打印沿用对象”（PRTADPOBJ）命令。

监控未授权的访问

- 指示系统操作员注意 QSYSOPR 消息队列中的安全性消息。特别要指出的是，让他们将重复的未成功注册尝试通知安全主管。安全性消息的范围在 2200 到 22FF 和 4A00 到 4AFF 之间。他们具有前缀 CPF、CPI、CPC 和 CPD。
- 设置安全性审计来记录对对象的未授权访问尝试。

下一步，参见安全性审计。

安全性审计

当监控安全性时，操作系统可以记录在系统上发生的安全性事件。这些事件记录在称为**日志接收器**的特殊系统对象中。可以设置日志接收器来记录不同类型的安全性事件（如更改系统值或用户概要文件）或访问对象不成功的尝试。以下值控制记录哪些事件:

- 审计控制（QAUDCTL）系统值
- 审计级别（QAUDLVL）系统值
- 用户概要文件中的审计级别（AUDLVL）值
- 用户概要文件中的对象审计（OBJAUD）值
- 对象中的对象审计（OBJAUD）值。

审计日志中的信息用于:

- 检测尝试的安全性违规。
- 计划迁移至更高的安全级别。
- 监控秘密对象（如机密文件）的使用。

命令可用于以不同的方式查看审计日志中的信息。

第 12 章 基本系统安全性计划表单

可以从浏览器复制或打印这些表单。

要打印整个基本安全性信息，选择正确的窗格，然后单击“信息中心”栏中的 PDF 图标。

要打印单个计划表单，单击与要打印的计划表单对应的链接。单击正确的窗格，然后单击浏览器中的“打印”图标。这将为您打印已选择的表单。

以下是成功计划和使用基本系统安全性所需要的所有计划表单的完整列表:

- “物理安全性计划”表单
- “应用程序描述”表单
- “命名约定”表单
- “库描述”表单
- “系统值选择”表单
- “系统责任”表单
- “用户组标识”表单
- “用户组描述”表单
- “单个用户概要文件”表单
- “权限列表”表单
- “输出队列和工作站安全性”表单
- “应用程序安装”表单

“物理安全性计划”表单

表 65. “物理安全性计划”表单

“物理安全性计划”表单	
准备人:	日期:
指示信息 • 在“计划资源安全性”中了解此表单。 • 使用此表单来描述与系统部件和连接的设备的物理位置相关的任何安全性问题。 • 您不必将此表单上的信息输入到系统。	
系统部件:	
描述保护系统部件的安全性措施（如已锁上的房间）:	
通常使用什么密钥锁位置？	
钥匙保存在何处？	
与系统部件相关的其它注释:	
备份媒体和文档:	
备份磁带存储在企业位置的何处？	
备份磁带存储在企业外的何处？	

表 65. “物理安全性计划”表单 (续)

安全主管、服务和 DST 密码保存在何处？	
重要系统文档（如序列号和配置）保存在何处？	

“物理安全性计划”表单			第二部分（共两部分）
第二部分的附加指示信息 • 以下列示其位置可能导致安全性暴露的任何工作站和打印机。指示您将采取什么保护措施。对于打印机，在*安全性暴露*列下列示机密打印报表的示例。 • 如果允许系统自动配置本地设备，您可能在安装系统之后才知道工作站和打印机的名称，如果准备此表单时您不知道这些名称，则填写描述（如位置）并稍后添加名称。			
工作站和打印机的物理安全性			
工作站或打印机的名称	它的位置或描述	安全性暴露	要采取的保护措施

“应用程序描述”表单

表 66. “应用程序描述”表单

“应用程序描述”表单	
准备人:	日期:
指示信息 • 在“描述您的应用程序”和“计划资源安全性”中了解此表单。 • 为每个应用程序准备单独的表单。 • 您不必将此表单上的信息输入到系统中。	
应用程序名称:	缩写:
应用程序的简要描述:	
主菜单名称:	库:
初始程序名称:	库:
为文件和程序列示由应用程序使用的库:	
定义应用程序的安全性目标，如是否有任何信息是机密的:	

“命名约定”表单

表 67. “命名约定”表单

“命名约定”表单	
准备人:	日期:

表 67. “命名约定”表单 (续)

指示信息 • 在“描述您的应用程序”中了解此表单。 • 您不必将此表单中的信息直接输入系统。 • 使用此表单来描述您将如何将名称指定给系统上的对象。给出每个对象的示例。	
对象类型	**命名约定**
组概要文件	
用户概要文件	
权限列表	
库	
文件	
日历	
设备	
磁带	

“库描述”表单

表 68. “库描述”表单

“库描述”表单	第一部分（共两部分）
准备人:	日期:
指示信息: • 在“计划用户安全性”和“计划资源安全性”中了解此表单。 • 使用此表单来描述您的主库，并定义它们的资源安全性需求。 • 对系统上的每个主应用程序库都填写一个表单。 • 在“设置资源安全性”中了解如何输入此表单中的信息。	
库名称:	描述性名称(文本):
简要描述此库的功能:	
为库定义安全性目标，如是否有任何信息是机密的:	
库的公共权限:	
库中对象的公共权限:	
新对象的公共权限（CRTAUT）:	
库所有者:	

“库描述”表单	第二部分（共两部分）
准备人:	日期:
库名称:	
第二部分的附加指示信息: • 在下面的图表中，列示需要特定权限的任何个人或对象。 • 指定所需权限的类型: *ALL、*CHANGE、*USE 或 *EXCLUDE。	
列示库对象的特定权限	

组概要文件或用户概要文件	对象名称	对象类型	所需权限	权限列表

系统值选择表单

表 69. “系统值选择”表单

“系统值选择”表单		第一部分（共两部分）
准备人:		日期:
指示信息 • 在“计划整体方法”中了解有关此表单的更多信息。 • 使用此表单来记录您对影响安全性和定制的系统值的选择。 • 使用“设置”菜单中的选项 **1** 来输入此表单的“第一部分”。		
来自“更改系统选项”屏幕的值		
系统值 / 网络属性	**建议的选项**	**您的选择**
系统名称		
日期分隔符（QDATSEP）		
日期格式（QDATFMT）		
时间分隔符（QTIMSEP）		
新设备的设备命名格式（QDEVNAMING）	1（iSeries 系统）	
系统打印机（QPRTDEV）		
安全级别（QSECURITY）	40	
允许安全主管注册到任何显示站（QLMTSECOFR）	N	
保存有关已完成的打印机输出的作业记帐信息（QACGLVL）	N (*NONE)	

“系统值选择”表单		第二部分（共两部分）
“第二部分”的附加指示信息 • 在“设置系统值”中了解有关此表单的“第二部分”的更多信息。 • 使用“使用系统值”（WRKSYSVAL）命令来输入“第二部分”。		
安全性系统值		
系统值	**建议的选项**	**您的选择**
不活动的作业超时时间间隔（QINACTITV）	30 至 60	

不活动的作业消息队列（QINACTMSGQ）	*DSCJOB	
限制设备会话（QLMTDEVSSN）	1（是）	
要对失败的注册尝试执行的操作（QMAXSGNACN）	3（都禁用）	
允许的最大注册尝试次数（QMAXSIGN）	3 至 5	
密码到期时间间隔（QPWDEXPITV）	30 至 60	
最大密码长度（QPWDMAXLEN）	8	
最小密码长度（QPWDMINLEN）	6	
需要不同密码（QPWDRQDDIF）	7（6 个唯一密码）	
其它系统值		
系统值	**建议的选项**	**您的选择**
断开连接的作业超时时间间隔（QDSCJOBITV）	300	
注: 可能要设置一些其它与安全性相关的系统值。参见 *Security-Reference*（SC41-5302-04）的第三章，以获取与安全性相关的系统值和对它们的建议的完整列表。		

“系统责任”表单

表 70. “系统责任”表单

“系统责任”表单			
准备人:			日期:
指示信息: • 在“计划单个用户概要文件”中了解此表单。 • 使用此表单来列示具有除 *USER 以外的用户类的每个用户。 • 将信息从此表单传送到“单个用户概要文件”表单的*用户类*列。			
谁是您的主要安全主管？ 谁是您的后备安全主管？			
概要文件名称	用户名称	类	注释

“用户组标识”表单

表 71. “用户组标识”表单

“用户组标识”表单	
准备人:	日期:

表 71. “用户组标识”表单 (续)

指示信息:

- 在“计划用户组”中了解此表单。
- 此表单帮助您标识具有类似的应用程序需要的用户组。
  1. 在表单的顶部列示您的主要应用程序。
  2. 在左侧列中列示您的用户。
  3. 标记每个用户所需要的应用程序。
- 您不必将此表单上的信息输入到系统中。

		对应用程序需要的访问权						
用户名称	部门	APP:	APP:	APP:	APP:	APP:	APP:	APP:

注:

- 如果您有一个*不严格的*安全性环境，则使用 **X** 来标记用户所需要的应用程序。
- 如果您具有*严格的*安全性环境，您可能需要使用 **C**（更改）和 **V**（查看）来指定*如何*使用应用程序。

“用户组描述”表单

表 72. “用户组描述”表单

“用户组描述”表单	第一部分（共两部分）
准备人:	日期:

第一部分的指示信息

- 在“计划用户组”中了解如何准备此表单。
- 在“设置用户安全性”中了解如何输入此表单。
- 为将使用该系统的每个组准备一个单独的表单。
- 使用“创建作业描述”（CRTJOBD）命令来创建组的作业描述。作业描述具有组的初始库列表。

组概要文件名称:

组的描述:

组的主要应用程序:

列示组所需要的其它应用程序:

列示组所需要的每个库。标记（✓）应该在组的初始库列表中的每个库:

注: 查看先前节中列示的每个应用程序的“应用程序描述”表单，以查出应用程序使用哪些库。

“用户组描述”表单		第二部分（共两部分）
“第二部分”的附加指示信息 • 下表列示出现在“创建用户概要文件”屏幕上的所有字段。字段分为两组：您需要进行选择的为一组，IBM 建议使用缺省值的为一组。 • 使用“使用用户概要文件”屏幕或“创建用户概要文件”（CRTUSRPRF）命令来将表单的此部分的信息输入到您的系统中。		
为组概要文件中的这些字段选择值:		
字段名称	**建议的选项**	**您的选择**
组概要文件名称（用户）		
密码	*NONE	
用户类（用户类型）	*USER	
当前库（缺省库）	*与组概要文件名称相同*	
要调用的初始程序（注册程序）		
初始程序库		
初始菜单（第一个菜单）		
初始菜单库		
限制能力（限制命令行使用）	*YES	
文本（用户描述）		
作业描述	*与组概要文件名称相同*	
作业描述库		
组概要文件名称（用户组）	*NONE	
打印设备（缺省打印机）		
输出队列	*DEV	
注：这些字段是以出现在“创建用户概要文件”屏幕上（使用 F4）的次序排列的。		
对以下字段使用系统提供的值（缺省值）：		
记帐代码	键盘缓冲	公共权限
辅助级别	语言标识	将密码设置为到期
辅助操作请求程序	限制设备会话	排序顺序
编码字符集标识	最大存储量	特权
国家或地区标识	消息队列	特殊环境
显示注册信息	密码到期时间间隔	状态
文档密码	优先级限制	用户选项
注：此列表中的字段按字母顺序排列。		

“单个用户概要文件”表单

表 73. “单个用户概要文件”表单

“单个用户概要文件”表单	
准备人:	日期:

表 73. “单个用户概要文件”表单 (续)

指示信息: • 在“计划单个用户概要文件”中了解如何准备此表单。 • 使用此表单来记录有关单个系统用户的信息。为系统上的每个用户组（组概要文件）填写一个表单。 • 对您想要对单个用户指定的任何附加字段使用右边的空白列。 • 在“设置单个用户”中了解如何输入此表单。						
组概要文件名称:						
创建的对象的所有者:			对创建的对象的组权限:			
组权限类型:						
对组的每个成员生成一项:						
用户概要文件	文本（描述）	用户类	限制能力			

“权限列表”表单

表 74. “权限列表”表单

“权限列表”表单					
准备人:			日期:		
指示信息 • 在“计划资源安全性”中了解此表单。 • 为每个权限列表准备一个表单。 • 使用该表单来列示列表、组和可以访问列表的单个用户所保护的对象。 • 在“设置资源安全性”中了解如何输入此表单。					
权限列表名称:					
描述:					
列示列表所保护的对象					
对象名称	对象类型	对象库	对象名称	对象类型	对象库

表 74. “权限列表”表单 (续)

列示可以访问该列表的组和用户					
组或用户	允许的访问类型	列表管理？	组或用户	允许的访问类型	列表管理？

“打印机输出队列和工作站安全性”表单

表 75. “打印机输出队列和工作站安全性”表单

“打印机输出队列和工作站安全性”表单				
准备人:		日期:		
指示信息 • 在“保护打印机输出”中了解此表单。 • 对于需要特殊保护的任何工作站和输出队列，在此表单上生成一项。 • 在“保护工作站”中了解如何输入此表单。				
列示受限制的输出队列的参数:				
输出队列名称	输出队列库	显示任何文件（DSPDTA）	检查权限（AUTCHK）	操作员控制（OPRCTL）
安全主管工作站: 如果您将安全主管限制于特定工作站（系统值 QLMTSECOFR 为是），则以下列示对安全主管和任何具有 *ALLOBJ 权限的人授权的工作站:				
以下列示受限制的工作站的权限:				
工作站名称	已授权（*CHANGE 权限）的组或用户			
注: 受限制的工作站应该具有设置为 *EXCLUDE 的公共权限。				

“应用程序安装”表单

表 76. “应用程序安装”表单

“应用程序安装”表单		第一部分（共两部分）
准备人:		日期:
指示信息 • 在“计划您的应用程序安装”中了解此表单。 • 为您将安装的每个应用程序准备一个表单。 • 使用此表单来计划您在装入应用程序后将如何建立对它们的所有权和公共权限。 • 在“设置资源安全性”中了解如何输入此表单。		
应用程序名称:		
描述:		
列示并解释安装应用程序必须创建的任何概要文件:		
库名称:		
	安装之前	安装之后
库所有者		
对象所有者		
库公共权限		
对象公共权限		
新对象的公共权限		
库名称:		
	安装之前	安装之后
库所有者		
对象所有者		
库公共权限		
对象公共权限		
新对象的公共权限		

“应用程序安装”表单		第二部分（共两部分）
库名称:		
	安装之前	安装之后
库所有者		
对象所有者		
库公共权限		
对象公共权限		
新对象的公共权限		
库名称:		
	安装之前	安装之后
库所有者		
对象所有者		
库公共权限		

对象公共权限		
新对象的公共权限		
库名称:		
	安装之前	安装之后
库所有者		
对象所有者		
库公共权限		
对象公共权限		
新对象的公共权限		

中国印刷