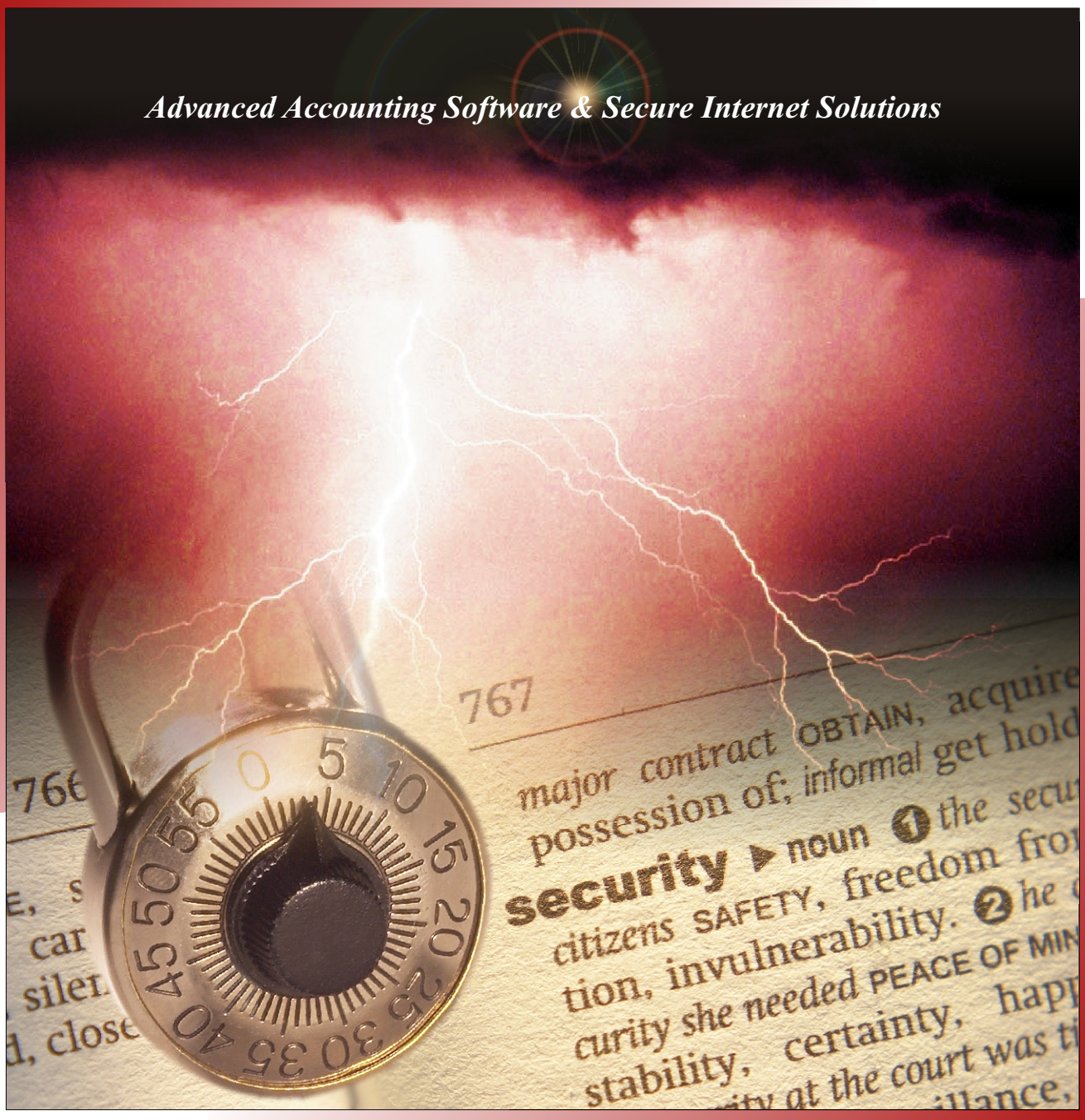
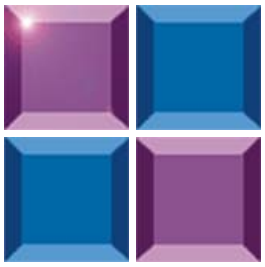
DATA PRO ACCOUNTING SOFTWARE, INC.



Advanced Security Administrator
Reference Manual



DATA PRO ACCOUNTING SOFTWARE, INC.

Advanced Accounting Software & Secure Internet Solutions

Version 7.3

This page intentionally left blank.

TABLE OF CONTENTS

Description	Page
CHAPTER 1 INTRODUCTION	*1-1*
SECURITY OBJECTS	**1-3**
AUTHORIZATIONS	**1-5**
USER LOGGING	**1-5**
SYSTEM INTEGRATION	**1-5**
DATA FILE DESCRIPTIONS	**1-6**
OVERVIEW OF A TYPICAL CONFIGURATION	**1-8**
System Manager	1-8
System Configuration	1-9
Creating, Updating & Enabling Company Rights	1-9
Set Up Groups	1-9
Special Groups	1-9
Set Up Users	1-12
Set Up Authorities	1-12
Force Password Change	1-13
CHAPTER 2 SET UP AND MAINTENANCE	*2-1*
SET UP USERS	**2-1**
To Access the Maintain Users Screen:	2-1
Inquiry Mode	2-3
Add Mode (SSA0100)	2-3
To Add a New Record:	2-3
To Set Option Rights:	2-9
To View Groups/Users that are Assigned to a Specific Option ID:	2-12
To View the Groups/Users which are Assigned to a Specific Option ID:	2-12
Change Mode (SSA0101)	2-13
To Modify a Record:	2-13
Delete Mode (SSA0102)	2-13
To Remove a User Profile From the System:	2-13
Copy Mode (SSA0103)	2-13
To Copy a Record:	2-14
SET UP GROUPS	**2-14**
Inquiry Mode	2-14
Add Mode (SSA0200)	2-15
To Add a New Record:	2-15
To Copy Rights from a Group:	2-21
Change Mode (SSA0201)	2-21
Change Mode (SSA0101)	2-21
To Modify a Record:	2-22
Delete Mode (SSA0202)	2-22
To Remove a Record from the System:	2-22
Copy Mode (SSA0203)	2-22
To Copy a Group Profile:	2-23
ASSIGN USERS TO GROUPS (SSA0600)	**2-23**
CREATE COMPANY RIGHTS (SSA0300)	**2-23**
To Create Company Rights:	2-23
UPDATE COMPANY RIGHTS (SSA0301)	**2-24**
DELETE COMPANY RIGHTS (SSA0302)	**2-25**
ENABLE COMPANY RIGHTS (SSA0303)	**2-25**
ADD AN AUTHORITY (SSA0700)	**2-26**
CHANGE AN AUTHORITY (SSA0701)	**2-27**
DELETE AN AUTHORITY (SSA0702)	**2-27**

TABLE OF CONTENTS (continued)

Description	Page
COPY AN AUTHORITY (SSA0703)	**2-28**
REPLACE AN AUTHORITY (SSA0704)	**2-30**
ENABLE AN AUTHORITY (ssa0705)	**2-31**
FORCE PASSWORD CHANGE (SSA0601)	**2-33**
SECURITY CONFIGURATION (SSA0400)	**2-33**
MAINTAIN DATA FILES (SSA0401)	**2-37**
MAKE COMPLETE DATA BACKUPS	**2-38**
CHAPTER 3 ERROR CODES	***3-1***
CHAPTER 4 PRINT REPORTS	***4-1***
STANDARD FEATURES FOR REPORTS	**4-1**
CTRL + O (Output Options)	4-1
Range of Accounts	4-2
Data Record Retrieval	4-2
Cancel the Print Job	4-2
PRINT USERS (ssa0104)	**4-2**
PRINT A GROUP (ssa0204)	**4-4**
PRINT AN AUTHORITY (ssa0706)	**4-6**
LIST LOGGED-IN USERS (ssa0610)	**4-8**
PRINT ACTIVITY LOG (ssa0615)	**4-10**
INDEX	***1***

CHAPTER 1 INTRODUCTION

This chapter will cover the general concepts of the **Advanced Security Administration** module. This program is designed to provide control and tracking of users accessing the **Infinity POWER** programs. It allows a ***"System Manager"*** to identify and control access to the programs, menu options and other special system features by user, by group and by company.

The features included here should not be confused with the **"Standard Security"** feature that is also included with all versions of **Infinity POWER** starting with **Version 6.5** and higher. It is also the only version of security available for the **Infinity POWER Small Business Solution**. This is a completely different type of implementation all together. If you simply desire to place a password on the main menu to keep unwanted users out of your accounting software, then, you may just want to implement the **"Standard Security"** option during the installation of your software or by running **Winstall** for **Windows Graphical User Interface** users, or **installpwr** for **UNIX/Linux Character-based** users.

"Standard Security" will provide all users **COMPLETE** access to all installed accounting modules and options within each accounting module. Therefore, if you want to provide any other levels of restrictions, then the use of the **Advanced Security Administrator** is **REQUIRED**.

NOTE

The Small Business Solution System Administrator version operates in Standard Security mode only.

The **Advanced Security Administrator** is an advanced security program designed primarily for multi-user environments, where users' activities and access to specific accounting options are of a highly sensitive nature and must be monitored and closely controlled. The system comes with a broad range of flexibility to allow users the ability to configure the system as tightly as they desire. However, in doing so, do not lose track of the need to make the system usable by those who operate the software each and every day.

Too many passwords or layers of required authorizations can be very distracting and annoying. Therefore, great care should be taken up front to analyze each user's processing requirements before you start your security implementation.

To better deal with the advanced concepts covered with this product, a quick overview of concepts may help simplify your view of the accounting system. First, the **Infinity POWER** product line is composed of a wide range of accounting applications which include over fifteen **(15)** variations of accounting software products. Therefore, when we refer to your system, we are referring to the combination of accounting modules you have purchased and installed on your computer system.

Forget that your actual computer system may either be a stand alone Windows PC, a Local Area Network **(LAN)** or a multi-user system running under **UNIX/Linux**. Regardless of the operating system platform, all **Infinity POWER** accounting software products are designed to work in the same way.

NOTE

The Small Business Solution System Administrator version operates in Windows platform only.

Within each accounting software program, several different accounting **"options"** exist. These options perform specific and varying functions within each accounting software program. They all combine together, however, to make up the overall system. Each accounting menu option is tracked by what we call its **"Option ID."** The Option ID allows the system to know specifically which exact accounting option you want to run.

For instance, if you wish to make a journal entry in your General Ledger program, you would go through a series of menu options until you found the option, ***"Record Journal Entries."*** From the system's point of view, however, you have chosen **"Option ID GL0101."**

The significance of this concept is that by using this advanced security program, the **"System Manager"** will have the ability to include or exclude certain users from all options within a module, such as General Ledger. This would go all the way down to a specific **"Option ID"** such as ***"Recording a Journal Entry."***

Therefore, you may create a very specific and detailed set of security provisions or a very simple level, depending on your specific security needs. Only you can decide which level is right for you. However, this manual will try to point out as we go, some of the problems that can be generated when you make certain decisions on security and how they will impact your firm.

As we've mentioned so far, the **Advanced Security Administrator** module allows a high level of security control to be placed on the access to the **Infinity POWER** programs and thus, your accounting data files. The **Advanced Security Administrator** allows an individual, whom we will identify as the ***"System Manager,"*** to control access to the accounting programs by user, by groups of users and on a company by company basis for those firms who process more than one set of accounting data files ***(multi-company processing)***.

The **"System Manager"** can be the owner of a company, an MIS staff member, the head of accounting, or a third party installer or consultant for your firm. The key is that they alone will be responsible for implementing the level of security you desire for your firm. This individual functions in much the same way as the System Administrator would for any **UNIX/Linux** or Local Area Network system. They are responsible for the set up and maintenance of the system and required to keep it working properly on an on-going basis.

Therefore, make sure that whomever this position is assigned to, is readily available should something happen to your system that would require their level of security and access to correct. The **Advanced Security Administrator** module provides access to a single **"super user"** who will literally have access to all accounting options throughout all accounting modules ***(i.e., System Manager)***. This user will also have all override capability for all other users.

This is the highest level of security access that an individual can have within the software. Make sure this password is secure and available to only those that management deems necessary. Just like any other high level security system, the **Advanced Security Administrator** module provides for the setup of both individual users and groups of users. This provides a high level of flexibility in the way the system can be configured on a user by user basis.

Each user can be assigned a unique set of access rights to various system options or a user may be a member of one or more groups having rights to these options. Separate sets of access rights for groups and users may be maintained on a company by company basis. Alternatively, the ***System Manager*** may choose not to maintain rights by company, but to maintain a set of **"default rights"** that applies to all companies being processed on the system.

The ***System Manager*** will use a specific **"User ID"** that allows him or her access to all **Infinity POWER** accounting software options. This ***"special"*** User ID is called **SYSADM**. It is created automatically when the **Advanced Security Administrator** module is installed.

At the time of installation, the ***System Manager*** **should** define a password for the **SYSADM** User ID. It is very important to write down and remember this password. Failure to remember the **SYSADM** password will cause the system to be inaccessible in a supervisory capacity. Plus, if no other users have been setup by the time it is discovered that the **SYSADM** password is forgotten, no one will be able to access the programs. Therefore, as a business owner, it is highly advisable to make sure that you also have this password, even if you are not the ***System Manager*** of the system.

If the **SYSADM** password is lost or forgotten, the **Security Files (Advanced or Standard)** in the **DPSS** directory must be removed and completely reinstalled and configured from scratch. This may be accomplished by using the **Data Pro Infinity POWER Installation Wizard (Winstall.exe)** which may be run from the accounting server's Program Menu Bar. In other words, ***DO NOT LOSE THIS PASSWORD!!!*** Data Pro Technical Support cannot assist your firm in recovering this information. Configuring security systems is time consuming and requires serious thought process and losing this key information is expensive to any organization and will cause down time for your company.

Without the security system in place, no user will be able to access the programs. For instance, the security system data files are stored in a directory under the program directory called **"DPSS"** ***(i.e., POWER\DPSS)***. On either network or **UNIX/Linux** systems, these directories must have full **"read/write"** user rights for all users who will be entering the **Infinity POWER** programs. Therefore, these same users could possibly have access to these directories at the operating system level, unless other security provisions are made at that level as well.

By deleting the security files stored in this directory, all security implementation would be removed from the **Infinity POWER** programs. However, no one, including the System Manager would be able to get into the accounting software. This would be the equivalent of not remembering the **SYSADM** password and not having any other users defined in the system. No one will be able to get in.

That is why the **SYSADM** password and safely storing the **System Administrator** and **Advanced Security Administrator** program CD is so important. In either case, the software will need to be re-installed so that access may once again be gained to the accounting software programs and your data files.

SECURITY OBJECTS

There are three types of **"security objects"** that may be guarded by access rights. The first, a **"standard object,"** is as simple as a menu option, such as ***"Record a Journal Entry."*** The second, a **"custom object,"** may be a specific window within a program, a data field, or any other specific area of the system for which security access is explicitly built into the system. This section does not apply to the Small Business Solution System Administrator version since only operates in Standard Security mode.

NOTE

See the ***Security Objects Definitions Reference Manual*** found in your ***System Administrator User Manual*** for a listing of security objects by module and their definitions.

The third object is a **"system object."** It is similar to a **"custom object"** except that it deals with features that will be controlled on a system wide basis, not by module. There are currently two choices of system objects. These are the options to ***"Execute DOS or UNIX Commands"*** and ***"Session Backup/Restore."***

You may or may not provide access to these options for a user or a group of users, but whatever your configuration, they are invoked system wide. Therefore, if you do not want any of the accounting users to have access to the operating system, you may control their access with these two options. All **"custom"** and **"system"** objects are created by Data Pro Accounting Software and are included standard within the programs. No method other than **"custom programming"** exists to add additional custom or security objects to the accounting modules.

A good example of a **"Custom Object"** would be the ***"On-Line Inquiries"*** and ***"Quick Add"*** features found by pressing the **F1** key throughout most accounting modules in the Character-based version of the products ***(Windows or UNIX/Linux)***. These are the options always found on the right side of this overlay screen. Any **"system"** objects would be found on the left side of this overlay screen. These have been defined so that the ***System Manager*** may control, within each accounting module, which user or groups of users can have access to these features. Therefore, you may want a user to have the ability to perform Inventory and/or Customer **"Inquiries"** during Sales Order Entry, but you may not want them to have the ability to **"add"** new inventory items or customers on-line.

Controlling these **"custom objects"** would be the responsibility of the ***System Manager*** in his definition of rights for users and/or user groups. If you feel you would like additional **"custom"** or **"system"** objects added to your system, please contact our **Technical Support Department** at **(727) 803-1550** for a custom programming price quotation.

AUTHORIZATIONS

Each **"security object"** that can be assigned to a user or a group of users may also be specified as requiring an ***"Authorization."*** This is the equivalent to a manager override feature. For instance, you may want to provide access to a specific menu option in Point of Sale to most sales representatives. However, you don't want them accessing the option unless a manager is around to oversee their functions.

NOTE

The Small Business Solution System Administrator version operates in Standard Security mode only.

As ***System Manager***, this is where you would provide access to the option or security object, but would also specify that an **"authorization"** is required as well. Therefore, until someone else who has full access to this option **"logs in"** to the system at this point in the program, no further access to this option or security object will be provided. In this scenario, if a user has access rights to a security object and authorization is required, the system will prompt the user for a User ID and Password to gain access to this option.

USER LOGGING

Additional control over security is provided by enabling the **"User Logging"** feature. When this feature is enabled, the system records user activity information to a **"log file."** Three levels of increasingly detailed logging information is available. This includes user login and logout information, login attempts / failures and a user option and feature use report. This information is available in a printed report format. At periodic intervals, the ***System Manager*** may choose to purge this log file to free up additional disk space.

NOTE

Once the **Advanced Security Administrator** module is enabled, it applies to **ALL** users logging into the **Infinity POWER** system. All users must be set up with user ID's and Password's so that they may access the system. Please refer to the ***Installation Guide*** for information regarding the installation procedure for the **Advanced Security Administrator**.

SYSTEM INTEGRATION

The **Advanced Security Administrator** module integrates with all **Infinity POWER** modules. No additional steps are required to create integration with any other module. This is handled automatically by the system.

If, at a later point in time, you install additional accounting modules to your system, it will be necessary to run the options ***"Update Company Rights"*** and ***"Enable Company Rights"*** respectively. These options will tell the system to re-check what has been loaded on your computer system and to provide access in the **Advanced Security Administrator** module to these options.

For users that do processing for more than one company ***(i.e., multi-company processing)*** a key system integration feature should be considered here. First, do all accounting users on your system need access to all data files on the system? Second, if they do, do they need equal access to the same features across companies? Depending on how you answer these questions, you would want to configure your security system differently. When you set up the security options for each company, you have the ability to define a default company or not.

If you choose to do so and designate one of your companies to represent the **"master"** for security definitions, then regardless of how many other companies you process in, no other set up of security features will be required. In other words, if you are processing for five different companies and you define **Company #1** as the default, any security changes you make in **Company #1** will automatically affect **Companies #2 through #5** as well.

If, on the other hand, you do not want the same security levels and access to all users across all companies, then you would leave this feature **"blank."** This will tell the system that security definitions will be done on a **"company by company"** basis instead. Therefore, if you want to make any changes to user access to various options, you will have to make it several times in all companies accordingly.

This is similar to the implementation of user groups versus the set up of individual users. **"Groups,"** represent the **minimum** level of access that a single user within that group will have throughout the system. This means that regardless of whom you are, if you belong to a **"group"** and it has access to specific options, these options cannot be taken away at the individual level.

Additional access can be provided to individuals regardless of the groups they are members of, but **"groups"** establish the minimum level of access for all users in the group. The similarity comes in the form of how much work is required by the ***System Manager*** to make changes at a **"group"** level versus a **"user"** level.

If you have created two groups for instance, Sales and Accounting, and have fifty users in each group, try to determine whether it would be easier to allow access to five new options at a group level or allow access fifty times at a user level. Once a change to access is made at a group level, all users who are members of that group immediately have full access to the new options without any further set up required.

Therefore, the same consideration should be made in terms of system integration across all companies. You should look at the overall scheme of things and determine whether it makes more sense to change security on a company by company basis or to make changes to one default company that is then the example company for all others.

All of the variations discussed here are possible within the **Advanced Security Administrator** module. These parameters are featured here for the ***System Manager*** to consider before creating a maintenance nightmare that could take lots of unnecessary time later on to keep up with.

DATA FILE DESCRIPTIONS

The **Advanced Security Administrator** module creates and utilizes several data files. A description of the information contained in each file and its naming structure is described in the following table.

File Type	File Name(s)	Description
Security Configuration	**SYSSS0.dbf**	This file contains certain configuration information, such as your activity logging, password control, login control and access rights information.
User File	**SYSSS1.dbf** and **SYSSS1.mdx**	This file contains general information for each user. This includes description, password (encrypted), user number, enabling parameter, login and logout time, last password change date/time and next password change date and time.
Group File	**SYSSS2.dbf** and **SYSSS2.mdx**	This file contains general information for each group. This includes description, group number, and enabling parameter.
Group/User Assignment File	**SYSSS3.dbf and SYSSS3.mdx**	This file contains information regarding the user/group assignments.
Permissions File	**coSS4.dbf and coSS4.mdx**	This file contains all the access right information and authority information for each user and group by security object. The content of this file is based on what modules were installed and any additional custom security objects loaded with the Advanced Security Administrator. There is one permission file created for each company, unless a default company is being used as the master controlling company of security.

File Type	File Name(s)	Description
Authority File	**SYSSS5.dbf and SYSSS5.mdx**	This file contains all of the authority information for each option by company and by user. If an option requires an authorization, this file determines which user or users are authorized to approve access to the option.
Company Directory File	**SYSSS6.dbf and SYSSS6.mdx**	This file contains general information about those companies for which rights are secured.
Control File	**SYSSS7.ACL**	This file contains the status of activated security levels, information on users logged into the system and also determines User ID numbers and Group numbers to be assigned.
Activity Log File	**SYSSS8.dbf and SYSSS8.mdx**	This file contains all activity for all users and groups based on the level of activity selected in the System Configuration.
Custom Object File	**SYSSS9.dbf and SYSSS9.mdx**	This file contains any custom security objects that have been predefined in the system.

All of these files reside in the specified path given at the time of installation ***(not the data path)***, as they are considered security control files. Normally, the default path for these files would be **\POWER\DPSS** unless you specified a custom program directory name during installation. Whatever you specified would then be followed by **\DPSS**.

If you are installing two sets of the accounting software programs on either two local area networks or a Windows network and a **UNIX/Linux** server, you will want to install first the version of products that will ultimately be the location of the security control data files. In a **Multi-Platform** environment, for instance, it would be normal to have a **UNIX/Linux** version of the products installed on a **UNIX/Linux** server. This means that all **UNIX/Linux** users could use their dumb terminals and PC workstations as desired. They would all be using the **UNIX/Linux** version of the products to perform their normal accounting functions.

NOTE

The Small Business Solution System Administrator version only operates in a Windows platform.

You would then have the Windows versions ***(Graphical or Character-based)*** of the products call the **UNIX/Linux** server data file path for storage of all the accounting data files to be used by both versions of the products. Therefore, the Windows users would use the Windows versions of the accounting products, although the data is actually being stored not on the network, but a **UNIX/Linux** server.

Through the use of ***TCP/IP*** and ***NFS*** gateways **(i.e. Samba)**, a **UNIX/Linux** server can be ***"mounted"*** just like any other hard drive on a local area network. To the user, this mounted drive is transparent. It looks just like another network drive. In fact, because of ***Infinity POWER's*** unique ***"binary file compatibility"*** data files can literally be copied from one operating system to another without any data file conversions. In other words, accounting data files generated under **UNIX/Linux** can be copied to the local area network and then immediately processed by the **Windows GUI** or **Character-based** versions of the products without any further steps and vice versa.

Once the initial set of security files has been established on the first server ***(network or UNIX/Linux)***, the second installation may then call the original installation to utilize the same security data file path across both servers. Only during the second installation can you override the default placement of the security system data files. If you attempt to install the security files in a location where there are no previous set of installed security files, you will get an error message during the installation.

With the previous version already installed, however, you may then choose the override and tell the system to call the other mounted drive and use the other installations security file path. Therefore, during your normal backup procedures, you should make certain to backup the ***Advanced Security Administrator*** files ***after*** you have completed your set up.

These files are not backed up by the Session Backup/Restore utility options found within the program. These options only back up data files. Therefore, the more complex your security set up and definitions are, the more a separate backup on a frequent basis is required. Many of the security configuration files will be fairly large in size and will need to utilize either a tape backup or some kind of ***"zipped"*** or compressed backup utility to store them to floppy disks.

The field names and data in the following **Advanced Security Administrator** data files are encrypted. Therefore, access to these files is unavailable through a third party programming utility product.

SYSSS0.DBF
SYSSS1.DBF
SYSSS7.DBF

OVERVIEW OF A TYPICAL CONFIGURATION

This section will cover the recommended steps in configuring the **Advanced Security Administrator** module. Included are guidelines that summarize the procedures involved in getting your security system up and running. Once the **Advanced Security Administrator** has been installed through the **Infinity POWER** installation routines, there are several items which you will need to plan out so that your security system is structured correctly.

These items of consideration are discussed in detail below.

System Manager

Before anyone can work on the **Infinity POWER** system, a ***System Manager*** must be designated to set up and configure the **Advanced Security Administrator** module. During the installation routine, the **"SYSADM"** User ID is established automatically. The **"User ID"** is a record which identifies a person logging into the system. The **"SYSADM"** User ID is specifically designed for the ***System Manager***.

All User ID's are supplemented with an optional password. The password must be at least seven **(7)** characters in length. The password must contain at least three **(3)** alpha characters and at least two **(2)** numeric characters. **Passwords** are **"case sensitive."** Case sensitive means the system recognizes the difference between upper and lower case characters. **User ID's** are **not** case sensitive.

The person performing the installation ***(System Manager)*** can enter a password for the **SYSADM** User ID. The **SYSADM** will have all access rights ***(privileges)*** to all menu options and any custom objects added to the system. Therefore, it is highly recommended that a password be installed at this point.

For additional information on the installation routine, refer to the **Infinity POWER** ***Installation Guide***.

System Configuration

Once the **Advanced Security Administrator** module is enabled through the installation routine, you will need to log into the **Infinity POWER** system as the **SYSADM**. The ***System Manager*** will be responsible for the set up of the System Configuration, creation and enabling of the Company Rights and maintenance of the User ID's, Groups and Authorities.

First, the set up of the System Configuration is required so that you can define the parameters of usage for the **Advanced Security Administrator** module.

Creating, Updating & Enabling Company Rights

Once the Security Configuration is complete, the next step is to **"Create Company Rights."** This option will use the system database of all security objects for all modules installed on your system to create the **"company rights"** file for the currently selected company. Each company will have an individual **Permissions File (coSS4.dbf)** in the assigned **Advanced Security Administrator** directory path.

The **"Update Company Rights"** option is used for updating a current set of permissions for a company. This option will allow you to update standard menu options, custom menus and custom security objects. For example, you may have added a new module to an existing **Infinity POWER** system.

You must **"Update Standard Menu Options"** so that they are recognized by the security system. Likewise, custom security objects will also need to be loaded and updated using the **"Update Custom Security Objects"** option. The **"Update Company Rights"** option also allows you to ***"Use Access Rights From Another Company."*** This will allow the ***System Manager*** to duplicate a permissions file from another company.

After the ***System Manager*** has established the company rights, you must **"Enable Company Rights"** before any users are allowed access.

Set Up Groups

It is recommended that users be put into groups for convenience. You can organize users into groups according to the information they need or tasks they perform. Groups can be added, changed, deleted and copied. Groups can be enabled and disabled any time by the ***System Manager***. For example, you may want to put all your sales staff in a group called **"SALES."** Then, when you want to assign access rights ***(privileges)*** to all the sales staff, you can use the **"group"** as a shortcut. Otherwise, if only User ID's were used, you would have to update each and every salesperson's User ID.

This may not be significant if there are only three sales representatives on your staff. However, if you have fifty, it's another story. It is also important to consider that certain groups of people might need access to certain files. For example, you may want all department managers to have access to the Employee Comments File in Payroll, to note comments about their employees periodically. You could do this very easily by creating a group called **"MANAGERS."**

Group set up allows the ***System Manager*** to define the access rights ***(privileges)*** for each individual menu option and custom object given to that group. It also allows for the assignment of **"Authorities"** on any menu option or custom object. Again, these **"authorities"** are equivalent to manager override capabilities. Therefore, although a user can access an option, they cannot complete the transaction until a user with a manager override capability logs in and allows them to proceed.

Special Groups

Depending on you how you have configured the Master Configuration, you may have a single company ***(the default company)*** controlling security rights and access for every company or your may have security implemented on a company by company basis. If you are processing just one set of books or one company, this is not relevant. However, if you are processing multiple companies, you may decide you want to have certain levels of control across every company, even if there are varying levels of setup by company.

For instance, you may only want the ***System Manager*** to be able to **"create new year's data files."** If you have five companies with ten different groups in each company with dozens of users in each group, and a lot of accounting modules, it could be a very time consuming task to restrict these rights in every accounting module. This is where the concept of two unique types of **"groups"** comes into play. As System Manager, you may create a special group that would transcend all companies and restrict specific access rights across all of the companies.

The first special group is called **_PERMALL**. It must include the underline as the first character in the name of the group. This tells the system that this group name is unique. The **_PERMALL** Group, when created ***(optionally)*** overrides access rights to all companies. This does not mean that they will have access to all options in every module, unless this level of access rights have been assigned to this specific group.

IMPORTANT NOTE

When upgrading your software to a new version, you must go into the **_PERMALL** group and grant or not grant rights to the new security objects after the upgrade is complete.

In other words, if your desire is to restrict only a few options in various accounting modules so that only the ***System Manager*** will have access, you would want to set the permissions to all options to be turned on. This would mean that all users would be able to access these options, unless they belong to another group as well that restricts access to other specific options. Then you would, on a module by module basis, turn off the access rights to those specific options you want to restrict. In doing so, all users, regardless of the company or group, and user access rights would not be allowed to access the specific Option ID's that have been restricted in the set up of this unique group.

Therefore, if you only wanted the ***System Manager*** to be able to **"Start New Year's Data Files,"** this would be the overriding control mechanism, regardless of how any other group is set up. If another group is set up called **"SALES"** for instance, although members of this group could be given rights to the option to start new year's data files, the fact that there is a **_PERMALL** group set up will supersede all other group setups.

All users set up in any company are automatically a member of the **_PERMALL** Group. Therefore, no other special set up is required. This is also an ideal way to create a very simplified security setup. If the objective is to restrict certain options in various modules and allow all users access to the remaining functions, then this can actually be the only **"group"** that needs to be set up.

The overall permissions flag will need to be turned on at the user set up level. Other than that, it's that simple. If other restrictions are desired, then other groups should be established. The **_PERMALL** group affects all companies that are set up on the system. Another similar type group can be set up to control access on a company by company basis. This group is called **_PERMCO**.

The **_PERMCO** group, when created ***(optionally)***, allows you to restrict certain access rights to a specific company only. All users are automatically a member of the **_PERMCO** group as well. This group can dictate which options are to be denied access globally in a specific company. A good example would be where during the year end closing procedures you want to temporarily disable transaction options to all users for the company you are closing. This allows you to temporarily restrict ***(or override)*** access rights without changing the users' and groups' access rights.

IMPORTANT NOTE

When upgrading your software to a new version, you must go into the **_PERMCO** group and grant or not grant rights to the new companies when the upgrade is complete.

Unlike the normal group and user access rights where there is a minimum level of access ***(i.e., if the user or any group the user belongs to has access, access is allowed)***, disabling access in the **_PERMALL** and **_PERMCO** cancels ***(overrides)*** any other access rights. Another good example of using a **_PERMCO** group would be where a business owner is running several companies. In addition to the businesses, he or she is running their personal accounting on the system as well.

Where the business owner may have an accounting department to run the financial data of the companies, they may not want the same staff members having access to their personal data files. Instead of using a **_PERMALL** group which would restrict access in every company, the **_PERMCO** group would allow full access in all companies except the company where the **_PERMCO** group is established.

In this case, the **_PERMCO** group would be set up uniquely in the owner's personal data files. Therefore, he or she would not have to worry about restricting access to the other staff members doing their daily functions, but can restrict access in a unique company. The business owner would have to login to their personal company as **SYSADM** to perform this function, since this would be the only user to have access to this company.

Like the **_PERMALL** group, the **_PERMCO** group's rights supersede the set up of any other groups on the system. Therefore, from a hierarchial point of view, **_PERMALL** is the highest level of control, then **_PERMCO**, then all other groups, and then unique definitions by user.

Set Up Users

There are several different types of users that will be set up on the security system. Some users may have access rights to all options, whereas, others may only have access to a few options. Users can be added, changed, deleted and copied. Users can also be enabled and disabled at any time by the ***System Manager***.

You will have normal users, users that have **"Authority"** privileges and you will have the ***System Manager* (SYSADM)** which controls and manages the entire security system. Users can be assigned to multiple groups, therefore having access to all the options defined in each of those groups. Users can also have their own access rights assigned.

For example, a specific User ID called **TOM** is a member of the **ADMIN** group. This group does not have access to the Accounts Payable data files. Although **TOM** is a member of **ADMIN**, we could go to his unique set up as a user and provide him access to specific Accounts Payable options.

Therefore, if we wanted him to be able to use the option ***"Voucher Vendor Invoices"*** in Accounts Payable, this can be established without providing him any other access rights in the Accounts Payable program.

Users can be given additional rights that groups that they belong to do not have. In Tom's case, we provided him an additional access that all of the other members of **ADMIN** do not have. However, it does not work the other way around. If **ADMIN** had full access to **ALL** Accounts Payable options, we could not restrict Tom's access to the option ***"Voucher Vendor's Invoices."*** This is because the group he belongs to has access. As a member, he will have full access. A group's rights represent a user's minimum level of rights, not their maximum. This must be considered when creating security access levels throughout the system.

Set Up Authorities

"Authorities" are users who have been given additional privileges. These privileges include having the **"Authority"** to allow access to menu options or custom objects where other **"normal"** users to do not have access. Authorities can be added, changed, deleted, copied and replaced. Authorities can also be enabled and disabled at any time by the ***System Manager***.

For example, the Advanced Point of Sale module may be set up to allow access to the option ***"Record a Refund,"*** to all the cashiers. However, by turning **"on"** the **"Authority"** for that specific menu option, another User ID who has been defined as the authority for this option must login to allow the cashier to proceed. This is very similar to what would be considered a **"manager override."**

When an **"Authority"** is created, you will define the User ID, the system and the Option ID. Ironically, when authorities are assigned to specific users, the user acting as the authority does not have to have permissions to the option to be able to have the authority or manager override on the option. You must be careful in how you set up authorities. If you specify you want authorities on all options, this means that every time someone wants to process any option that a manager override must occur. This would be very cumbersome. Therefore, when a user setup is defined, normally no authorities should be flagged overall and only the exception options should be designated.

Force Password Change

This option will allow the ***System Manager*** to force a password change on all users the next time they access the system. This particular option overrides the password interval aging, however, it does not change the password interval's status. The **"Force Password Change"** is over and above the regular password aging interval.

This option may be enforced after the System Manager initially sets up the Advanced Security Administrator module. This will give each User ID the opportunity to assign his/her own password.

CHAPTER 2 SET UP AND MAINTENANCE

This section discusses the procedures involved in the set up and maintenance of the **Advanced Security Administrator** module. All sections of this chapter and **Chapter 1** should be read before attempting to set up the security options. This section will cover in detail all of the Set Up and Maintenance menu options.

SET UP USERS

This section discusses the ways to add, change, delete and copy **"Users"** in the **Advanced Security Administrator** module. It also covers how to assign these **"users"** to **"groups,"** if you decide to set up **"groups"** within the security system. There is also a report function that will enable you to print and verify all information input into this option for each user. This section reflects the Advanced Security Administration module functions.

To Access the Maintain Users Screen:

1. In the Advanced Security Administrator module, <click> the **Set Up and Maintenance** main menu option.
2. <Click> the **Set Up Users** menu option. The Maintain Users screen displays.

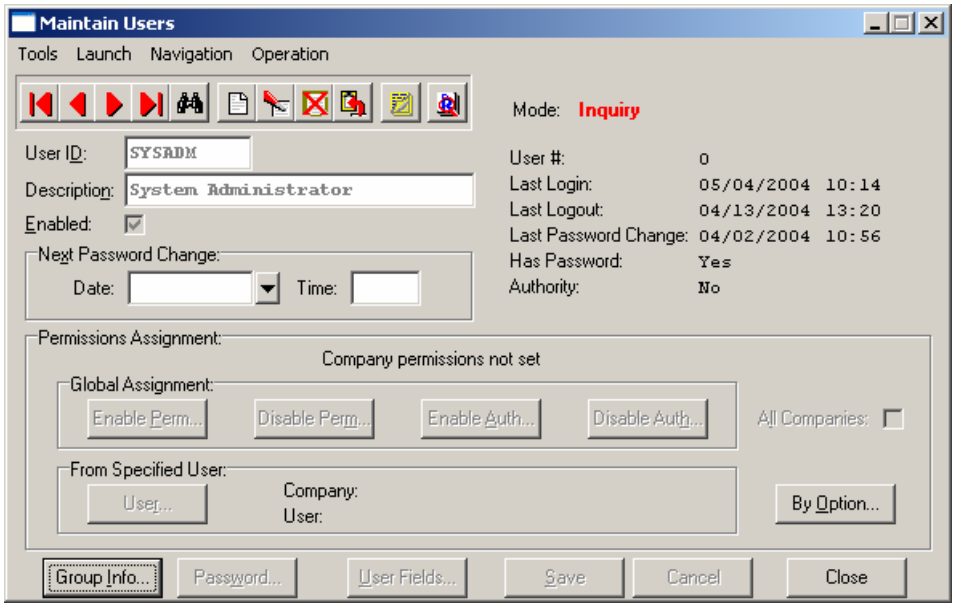


Figure 2-1. Maintain Users Window

Inquiry Mode

The **"Inquiry"** mode allows you to view various summary information about the users set up in the Security System.

1. Navigate to the record you wish to view. You may find a record using the navigation tool bar or <click> on the **Navigation** option on the Menu Bar and then the appropriate navigation option.
2. Once a user has appeared on the screen, <click> on the following keys to view important information. <Click> the **Group Info** button to review information about the group or groups this user belongs to. Once a group has appeared on the screen, <click> the **By Option** button to review the rights given to each individual module for this group.

> **NOTE**
>
> When accessing the **By Option** button, you will enter a file system that you wish to view. The screen provides the option to view the first detail record, page up the detail list, page down the detail list, view the last record in the detail list, view a specific detail record based on text or view a specific detail record based on a line number.

3. When you select to view by either a record based on text or a record based on a line number, enter the appropriate information ***(either text or a line number)*** and <click> the **OK** button.

Add Mode (SSA0100)

This mode allows you to set up new users in the **Advanced Security Administrator** module. This option should not be performed until the company has been set up and Company Rights have been created or updated and enabled.

This option is used to set up new users and define the specific access rights for those users. These access rights include passwords, permissions, authorizations and group information. It is recommended that **"groups"** be set up and utilized whenever possible. Using groups will simplify later administration and maintenance in regards to rights assigned by group vs. rights assigned by individual User ID. Each group will dictate the minimum level of access rights ***(privileges)*** available to the users assigned to that group.

When a user has had permissions **"enabled"** to access specific options, either by defining them on the actual User ID or a group in which the User ID has been assigned, the user will have access to these options. For instance, a User ID may be set up having no access rights to any option. If this User ID is assigned to a group which has access rights to a variety of options, they will have access to these specified options, even though their User ID is set to not have access to these specified options.

To Add a New Record:

1. <Click> on the **Add a New Record** button or select the **Operation** option from the Menu Bar and select the **Add** sub-menu option. A screen displays with the following data items.

The following table describes the Maintain Users screen details:

Data Item	Description
User ID	Ten **(10)** character *(alpha/numeric)* field which will be used to identify each individual user as they log into the system.
Description	This is a thirty (**30**) character *(alpha/numeric)* description of the user which is being added. This description will display on selection screens, maintenance and activity reports.
Enabled	This data item is used by the ***System Manager*** to manage the enabling or disabling of this particular User ID. If this data item is <clicked> **"on,"** the **Advanced Security Administrator** will allow the login of this User ID. If the User ID and Password entered during the login procedure are not valid, you are given additional attempts to log in, based on the **"number of login attempts"** you have set up in the Security Configuration. If this data item is left blank, and this User ID is used to log into the **Infinity POWER** system, they will receive the error message, **"User login disabled."** This feature can be used by the ***System Manager*** as a control tool to quickly remove access to the system for any single user. If the user is already logged into the system, this will not remove them from the system, but will prevent their access in the future. This is particularly useful in situations where an employee may be terminated and the ***System Manager*** does not have the time to manually remove that user from all groups in which they may be a member.
Next Password Change Date	This data item is dictated based on options set up in the Security Configuration. If you have chosen to require passwords during the login procedure and have the **"password aging"** enabled, the **"password aging interval"** will define the Password Change Date. The Password Change Date can be over written manually if you choose to set a specific date. Once a date has expired, the system will reset the Password Change Date based on the aging interval defined in the Security Configuration. If the password control is not enabled in the Security Configuration, you will not have access to this data item.
Next Password Change Time	This data item is dictated based on options set up in the Security Configuration. If you have chosen to require passwords during the login procedure and have the **"password aging"** enabled, the **"password aging interval"** will define the Password Change Time. The **Password Change Time** can be overwritten manually if you choose to set a specific time. Once a time has expired, the system will reset the Password Change Time based on the aging interval defined in the Security Configuration. If the password control is not enabled in the Security Configuration, you will not have access to this data item.

The next four data items deal with setting permissions and authorities for a particular user. Keep in mind the concept behind these functions before answering these questions. First, these features are designed to allow or disallow access to specific menu options and custom security objects. See the ***Security Objects Definitions Reference Manual*** found in your ***System Administrator User Manual*** for a listing of security objects and their definitions.

These are done on a **"global"** basis for all accounting modules that you currently have installed on your system.

The rule of thumb to use with these next four options is the amount of control or changes that you want to apply to a particular user. In other words, are you trying to limit access to a few options and provide access to the other **95%** of the system? Or, are you trying to keep the user out of almost everything and provide them access to **5%** of the options in the system?

The same considerations should be taken when you set up user groups. Plus, if user groups have already been set up with the appropriate rights for a user, no additional effort has to be made in this section. The group assignments will prevail automatically once a user has been assigned to a group or multiple groups. A group provides each user its minimum level of access to specific programs or all programs. Therefore, if you have set up a group that provides access to every option in every module, you cannot take that access away from any user in that group.

If this is not what you want to do, then set up groups with less rights and add more access for this user by using the ***"By Option"*** button on this screen. This data item will provide you the ability to turn on and off access to specific menu options and custom security objects on a module by module basis. These next four options are for complete global set up of all features. Therefore, answering ***(Y)***es on ***"Enable Perm"*** will set the default access for this user to allow access to every option in every module.

If you only want to secure a few options, this is what you would want to do. If you only want to allow access to a few options, you would answer ***(N)***o. In either case, you will be defining for the ***System Manager*** how much additional effort will be required to fine tune their access rights. The same concept works with ***"Authorities"*** as well. This feature works as a manager override option and again you must decide how much override requirements you want for a user on each and every option. Careful planning should be considered before implementing these features.

Keep in mind, a user does not have to belong to a group. Therefore, you may control each user on an individual basis if desired. However, as you deal with larger numbers of users who have similar computing needs, you will find the implementation and control of groups is significantly easier on the ***System Manager.***

Data Item	Description
Enable Perm	This is a **(Y)**es or **(N)**o question which allows the System Manager to set this user's global access to all options for all accounting systems ***(menu options and custom security objects)***. When a user has had permissions **"enabled"** to access specific options, either by defining them on the actual User ID or a group in which the User ID has been assigned, the user will have access to these options. The **"By Option"** button on this screen will specifically allow you to make changes to rights on a module by module basis. This data item is setting a global default. Once rights have been modified in the **"By Option"** section, answering **(Y)**es to this prompt again now or later in the **"Change Mode"** option will supersede any customization that has occurred. Therefore, you must be careful in using this option so as not to override specific configurations made for this user.
Disable Perm	This is a **(Y)**es or **(N)**o question which allows the System Manager to set this user to be denied access to all options for all systems ***(menu options and custom security objects)***. When a User ID has had permissions **"disabled"** to access specific options, they will not have access to those options unless they have been assigned to a group that has **"enabled"** access rights to those same options.

Data Item	Description
	Keeping in context with the discussion in this section, if you want to allow only a limited amount of access to a user ***(the 5% access instead of 95%)***, you would answer **(Y)**es to this data item. You would then proceed to the **"By Option"** button to specifically set up the few options that you want a user to have access to. This data item is setting a global default. Once rights have been modified in the **"By Option"** section, answering **(Y)**es to this prompt again now or later in the **"Change Mode"** option will supersede any customization that has occurred. Therefore, you must be careful in using this option so as not to override specific configurations made for this user.
Enable Auth	This is a **(Y)**es or **(N)**o question which allows the System Manager to set the user to obtain authorization on all options for all systems (menu options and custom security objects). This will prompt the user for a User ID and Password which has authorization to access and proceed with the given option. Answering **(Y)**es to this data item will be telling the system that you will be requiring another user (manager override) to login and provide specific access each time this user wants to access a specific menu option or custom security object. Therefore, careful consideration should be made as to how many authorities will be required for a user. If you want to allow a user to use an option, but only after a manager has approved use of the option, you must first provide them permission to access the option. Once access rights to the option have been provided, an authority must be assigned to the same option. These data items work similar in concept to permissions. The question to consider is whether a user will require manager overrides on **5%** of the options they are using or **95%**. Based on this criteria, you would respond **(Y)**es or **(N)**o accordingly. This data item is setting a global default. Once authorities have been modified in the **"By Option"** section, answering **(Y)**es to this prompt again now or later in the **"Change Mode"** option will supersede any customization that has occurred. Therefore, you must be careful in using this option so as not to override specific configurations made for this user.
Disable Auth	This is a **(Y)**es or **(N)**o question which allows the System Manager to set this user to allow access to all options for all systems, without requiring authorization. If your desire is to allow a user access to the options without requiring a manager override, then you should answer **(Y)**es to this question. This data item is setting a global default. Once authorities have been modified in the **"By Option"** section, answering **(Y)**es to this prompt again now or later in the **"Change Mode"** option will supersede any customization that has occurred. Therefore, you must be careful in using this option so as not to override specific configurations made for this user.
Set All Companies	This question allows the System Manager to define whether or not access options specified in this User ID will be effective in all companies accessed by this User ID. This feature will only affect those company data files that have already had security rights setup at this point. If you **"add"** new companies in the future, you will be required to use the **"Update Company Rights"** feature to be able to enable access to those new companies by a user set up in this option. If you are performing multi-company processing, this is a key question. A business owner may want to allow specific users access to data in some companies and not in others. Therefore, you must consider this before granting full access to all companies with this option.

Data Item	Description
	If you leave this check box blank, then the System Manager will be required to press F4 to access the "Change a Company" feature and then set up the users for the other desired companies as well as the currently loaded company.
Permission Assignment From Specified User	By <clicking> on the **User** button, you will be prompted for a specific user from a specific company to copy rights from. This will copy all access right information from that specified User ID in that specified company. This option can be a real time saver if utilized properly. Even if some changes would be required to configure the new users rights specifically, getting most of the work done by using this copy function can save a great deal of time.
Password	This data item allows the System Manager to assign an initial password to the user being added. This password will be functional until the next scheduled password change date and time. The system will automatically request a new password at that scheduled time if the "password aging" is enabled in the Security Configuration. This data item is also used to issue a new password if the user forgets or loses their current password. You may set a new password at any time.
By Option	This allows the System Manager to define access rights by module and by individual menu option. This is the key option in defining specific rights for a user. On this screen, the system allows complete modification of access rights for an individual user. Keep in mind, if the user is a member of a group, the groups rights will prevail in terms of minimum rights. In other words, you will not be allowed to remove rights on this screen for options that have been granted access via a group. You may, however, grant additional access rights above and beyond those rights granted by a group.

To Set Option Rights:

1. <Click> the **By Option** button. The Option Rights Screen displays.

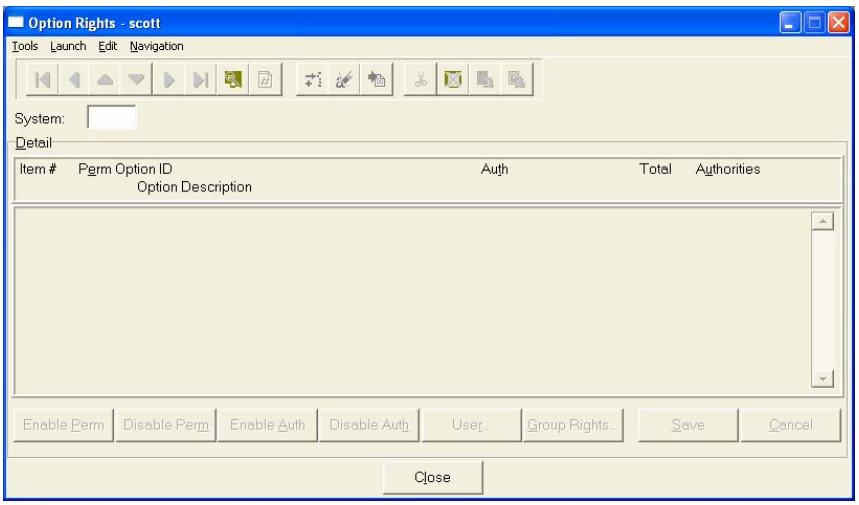


Figure 2-2. Option Rights Screen

The following table describes the Option Rights Screen details:

Data Item	Description
System	This data item requires the entry of a module identifier. This would represent the two or three character abbreviation of the accounting module you want to provide access changes to. For instance, if you want to call up General Ledger, then enter **"GL"** in this data item. **"AR"** would represent Accounts Receivable. The following list includes all of the possible choices. You cannot, however, provide access to modules that are not currently loaded on your system. **Sys ID** **Module Name** XX System Administrator SSA **S**ecurity System Administrator PT Productivity Tools GL General Ledger AP Accounts Payable PO Purchase Order Entry AR Accounts Receivable IM Manufacturing Inventory Management SO Sales Order Entry PS Point of Sale PR Payroll JC Job Cost Main Module CR Check Reconciliation TE Time Sheet Entry RW Report Writer RWR Report Writer (Run Time) FC POWER Upgrade Utility ME Menu Editing Tool FG Forms Generator Tool SD Customer Support Management SYS System (Global Functions) DPW System for Windows (GUI) (Global Functions) DPL NPC Direct Deposit
Enable Perm	This option sets the default permissions flag for all options that are available for the module selected on this screen. It will not affect any other module's configuration, only the system specified in data item #1. Answering **(Y)**es will make all permissions available for this user. Keep in mind, however, that group level access will always prevail, regardless of what you set up here by user. This data item and ***"Disable Permissions"*** work as a toggle for the default value for each option.

Data Item	Description
Disable Perm	This option sets the default permissions flag for all options that are available for the module selected on this screen. It will not affect any other module's configuration, only the system specified in data item #1. Answering **(Y)**es will make all permissions unavailable for this user. Keep in mind, however, that group level access will always prevail, regardless of what you set up here by user. This data item and ***"Enable Permissions"*** work as a toggle for the default value for each option.
Enable Auth	This option sets the default authorizations flag for all options that are available for the module selected on this screen. It will not affect any other module's configuration, only the system specified. Answering **(Y)**es will set all authorizations to be on for this user. Keep in mind, however, that group level authorizations will be displayed prior to entering any changes in this option. Changes made here will be in addition to those entries made at the group level. This data item and ***"Disable Authorizations"*** work as a toggle for the default value for each option.
Disable Auth	This option sets the default authorizations flag for all options that are available for the module selected on this screen. It will not affect any other module's configuration, only the system specified. Answering **(Y)**es will set all authorizations to be off for this user. Keep in mind, however, that group level authorizations will be displayed prior to entering any changes in this option. Changes made here will be in addition to those entries made at the group level. This data item and ***"Enable Authorizations"*** work as a toggle for the default value for each option.
User	By <clicking> on the **"User"** button, the Use Rights from User window displays and prompts you for a specific user from a specific company to copy rights from for this specific module or system. This will copy all access right information from that specified User ID from that specified company. This option can be a real time saver if utilized properly. Even if some changes would be required to configure the new users rights specifically, getting most of the work done by using this copy function can save a great deal of time.
Group Rights	Answering **(Y)**es to this prompt will generate an overlay screen that will show all of the groups that this user is a member of. It is a scrolling screen that you may use the up and down arrow keys to scroll through. When you are done viewing the groups, <click> on **"Cancel"** to exit. All of these data items are prompted from the left portion of the screen. On the right side of the screen, several fields of information will be displayed. They cannot be changed on this screen and are simply a summary of the configuration that currently exists. The fields of information that are displayed include the User #, whether Company Permissions have been set, Date and Time of last login for this user, Date and Time of last logout for this user, Date and Time of last Password change, status of whether the user has a password defined, and whether the user is an authority. As changes are made to this user's profile, these changes will automatically be updated on this screen. <Click> **"Save"** and you will be prompted to add another user. If you are done, <click> **"Cancel"** to exit to the menu.

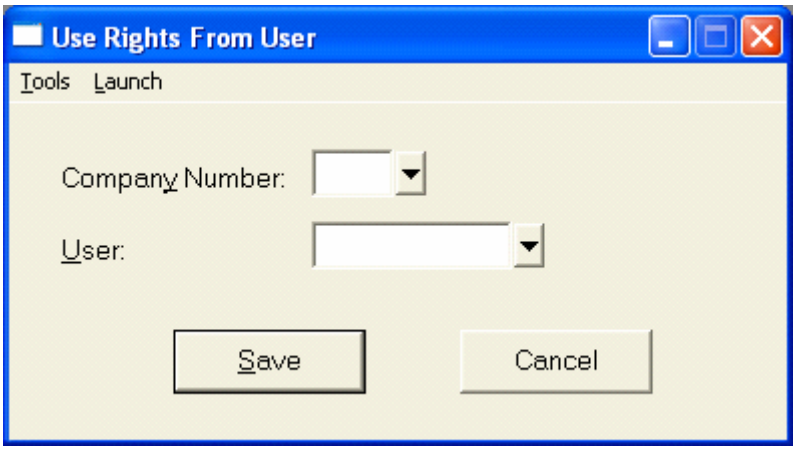


Figure 2-3. Use Rights From User Window

To View Groups/Users that are Assigned to a Specific Option ID:

This section displays all of the option ID's for the system loaded. On each line, the screen will display the Option ID, its description, the current status of Permissions, Authorizations, whether they are implemented at a group level and the total net affect on this menu option. You may use the up and down arrow keys to scroll through the list of available Option IDs. When you decide to change an Option ID, simply change each field to be set to your specifications.

Depending on how all of the flags have been setup at the group level, plus the overhead setup from the Security Configuration screen, the default values will be displayed. By <clicking> on the **"Authorities"** button, the system will display any authorities that have been assigned to any of these Option IDs.

The Select Authority window displays listing the users who have been given an **"authority"** or manager override for this specific Option ID.

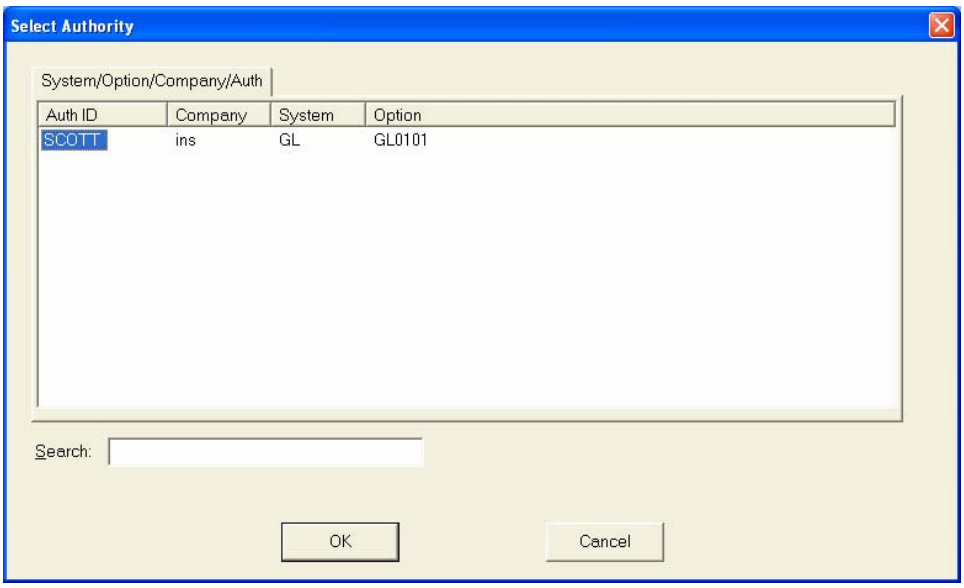


Figure 2-4. Select Authority Window

To View the Groups/Users which are Assigned to a Specific Option ID:

1. <Double-click>on the group or user in the **Auth ID** column next to the specific option listed or highlight the Auth ID.
2. <Click> the **OK** button. A Window will appear showing if the Authority is enabled or disabled.
3. <Click> the **Close** button to exit the screen.

OR

4. <Click> **Cancel** button to view other authority and group assignments by system.
5. Press the **ESC** key to exit when you are finished. You will be returned to the original editing screen for the setup of a user.
6. Complete any desired changes then <click> the **Save** button to save all of your changes, or <click> the **Cancel** button to exit without saving any changes.

Change Mode (SSA0101)

This mode allows you to change a user profile, including user access rights. By selecting this option, you have the ability to make changes to a user's profile, including the definition of their specific user rights. Keep in mind that group access rights will always establish the minimum rights provided to a user. Therefore, rights assigned at a group level cannot be removed by this option.

To Modify a Record:

1. Navigate to the record you wish to change. You may find a record using the navigation tool bar or <click> on the **Navigation** option on the Menu Bar and then the appropriate navigation option.
2. If you are changing a record, <click> on the **Modify the Current Record** button or select the **Operation** option from the Menu Bar and select the **Change** sub-menu option.
3. Make the desired changes and <click> the **Save** button to save your changes or <click> on the **Cancel** button to exit without saving any changes.

Delete Mode (SSA0102)

This mode allows you to remove a user profile from your system. The user should not be currently logged into the system. By selecting this option, you will have the ability to remove a user from the system. Make sure this is what you want to do, otherwise, you will have to setup all of their information again. If you simply want to temporarily prevent them from logging into the system, you do not need to remove them from the system with this option. Instead, you would simply have the ***System Manager*** go to the change mode and make sure the **"Enabled"** data item is left blank.

In doing so, you would prevent them from entering the system until you desire, but you would not have to reconfigure their user profile. If you do want to remove them from the system, make sure that they are not currently logged into the software first.

To Remove a User Profile From the System:

1. Navigate to the record you wish to delete from the system. You may find a record using the navigation tool bar or <click> on the **Navigation** option on the Menu Bar and then the appropriate navigation option. This option allows you to delete users that you may have entered by mistake, or you no longer want.
2. If you are removing a record, <click> on the **Delete the Current Record** button or select the **Operation** option from the Menu Bar and select the **Delete** sub-menu option.
3. <Click> the **Save** button to confirm you want to delete the selected record or <click> on the **Cancel** button to exit without deleting the selected record.

NOTE

Once a user is deleted from the sytem, the record cannot be retrieved again. A backup of data files is always recommended prior to deletion of records.

Copy Mode (SSA0103)

This mode allows you to create a user profile based on the contents of an existing user profile. This option provides a quick and easy way to set up new users that will have the same or similar profile of other existing users on the system.

To Copy a Record:

1. Navigate to the record you wish to copy. You may find a record using the navigation tool bar or <click> on the **Navigation** option on the Menu Bar and then the appropriate navigation option.
2. <Click> on the **Create a Record Based on the Current Record** button or select the **Operation** option from the Menu Bar and select the **Copy** sub-menu option. All record information, except for the User ID, is copied to a new record.
3. Enter the new **User ID** for this record then change the name in the second data item.
4. Make any desired edits to the information and <click> the **Save** button to confirm you want to copy the selected record. The new record is added to the system file.

OR

5. <Click> the **Cancel** button to exit without copying the selected record.

SET UP GROUPS

This section discusses the ways to add, change, delete and copy groups in the **Advanced Security Administrator** module. It also covers how to assign these users to groups, if you decide to set up groups within the security system. There is also a report function that will enable you to print and verify all information input into this option for each group.

NOTE

Two special groups can be set up, **_PERMALL** and **_PERMCO**. The _PERMALL group, when created *(optionally)* overrides access rights to all companies. This does not mean that they will have access to all options in every module, unless this level of access rights have been assigned to this specific group. The _PERMCO group would allow full access in all companies except the company where the _PERMCO group is established.

Refer to ***Chapter 1 Introduction, Set Up Groups>Special Groups*** section for a detailed discussion on these special groups.

Inquiry Mode

The **"Inquiry"** mode allows you to view various summary information about the groups set up in the security system.

1. Navigate to the record you wish to view. You may find a record using the navigation tool bar or <click> on the **Navigation** option on the Menu Bar and then the appropriate navigation option.
2. Once a group has appeared on the screen, <click> the **By Option** button to review the rights given to each individual module for this group.

NOTE

When accessing the **By Option** button, you will enter a file system that you wish to view. The screen provides the option to view the first detail record, page up the detail list, page down the detail list, view the last record in the detail list, view a specific detail record based on text or view a specific detail record based on a line number.

3. When you select to view by either a record based on text or a record based on a line number, enter the appropriate information ***(either text or a line number)*** and <click> the **OK** button.

Add Mode (SSA0200)

Use this option to create a group profile. After assigning rights to the group, use the option ***"Assign User to Groups"*** to specify which users belong to a group. These users inherit the access rights of the group. This option is used to set up new groups and define the specific access rights for those groups. These access rights include permissions and authorizations information. It is recommended that **"groups"** be set up and utilized whenever possible. Using groups will simplify later administration and maintenance in regards to rights assigned by group versus rights assigned by individual User ID. Each group will dictate the minimum level of access rights ***(privileges)*** available to the users assigned to that group.

When a user has had permissions **"enabled"** to access specific options, either by defining them on the actual User ID or a group in which the User ID has been assigned, the user will have access to these options.

For instance, a User ID may be set up having no access rights to any option. If this User ID is assigned to a group which has access rights to a variety of options, they will have access to these specified options, even though their User ID is set not to have access to these specified options. Select ***"Set Up Groups"*** from the ***"Security Administration"*** menu.

To Add a New Record:

1. <Click> on the **Add a New Record** button or select the **Operation** option from the Menu Bar and select the **Add** sub-menu option. A screen displays with the following data items.

Data Item	Description
Group ID	This data is a ten **(10)** character alpha/numeric field which will be used to identify each individual group as they will be used throughout the system.
Description	This is a thirty (**30**) character alpha/numeric description of the group which is being added. This description will display on selection screens, maintenance and activity reports.
Enabled	This data item is used by the ***System Manager*** to manage the enabling or disabling of this particular Group ID. If this data item is turned on, the **Advanced Security Administrator** module will include this group's access rights in the overall permission settings for users that belong to this group. If this data item is left blank, the **Advanced Security Administrator** module will **NOT** include this group's access rights in the overall permission settings for users that belong to this group. The affect is similar to deleting the group altogether, except that it can be re-established easily by turning this data item back on. This feature can be used by the ***System Manager*** as a control tool to quickly remove this group's access to the system.

The next four data items deal with setting permissions and authorities for a particular group. Keep in mind the concept behind these functions before answering these questions. First, these features are designed to allow or disallow access to specific menu options and custom security objects. These are done on a **"global"** basis for all accounting modules that you currently have installed on your system.

The rule of thumb to use with these next four options is the amount of control or changes that you want to apply to a particular group and the groups' members. In other words, are you trying to limit access to a few options and provide access to the other **95%** of the system? Or, are you trying to keep the users out of almost everything and provide them access to **5%** of the options in the system?

The same considerations would be made when you set up users as well. When groups are set up with the appropriate rights for a group of users, no additional effort has to be made when adding these new users in terms of rights assignments. The group assignments will prevail automatically once a user has been assigned to a group or multiple groups.

A group provides each user its minimum level of access to specific programs or all programs. Therefore, if you have set up a group that provides access to every option in every module, you cannot take that access away from any user in that group. If this is not what you want to do, then set up groups with less rights and add more access for a user by using **"By Option"** on the **"Set Up Users"** screen.

This data item will provide you the ability to turn on and off access to specific menu options and custom security objects for that user on a module by module basis. These next four options are for complete global set up of all features.

Therefore, answering **(Y)**es to **"Enable All Permissions?"** will set the default access for this group to allow access to every option in every module. If you only want to secure a few options, this is what you would want to do. If you only want to allow access to a few options, you would answer **(N)**o. In either case, you will be defining for the **System Manager** how much additional effort will be required to fine tune access rights. The same concept works with **"Authorities"** as well. This feature works as a manager override option and again you must decide how much override requirements you want for a group of users on each and every option. Careful planning should be considered before implementing these features.

Keep in mind, a user does not have to belong to a group, therefore, you may control each user on an individual basis, if desired. However, as you deal with larger numbers of users who have similar computing needs, you will find the implementation and control of groups is significantly easier on the **System Manager**.

Data Item	Description
Enable Perm	This is a **(Y)**es or **(N)**o question which allows the ***System Manager*** to set this group's global access to all options for all accounting systems ***(menu options and custom security objects)***. When a group has had permissions **"enabled"** to access specific options, members of that group will have access to these options. The ***"By Option"*** button on this screen will specifically allow you to make changes to rights on a module by module basis. This data item is setting a global default. Once rights have been modified in that option, answering **(Y)**es to this prompt again now or later in the ***"Set Up Groups"*** option will supersede any customization that has occurred. Therefore, you must be careful in using this option so as not to override specific configurations made for this group.

Data Item	Description
Disable Perm	This is a **(Y)**es or **(N)**o question which allows the ***System Manager*** to set this group to be denied access to all options for all systems ***(menu options and custom security objects)***. When a Group ID has had permissions **"disabled"** to access specific options, a User ID will not have access to those options unless they also belong to a group that still has access rights to those same options or the User ID itself has access rights. Keeping in context with the discussion in this section, if you only want to allow only a limited amount of access to a group of users ***(the 5% access instead of 95%)***, you would answer **(Y)**es to this data item. You would then proceed to the ***"By Option"*** button to specifically set up the few options that you want this group of users to have access to. This data item is setting a global default. Once rights have been modified in the ***"By Option"*** area, answering **(Y)**es to this prompt again now or later in the ***"Set Up Groups"*** option will supersede any customization that has occurred. Therefore, you must be careful in using this option so as not to override specific configurations made for this user.
Enable Auth	This is a **(Y)**es or **(N)**o question which allows the ***System Manager*** to set the members of a group to be required to obtain authorization on all options for all systems ***(menu options and custom security objects)***. This will prompt each member of the group for a User ID and Password, which has authorization to access and proceed with the given option. Answering **(Y)**es to this data item will be telling the system that you will be requiring another user ***(manager override)*** to approve specific access each time a member of this group wants to access a specific menu option or custom security object. Therefore, careful consideration should be made as to how many authorities will be required for group members. If you want to allow group members the ability to use an option, but only after a manager has approved use of the option, you must first provide the group permission to access the option. Once access rights to the option have been provided, then an authority must be assigned to the same option. These data items work similar in concept to permissions. The question to consider is whether members of a group will require manager overrides on **5%** of the options they are using or **95%**. Based on this criteria, you would respond **(Y)**es or **(N)**o accordingly. This data item is setting a global default. Once authorities have been modified in ***"By Option"*** answering **(Y)**es to this prompt again now or later in the ***"Set Up Groups"*** option will supersede any customization that has occurred. Therefore, you must be careful in using this option so as not to override specific configurations made for this user.

Data Item	Description
Disable Auth	This is a **(Y)**es or **(N)**o question which allows the ***System Manager*** to set the members of a group to be required to obtain authorization on all options for all systems ***(menu options and custom security objects)***. If your desire is to allow members of a group access to the options without requiring a manager override, then you should answer **(Y)**es to this question. This data item is setting a global default. Once authorities have been modified in ***"By Option,"*** answering **(Y)**es to this prompt again now or later in the ***"Set Up Groups"*** option will supersede any customization that has occurred. Therefore, you must be careful in using this option so as not to override specific configurations made for this user.
All Companies	This question allows the ***System Manager*** to define whether or not access options specified in this Group ID will be effective in all companies accessed by this Group ID. This feature will only affect those company data files that have already had security rights setup at this point. If you **"add"** new companies in the future, you will be required to use the ***"Update Company Rights"*** feature to be able to enable access to those new companies by a group set up in this option. If you are performing multi-company processing, this is a key question. A business owner may want to allow specific members of various groups access to data in some companies and not in others. Therefore, you must consider this before granting full access to all companies with this option. If you leave this option blank, then the ***System Manager*** will be required to press **F4** to access the ***"Change a Company"*** feature and then set up the groups for the other desired companies as well as the currently loaded company.
Copy Rights From Group	By <clicking> on the **"Group"** button, you will be prompted for a specific group from a specific company to copy rights from. This will copy all access right information from that specified Group ID from that specified company. This option can be a real time saver if utilized properly. Even if some changes would be required to configure the new group's rights specifically, getting most of the work done by using this copy function can save a great deal of time.
By Option	This option allows the ***System Manager*** to define access rights by module and by individual menu option. This is the key option in defining specific rights for a group. On this screen, the system allows complete modification of access rights for an individual group. Keep in mind, if a user is a member of a group, the group's rights will prevail in terms of minimum rights. In other words, do not provide rights on this screen for options that you do not want all members of the group to have. If you want specific users to be allowed access that other members of the group do not have, you may do one of two things. First, you may create a secondary group that would provide those additional access rights and assign only those additional users to this group as well. Users may be members of more than one group at a time. Second, you can simply provide those additional rights to those specific users at the user level. Keep in mind the quantity of users and the amount of additional maintenance that this may represent for the ***System Manager*** in the future. If you <click> on the ***"By Option"*** button, the following screen will appear:

Data Item	Description
System	This data item requires the entry of a module identifier. This would represent the two or three character abbreviation of the accounting module you want to provide access changes to. For instance, if you want to call up General Ledger, then enter **"GL"** in this data item. **"AR"** would represent Accounts Receivable. The following list includes all of the possible choices. You cannot, however, provide access to modules that are not currently loaded on your system. The valid choices are: **Sys ID** **Module Name** XX System Administrator SSA Security System Administrator PT Productivity Tools GL General Ledger AP Accounts Payable PO Purchase Order Entry AR Accounts Receivable IM Manufacturing Inventory Management SO Sales Order Entry PS Point of Sale PR Payroll JC Job Cost Main Module CR Check Reconciliation TE Time Sheet Entry RW Report Writer RWR Report Writer (Run Time) FC POWER Upgrade Utility ME Menu Editing Tool FG Forms Generator Tool SD Customer Support Management SYS System (Global Functions)
Enable Perm	This option sets the default permissions flag for all options that are available for the module selected on this screen. It will not affect any other module's configuration, only the system specified. Answering **(Y)**es will make all permissions available for this group. Keep in mind that group level access will always prevail, regardless of what you set up by user. Enter **(N)**o if you feel that the majority of the options should not be accessible. This data item and ***"Disable Perm"*** work as a toggle for the default value for each option.

Data Item	Description
Disable Perm	This option sets the default permissions flag for all options that are available for the module selected on this screen. It will not affect any other module's configuration, only the system specified. Answering **(Y)**es will make all permissions unavailable for this group. Keep in mind that the user may still have access if they belong to another group that provides them access, or access has been provided at the user level. Enter **(N)**o if you do not want to change the default value of these fields. This data item and ***"Enable Perm"*** work as a toggle for the default value for each option.
Enable Auth	This option sets the default authorizations flag for all options that are available for the module selected on this screen. It will not affect any other module's configuration, only the system specified. Answering **(Y)**es will set all authorizations to be on for this group. Keep in mind that group level authorizations will be displayed from the settings on the overhead screen in this option. Enter **(N)**o if you feel that the majority of the options should not require an authorization. This data item and ***"Disable Auth"*** work as a toggle for the default value for each option.
Disable Auth	This option sets the default authorizations flag for all options that are available for the module selected on this screen. It will not affect any other module's configuration, only the system specified. Answering **(Y)**es will set all authorizations to be off for this group. Keep in mind that group level authorizations will be displayed from the settings on the overhead screen in this option. Enter **(N)**o if you feel that the majority of the options should require an authorization. This data item and ***"Enable Auth"*** work as a toggle for the default value for each option.
Copy Rights From Group	By <clicking> on the **"Group"** button, a new window will overlay your screen and prompt you for a specific group, from a specific company, to copy rights from for this specific module or system. This will copy all access right information from that specified Group ID from that specified company. This option can be a real time saver if utilized properly. Even if some changes would be required to configure the new group's rights specifically, getting most of the work done by using this copy function can save a great deal of time.
User Info	<Clicking> on the **"User Info"** button will generate an overlay screen that will show all of the users that belong to this group. You may choose one of the users to view and <click> on the "**OK**" button. When you are done viewing the members of this group, <click> on the **"Cancel"** button to exit. <Click> on the **"Save"** button to validate and you will be prompted to add another group. If you are done, <click> on the **"Close"** button to exit to the menu.

To Copy Rights from a Group:

1. <Click> the **Group** button. The Use Rights from Group window displays.

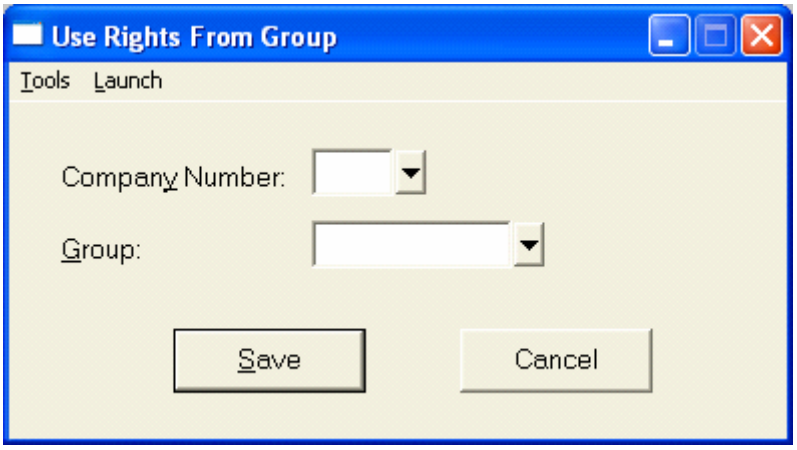


Figure 2-5. Use Rights From Group Window

2. Enter the desired **Company Number** and **Group ID** in the appropriate fields.
3. <Click> the **Save** button to save the selected Company Number and Group to be copied. You will now be returned to the previous screen where the system will display this information next to the **Group** button. If you <click> on the **By Option** button, the system displays all of the option ID's for the system loaded.

On each line, the screen will display the Option ID, its description and the current status of Permissions and Authorizations. You may use the up and down arrow keys to scroll through the list of available Option IDs. When you decide to change an Option ID, simply change each field to be set to your specifications.

By pressing the ***"Authorities"*** button, the system will display any authorities that have been assigned to any of these Option IDs. Simply <click> on the ***"Authorities"*** button on the line of the Option ID you want to view. A window will overlay the screen and show all of the users who have been given an **"authority"** or manager override for this specific Option ID. If no authorities have been assigned to the highlighted option, a message will state so at the bottom of the screen.

By pressing the **Close** button, you may view other authority assignments by system. Make sure to finish all changes and continue by <clicking> on the **Save** button to validate all changes made on these screens. Otherwise, your changes will be lost.

Change Mode (SSA0201)

Use this option to change a group profile, including the group access rights. By selecting this option, you have the ability to make changes to a group's profile, including the definition of its specific access rights. Keep in mind, that group access rights will always establish the minimum rights provided to a user.

Change Mode (SSA0101)

This mode allows you to change a user profile, including user access rights. By selecting this option, you have the ability to make changes to a user's profile, including the definition of their specific user rights. Keep in mind that group access rights will always establish the minimum rights provided to a user. Therefore, rights assigned at a group level cannot be removed by this option.

To Modify a Record:

1. Navigate to the record you wish to change. You may find a record using the navigation tool bar or <click> on the **Navigation** option on the Menu Bar and then the appropriate navigation option.
2. If you are changing a record, <click> on the **Modify the Current Record** button or select the **Operation** option from the Menu Bar and select the **Change** sub-menu option.
3. Make the desired changes and <click> the **Save** button to save your changes or <click> on the **Cancel** button to exit without saving any changes.

Delete Mode (SSA0202)

Use this option to remove a group profile from the system. By selecting this option, you will have the ability to remove a group from the system. Make sure this is what you want to do, otherwise, you will have to setup all of its information again.

If you want to temporarily remove this group from being used in evaluating permission settings, simply have the ***System Manager*** go to the change mode and make sure the **"Enabled"** data item is left blank. In doing so, you would remove the group from the system until you desire, but would not have to reconfigure the group profile again. If you do want to remove the group from the system, make sure that there are no members of the group currently logged into the software. Then, enter the name of the group to be deleted.

To Remove a Record from the System:

1. Navigate to the record you wish to delete from the system. You may find a record using the navigation tool bar or <click> on the **Navigation** option on the Menu Bar and then the appropriate navigation option. This option allows you to delete accounts that you may have entered by mistake, or you no longer want.
2. If you are removing a record, <click> on the **Delete the Current Record** button or select the **Operation** option from the Menu Bar and select the **Delete** sub-menu option.
3. <Click> the **Save** button to confirm you want to delete the selected record or <click> on the **Cancel** button to exit without deleting the selected record.

NOTE

Once a user is deleted from the system, the record cannot be retrieved again.
A backup of data files is always recommended prior to deletion of records.

First, you must navigate to the record you wish to delete. You may find a record using the navigation tool bar or <click> on the **"Navigation"** option on the Menu Bar and then the appropriate navigation option. This option allows you to delete groups that you may have entered by mistake, or you no longer want. <Click> on the ***"Delete the Current Record"*** button or choose the ***"Operation"*** option from the Menu Bar and then ***"Delete."*** This will place you into the **"Delete"** mode, then <click> on **"Save"** to validate your deletion of this record.

Make sure this is what you want to do, because once a group is deleted, it can not be retrieved again. A backup of data files is always recommended prior to deletion of records.

Copy Mode (SSA0203)

Use this option to create a group profile based on the profile of an existing group. This option provides a quick and easy way to set up new groups that will have the same or similar profile of other existing groups on the system.

To Copy a Group Profile:

1. Navigate to the record you wish to copy. You may find a record using the navigation tool bar or <click> on the **Navigation** option on the Menu Bar and then the appropriate navigation option.
2. <Click> on the **Create a Record Based on the Current Record** button or select the **Operation** option from the Menu Bar and select the **Copy** sub-menu option. All record information, except for the User ID, is copied to a new record.
3. Enter the new **User ID** for this record then change the name in the second data item.
4. Make any desired edits to the information and <click> the **Save** button to confirm you want to copy the selected record. The new record is added to the system file.

OR

5. <Click> the **Cancel** button to exit without copying the selected record.

ASSIGN USERS TO GROUPS (SSA0600)

This option allows you to specify which users belong to which groups. With this option, you can assign users to be members of **"groups."** A user, however, cannot be assigned to a group if the group has not been set up yet.

As discussed throughout this manual, users do not have to be assigned to groups to have access rights and authorities assigned to them. Only if there may become a significant level of maintenance should you consider the use of groups. Overall, it is recommended that groups are established and that access rights be assigned on this level. This way, when a change involving the group is required, it only has to be implemented at the group level and not for each individual user.

When you select this option, a new screen will appear prompting you to enter the Group ID. Enter the desired group or <click> the **Down Arrow** ***(F2 by default)*** to use the near match scrolling window to verify your current level of choices. Once the group has been selected, choose the User ID to assign to the group. Based on the current configuration of the system, an overlay window will appear telling you that you are about to assign a user to a group or asking you whether you want to delete this user from the group.

If the user has not been assigned to the selected group previously, you will be notified that this assignment does not currently exist and asked if you want to create this group assignment. <Click> on the **"Add"** button and the system will add the user as a member of the group. You will then be left on the same screen and prompted to enter the next group and user to be assigned or deleted from a group.

If the user has already been assigned to the group specified, the system will prompt you with the question ***"Do you wish to delete this group assignment?"*** <Click> on the **"Delete"** button if this is what you want to do, otherwise, <click> on the **"Cancel"** button and then on the **"Close"** button to exit this option.

CREATE COMPANY RIGHTS (SSA0300)

This option allows you to create an access rights file for the current company. Options contained in the files are based on the standard menu and custom security files.

Every company utilizing the **Advanced Security Administrator** module must have a company rights file, unless you have specified a default company in the Security Configuration. When you select this option, you will be prompted to enter the company number that you wish to copy rights from.

To Create Company Rights:

1. If you have already set up another company's security files and wish to duplicate that company's configuration, enter the three character Company ID in the **Company ID** text box. If you enter a Company ID that has not had its access rights set up in the system, a near match scrolling screen will appear showing the valid companies to choose from. Select a company or set up company rights from scratch by not entering any Company ID into this field.

2. <Click> on the **Start** button to validate and the system will either copy another company's rights or create your new company rights based on the current accounting modules loaded on your system.
3. If you load additional modules to the system after this option has been run, you must use the **Update Company Rights** option to include these new modules in the security configuration. If you select this option and the current company has already had its rights set up, you will receive an ERROR message stating the rights file for the company already exists.
4. <Click> on the **Close** button to leave this option.

UPDATE COMPANY RIGHTS (SSA0301)

This option allows you to update the access rights file associated with the current company. You may wish to update the access rights file if the standard menu file has changed or if you have received an update of custom security objects. You may also use this option to add options from a custom menu file.

Using this option is required only if you have made changes to the configuration of your system by adding new modules since you set up the company rights file. If so, you will need to update the current company to match. There are other reasons as well to use this option and they are covered in the following discussion regarding the four data items that will appear when you select this option.

Data Item	Description
Company	This data item is prompting for the Company ID to copy the access rights from. Enter the three character Company ID in the field. If you enter an invalid Company ID or simply <click> the **Down Arrow *(F2 by default)***, a near match scrolling screen will appear. Use the up or down arrow keys to scroll through the valid choices.
Update using custom menu in directory	Use this option to update your company rights by including any new custom menu files that have been updated on your system. Custom menu files are generated through the use of the **Infinity POWER *Menu Editing Tool***. This tool allows for the creation of additional or custom menus that can call both **Infinity POWER** options as well as a wide range of third party programs and utilities. This data item is prompting you for the path assignment where the programs find the custom menus. This could be the current drive or path or another drive and path if desired. You must include the full path assignment in your entry with all slashes and backslashes accordingly.
Standard Menu Options	If you have added new modules to the system, you would <click> **"on"** this check box so that the system will go through and update itself by looking at the current **DPMENU.SYS** file. This file includes the menu for all currently installed modules.
Custom Security Objects	You would select this option if **Data Pro Accounting Software** has made changes to the system that would allow you additional access to new custom security objects. Currently, this is the only way you would be able to receive these kinds of changes. You would <click> "**on"** this check box so that the system will go through and update itself. <Click> on the **"Start"** button and all updates will be performed. You may utilize this option as often as desired.

DELETE COMPANY RIGHTS (SSA0302)

This option allows you to delete the access rights file associated with the current company. Use this option if you have made a mistake in your set up of access rights or if you have decided to use another company's rights instead. Selecting this option will delete the access rights for the currently loaded company. Make sure this is what you want to do before proceeding and be sure to have a backup of your security files first.

Keep in mind that security files are not stored in the normal data file path. Therefore, make sure a specific backup of these files has been made before proceeding. When you select this option, you will be prompted to specify whether you want to delete the access rights file for the current company. <Click> on the **"Start"** button to proceed and the files will be deleted.

You may now create new access rights files from scratch or copy another company's files instead. You must, however, have an access rights file for each company that is going to have security implemented, unless you have specified a default company in the Security Configuration.

ENABLE COMPANY RIGHTS (SSA0303)

This option allows you to enable or disable a company rights file. If a company's rights file is disabled, users are denied access to all protected features while in that company. As the ***System Manager***, this is an ideal option to provide quick and efficient control over access to a company's accounting data files.

This option allows for the quick enabling or disabling of access rights files with no other steps involved. The reasons to use this option may vary, but good examples would include the following.

At the end of each year, all companies must use the options to ***"Start New Year's Files."*** The ***System Manager*** may utilize this option to disable rights to a specific company temporarily to ensure that no users are accessing that particular company's data files while these options are being run. It is essential to not have any files open when an option such as this is being executed. All data such as customers and vendors are being copied from one year's file to the new year. If any information is missed, then the option would not be working correctly.

Therefore, no interference can be allowed during the execution of this option. Therefore, the ***System Manager*** can choose this option and leave the check box blank on ***"Enabled?"*** In doing so, no further users would be allowed to enter these data files while the ***System Manager*** logs in as **SYSADM** and performs the necessary maintenance functions.

When he or she is done, they may then return to this option to turn them back on by <clicking> on the check box. This option should also be run for other options such as ***"Maintain Data Files"*** found in all programs. Those options are re-indexing and compressing the data files and user access during the use of these functions should be restricted. This option may be utilized as often as desired.

ADD AN AUTHORITY (SSA0700)

This option allows you to assign a user as an authority whose approval is required before other users may access a specific system option. If the user accesses an option subject to authorization, the designated authority must confirm access by supplying a User ID and password.

This option allows the assignment of authorities to specific Option IDs throughout the entire accounting system, on a company by company basis. By selecting this option, a new screen will appear with five data items. Each of these items are discussed here.

Data Item	Description
User ID	Enter the **User ID** whom you want to assign as the authority for this specific **Option ID**. Once assigned, this specific user will be required to enter an approval any time another user attempts to access the specified option. The user being assigned here **does not** have to have permissions assigned to them to be able to be used as an authority for this option.

Data Item	Description
System	Enter the two or three character System ID designation to select the specific module your option is stored in. This is the specific **Infinity POWER** program you want to access. XX System Administrator SSA Security System Administrator PT Productivity Tools GL General Ledger AP Accounts Payable PO Purchase Order Entry AR Accounts Receivable IM Manufacturing Inventory Management SO Sales Order Entry PS Point of Sale PR Payroll JC Job Cost Main Module CR Check Reconciliation TE Time Sheet Entry RW Report Writer RWR Report Writer (Run Time) FC POWER Upgrade Utility ME Menu Editing Tool FG Forms Generator Tool SD Customer Support Management SYS System (Global Functions)
Option ID	Enter the **Option ID** in the field that you want to assign an authority to. This is the specific menu option within a program. By <clicking> the **Down Arrow *(F2 by default)***, a near match scrolling search window will appear with the list of all valid choices for the system selected.
Enabled	Specify whether to enable this authority by <clicking> **"on"** the check box. Leaving the check box blank will allow the setup of the authority to continue, however, it will not be active until enabled.
All Companies	This option allows you to specify whether this authority should apply to all companies who have had access rights set up in the system. If you mean for this authority for this system and Option ID to be active in all companies, then <click> **"on"** the check box. Otherwise, leaving the check box blank will tell the system to enable this authority for the currently loaded company only.

Once the information is entered for these data items, <click> on the **"Add"** button to validate this screen. When it is done processing, you will be returned to the original data entry screen where additional authorities may continue to be added to the system. When you are done, <click> on the **"Close"** button to exit.

CHANGE AN AUTHORITY (SSA0701)

This option allows you to change the specific attributes of a specific authority and system option. The change applies only to the current company. Use this option to enable and disable specific authorities that have been created in the system. You do not have to delete an authority if you want to temporarily disable it. Instead, you would select this option. At this point, the system will prompt you to enter the User ID, the system, and the Option ID that you want to change.

If you type in an invalid Option ID, a near match scrolling screen will appear and show you all of the authorities available to this particular user. <Click> on the **"OK"** button to continue and the screen will then prompt you as to whether to enable this authority or not. Enter your choice according to your current needs.

Once you have made your change, you will be returned to the same screen so that you can continue to change additional authorities. When you are done, <click> on the **"Save"** button to validate your changes.

DELETE AN AUTHORITY (SSA0702)

This option allows you to delete a single authority or all authorities associated with a specific system option or all options. You may also perform the delete for the current company or for all companies.

Once authorities have been created in the system, they may need to be revoked or removed altogether at a later date. This option is designed to allow the various choices to be conveniently listed, depending on your circumstances. When you select this option, six **(6)** data items will appear on the screen. These items are discussed here.

Data Item	Description
All Authorities	By <clicking> on this check box, you will be telling the system to remove all authorities based on the way you respond to the following prompts. If you only want to remove a single or a few authorities in the system, you should leave this check box blank so that you may define a specific Authority.
Authority	If you have left the check box blank in the data field above, the system will then prompt you in this field for the User ID that you want authorities removed for. You must type in a valid User ID or leave the field blank to proceed. If you have <clicked> **"on"** the ***"All Authorities"*** check box, the system will skip by this field during this process.
All Companies	This data item is used to specify whether the deletions should affect only the currently loaded company or all companies where the authorities have been assigned. Enter your choice accordingly. <Clicking> "on" this box would define **"all"** companies.
System	This data item allows you to specify which system or accounting modules should be affected by these deletions. You may leave the field blank which will include all systems or specify the two or three character **System ID** representing the specific **Infinity POWER** module. For example, use **"GL"** for the General Ledger module.
Option ID	If you want to delete only a specific **Option ID**, you must specify it in this field. This data item does not have the scroll search near match window. Therefore, your entry must be specific. If you are not sure of the specific Option IDs assigned to a user, you may want to ***"Print an Authority"*** listing to review the assignments made by user to a specific option.
All Options	<Click> **"on"** this data item if your desire is to delete all authorities either for all users or for the user specified. If this is not what you want to do, then leave this check box blank.

When you <click> on the **"Start"** button to validate this screen, the system will delete the authorities based on the criteria entered on this screen. When completed, the system will display a statement as to how many authorities have been deleted.

COPY AN AUTHORITY (SSA0703)

This option allows you to copy a single authority or all authorities associated with a specific system option or all options. You may also copy to either a specified company or to all companies.

You may use this option to conveniently copy authorities that have already been set up in the system. You may copy an authority within the currently loaded company to a single company or to all companies configured in the system. When you select this option, seven **(7)** data items will appear. The following section details the questions involved in this option.

Data Item	Description
All Authorities	By <clicking> on this check box, you will be telling the system to copy all authorities based on the way you respond to the following prompts. If you only want to copy a single or a few authorities in the currently loaded company, you should leave this check box blank.
User ID	If you have left the check box blank in the data item above, the system will then prompt you in this field for the User ID that you want to copy authorities from. You must type in a valid **User ID** or leave the field blank to proceed. If you have <clicked> **"on"** the ***"All Authorities"*** check box, the system will skip by this field during this process.
All Options	<Click> on this data item if your desire is to copy all options either for all users or for the user specified. If this is not what you want to do, then leave this check box blank.
System	This data item allows you to specify which system or accounting modules should be affected by the copy option. You may leave the field blank which will include all systems or specify the two or three character **System ID** representing the specific **Infinity POWER** module. For example, use **"GL"** for the General Ledger module.
Option ID	If you want to copy a specific **Option ID**, you must specify it in this field. This data item does not have the scroll search near match window, therefore, your entry must be specific ***(i.e., GL0101)***. If you are not sure of the specific Option IDs assigned to a user, you may want to ***"Print an Authority"*** listing to review the assignments made by user to a specific option.
All companies	This data item allows you to specify whether the copy function should affect only the currently loaded company or all companies where the authorities have been assigned. Enter your choice accordingly.
Company	This data item is used to specify the company that the specified authorities should be copied to. Enter the three character **Company ID** that should be used in this copy function. If you are not affecting all companies with this copy option, you must enter a Company ID here to proceed.

When you <click> on the **"Start"** button to validate this screen, the system will copy the authorities based on the criteria entered on this screen. When completed, the system will display a statement as to how many authorities have been copied.

REPLACE AN AUTHORITY (SSA0704)

This option allows you to replace an authority with another. You may replace the authority for a single option or all options. You may also perform the replace for the current company or for all companies. This is a maintenance option that allows for the replacement of users as authorities on options. Personnel will come and go over time or may be temporarily unavailable and it is easier to replace the User IDs involved than to set up a new scheme of authorities from scratch.

With this option, you may perform replacements either globally or on an option by option basis.

The section details the six data items found on this screen.

Data Item	Description
Old User ID	In this data item, enter the User ID that is to be replaced. You must enter the specific User ID to proceed.
New User ID	Enter the new **User ID** that is to replace the User ID entered as the old User ID. If you enter an invalid User ID, a near match scrolling screen will appear to allow you to choose from a valid User ID that has been set up on the system. Select the desired User ID and <click> on the **"OK"** button to continue.
All Options	<Click> on this data item if your desire is to replace all authorities for the old user with the new user. If this is not what you want to do, then leave this check box blank.
System	This data item allows you to specify which system or accounting modules should be affected by the replacement option. You may leave the field blank which will include all systems or specify the two or three character **System ID** representing the specific **Infinity POWER** module. For example, use **"GL"** for the General Ledger module.
Option ID	If you want to replace a specific **Option ID**, you must specify it in this field. This data item does not have the scroll search near match window, therefore, your entry must be specific ***(i.e., GL0101)***. If you are not sure of the specific Option IDs assigned to a user, you may want to ***"Print an Authority"*** listing to review the assignments made by user to a specific option.
All companies	This data item allows you to specify whether the replacement function should affect only the currently loaded company or all companies where the authorities have been assigned. Enter your choice accordingly. When you <click> on the **"Start"** button to validate this screen, the system will replace the authorities based on the criteria entered on this screen. When completed, the system will display a statement indicating authorities have been replaced.

ENABLE AN AUTHORITY (SSA0705)

This option allows you to enable or disable a single authority or all authorities associated with one system option or all options. You may enable or disable either the current company or all companies.

You may use this option as an easy maintenance function designed to allow for the quick enabling or disabling of authorities. Just as quick as you can disable an authority, you can use this option to turn them back on. This section covers the seven **(7)** data items detailed on this screen.

Data Item	Description
All Authorities	By <clicking> on this data item, you will be telling the system to enable all authorities based on the way you respond to the following prompts. If you only want to enable a single or a few authorities in the currently loaded company, you should leave this check box blank.
User ID	If you have left the check box blank in the data item above, the system will then prompt you in this field for the User ID that you want to enable authorities for. You must type in a valid **User ID** or leave the field blank to proceed. Should <click> on the data field above, the system will skip by this field during this process.
All Options	<Click> on this data item if your desire is to enable all authorities for all options, whether it is for all users or for the user specified. If this is not what you want to do, then leave this check box blank.
System	This data item allows you to specify which system or accounting modules should be affected by the enable option. You may leave the field blank which will include all systems or specify the two or three character **System ID** representing the specific **Infinity POWER** module. For example, use **"GL"** for the General Ledger module.
Option ID	If you want to enable a specific **Option ID**, you must specify it in this field. This data item does not have the scroll search near match window, therefore, your entry must be specific ***(i.e., GL0101)***. If you are not sure of the specific Option IDs assigned to a user, you may want to ***"Print an Authority"*** listing to review the assignments made by user to a specific option.
All companies	This data item allows you to specify whether the enable function should affect only the currently loaded company or all companies where the authorities have been assigned. Enter your choice accordingly.
Company	This data field is used to specify the company where the specified authorities should be enabled. Enter the three character **Company ID** that should be used in this enabling function. If you are not affecting all companies with this enabling option, you must enter a Company ID here to proceed.

When you <click> on the **"Save"** button to validate this screen, the system will enable the authorities based on the criteria entered on this screen. When completed, the system will display a statement as to how many authorities have been enabled. It will then prompt you to press any key to continue.

FORCE PASSWORD CHANGE (SSA0601)

Use this option to force users to change their passwords at the time of the next login. Password aging need not be in effect. **NOTE:** If the ***"Password Required"*** configuration option is disabled, only users who already have passwords are prompted to change passwords.

Due to a security breach within your system or carelessness from one of your users, as ***System Manager*** you may determine that all users should change their passwords immediately. By using this option, the system will force all users, who already have passwords, to change their passwords the next time they login to the system.

All of the same password criteria still apply they just have to be different than the current password they have installed. Using this option would bypass a potentially significant process if the ***System Manager*** were forced to change each user's password. Select this option and a new screen will appear with a prompt at the bottom ***"Are you ready to begin?"*** <Click> on the **"Start"** button to begin and the system will initiate the forced change immediately and return you to the menu upon completion.

SECURITY CONFIGURATION (SSA0400)

This option allows you to configure general settings for your **Advanced Security** system. Among the settings you can control are the number of login attempts, password aging, and the recording of user activity. By selecting this option, the following screen will appear with twelve **(12)** data items for configuration.

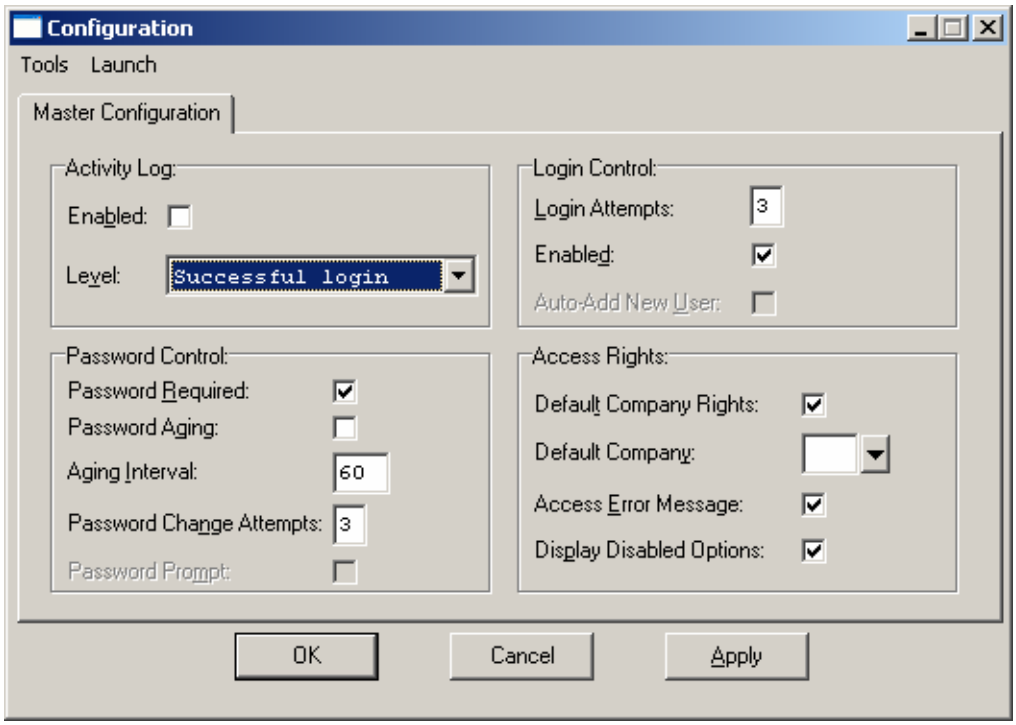


Figure 1-6. Configuration Window

Each of these data items are described in the following table.

Data Item	Description
Activity Log	The **"activity log"** is an optional feature of the **Advanced Security Administrator** module. It is used to record the ***"login"*** activity for all users. There are three **(3)** levels of information which can be recorded. Whichever variation you decide upon, it will be demonstrated system wide. All information is written to the **Activity Log File (SYSSS8.dbf)** and can be purged periodically by the ***System Manager***. The **Activity Log Report** can be printed at any time. It is recommended that the **Activity Log Report** be printed to ***"hard copy"*** so that the ***Activity Log File*** may be purged periodically.
Enabled	Selecting this check box enables the activity log file to record all information to the Activity Log file.
Level	There are three levels of activity information that can be recorded: **Successful Login** - Records all successful logins by user. This information will be shown on the **Activity Log Report** as a separate line item for each time a user logs in and logs out of the **Infinity POWER** system. The information includes date, time, User ID, Event and Error Code. A Code **"0"** signifies a successful login. **Login Attempts** - Records all attempts made to log into the **Infinity POWER** system. This information will be shown on the **Activity Log Report** as a separate line item for each time a user attempts to log into the **Infinity POWER** system. The information includes date, time, User ID, Event and Error Code. A Code **"0"** signifies a successful login, while a Code **"1"** signifies an unsuccessful login. **Option Selection** - Records all movement within the **Infinity POWER** system. This information will be shown on the **Activity Log Report** as a separate line item for each time a user accesses a menu option or custom object in the **Infinity POWER** system. The information includes date, time, User ID, Event and Error Code. All Error Codes issued on this level are defined in ***Chapter 3, Error Codes***. The **Activity Log Report** can be printed at any time. It is recommended that the **Activity Log Report** be printed to ***"hard copy"*** so that the ***Activity Log File*** may be purged periodically
Password Control	Password control is a highly recommended feature of the security system. It adds one more level of confidence to the business owner, knowing only privileged personnel can access important information about the company. The **Advanced Security Administrator** module can be set up to enable a **"Password Aging"** option. If you enable the Password Aging and set the Password Aging Interval to thirty **(30)** days, every thirty days, the system will require all users to change their passwords.

Data Item	Description
Password Required	Selecting this check box enables the password function to be required to enter the accounting system. When a password change is required, the user must choose a new password that is different from his previous password. It must contain at least three **(3)** different characters from the previous password. For instance, if the original password was **"TAMPA99,"** changing it to **"99TAMPA"** will not be accepted.
Password Aging	Selecting this check box will force all users to change their passwords periodically based on the defined **"Password Aging Interval."**
Aging Interval	This interval is set up in the Security Configuration and will be used to force a change in passwords.
Password Change Attempts	The **"Change Password Attempts"** option sets a maximum number of attempts to change a password. When a user is prompted to change their password, they are given ***"x"*** many attempts, before the system will deny access. Setting this number to zero **(0)** will allow them to attempt a change as many times as desired. The user may then login again and attempt to re-define their password. The system can be set to a maximum number of **"9"** or to **"0"** which will enable unlimited password attempts.
Login Control	This set up option allows the ***System Manager*** to determine whether to allow logins or not. If this feature is not turned on, it will not allow any User ID ***(besides the SYSADM)*** to log into the system. This feature is very useful for those occasions when maintenance or special auditing functions are occurring within the company. The ***System Manager*** can come to this option to control the login capability of all users.
Login Attempts	This option allows the ***System Manager*** to define the number of attempts to be given to the Users during the ***"System Login."*** If a user attempts to login and uses the ***"x"*** number of attempts and fails, they will be denied access to the system. The user can then re-enter the system and attempt their login and password a second time. The system can be set to a maximum number of **"9"** or to **"0"** which will enable unlimited login attempts.
Enabled	By default, the **"Login Enabled"** feature will be turned on.
Access Rights	The **"Access Rights"** portion of the System Configuration allows the ***System Manager*** the capability of assigning a default set of access rights based on a **"default company"** which has already had access rights defined.
Default Company	The system will prompt you for the company identifier ***(company number)*** to define the default company the security system should use. If a set of company files has already been set up with their own set of rights prior to this definition in the Master Configuration, they will continue to use their own rights.

Data Item	Description
Access Error Message	<Click> on this **"Access Error Message"** option if you wish to inform the users when they are denied access to a menu option or custom object. If the check box is left blank, when a user who does not have access rights attempts to access an option, the cursor will simply stay at the prompt and they will be refused access without a message. They will see the option from the menu, but will not be able to proceed.
Display Disabled Options	One of the most exciting and powerful features of the Advanced Security Administrator module is the ability with this option to determine whether a user can literally see options in which they have no access. Once the System Manager determines which users have specific access to various options within a program, this question will control whether those options still appear on the screen or are removed altogether. Depending on your situation you may want users to see that the options exist, but not let them have access. In other situations, a System Manager may determine that it would confuse some users to leave an option on the screen and not allow access to it. This option will remove menu options only. It does not remove a program definition such as "General Ledger" from the menu. It would also leave the choices such as "Enter Transactions" on the screen as well. What it does remove is the specific Option ID's such as "Record a Journal Entry." Therefore, as a user, if you do not have access to this specific option and this question is turned off, you will not see the option even listed on your screen. Keep in mind, turning off this option will require the system to hide a variety of Option ID's and force it to track by user and group which screen displays a user should see. Therefore, some degradation in processing speed could occur.

The next section covers each of the twelve data items shown on this screen and how they can impact your overall security configuration. The screen is broken down into four sections covering the ***"Activity Log," "Password Control," "Login Control"*** and ***"Access Rights."***

Once your choices have been defined on this screen, <click> on the **"OK"** button to validate. All changes to the **Security Configuration** will be invoked at this point. You may change this configuration at any time. Obviously, the ***System Manager*** will want to tightly control which users, if any, have access to this option.

MAINTAIN DATA FILES (SSA0401)

This option includes both **"Pack"** and **"Re-Index"** utilities to manage your Advanced Security files after a hardware or media failure. This procedure will also physically remove records that have been marked for deletion.

You should **NOT** rely on this option to replace backups. Your backup procedures should include daily backups and weekly offsite backups.

There are several situations in which this option need be accessed.

- **Power *(hardware)* failure**
- **Media Errors *(bad disk)***
- **Remove records marked for deletion**

Before you execute the **Pack** option, check the file size of your Advanced Security files. The system will sort each of the current **"out of index"** files into new **"indexed"** files before deleting the old ones.

If you do not have enough disk space available to perform this function, an error will be generated at the time the system runs out of disk space. This, however, could be some time later, depending on the size of your data files. If your data files are **2MB** in combined size, you will need at least **2.2MB** in additional free space before proceeding with this option.

NOTE

This option will only reorganize undamaged data within your files. Therefore, you should carefully audit all information after you execute this option and make any necessary adjustments to your data.

The following files are available for maintenance:

- **User File**
- **Group File**
- **Group/User Assignment File**
- **Permissions File**
- **Authority File**
- **Company Directory File**
- **Activity Log File**

You may select individual files or all files for either of these procedures. There are buttons on the right hand side of the screen that allow you to **"Select All"** files, **"Un-select All"** files, and **"Invert Selection,"** which selects those files that were not selected in a previous pack or re-index condition. There is also a button called **"Details"** that provides pertinent information about that particular data file. This information includes the directory path and file name, the type of file, the pattern of the filename structure and the total records including those records marked for deletion in that data file.

To begin the procedure of a pack or re-index, simply <click> on the **"Start"** button, after selecting the files you wish to manage. You are then given the options to **"Pack"** or **"Re-Index"** the selected data file(s). **Pack** is a utility that physically removes any deleted records from that data file. These procedures display a **"Percentage of Completion"** graph on the screen while the files are being processed. **Re-Index** is a utility to rebuild the index file. It is also run automatically at the end of a **"Pack"** procedure.

Results:

All Records in all or specified Advanced Security Files will be packed and/or re-indexed.

MAKE COMPLETE DATA BACKUPS

Make sure that you make complete data backups as you add more and more information to your system. The file naming structure is designed to allow you to copy data files only; very quickly and easily.

We strongly recommend that the following backup procedures be followed to adequately protect your data files against any possible problems. Experience has shown that **"careless disregard"** of making adequate backups can literally cost you months of hard work and expense.

Any of the following problems could destroy all or part of your accounting information.

- **Hardware Failure of any kind (such as a hard disk failure)**
- **Power Failure or Fluctuations**
- **Improper Execution of certain operating system commands**
- **Careless Handling of Data Disks or Tapes (such as copying files the wrong direction)**

It is recommended that you make a backup of your data files on a daily basis. This does not mean for you to continue copying over the same backup that you may have made the previous day. Instead you should consider the following structure. Create five to seven daily backup sets of disks or tape cartridges, depending on your system. The number will vary based on the number of days you **"normally"** work on your files. Mark each set with the name of the day of the week that it is to be used for backup purposes. For instance, disk set or tape #1 may read Monday, disk set or tape #2 may read Tuesday, etc.

Only use these specific sets of disks or tapes on the days that are designated. This would mean that they would not be used more than once a week. Therefore, if problems were to occur and you did not realize it immediately, you could at least go back as far as a week to find your last set of valid data files. Of course the entries made during the last week may be lost, but that is better than many months or years worth of input. To go a step further, we recommend that you next make four additional sets of disks or tapes. These would be your weekly master backups. Mark them accordingly with the week number **(Week #1)** and at the end of every week, make a full backup of your data files.

Though you may have a complete daily backup for each day of the week, sometimes problems are not found within the week's time frame and all of those backups could be invalid. This way, you could go back several weeks at a time to find your last set of valid files. Next, you will want to go further and create a monthly master set of disks or tapes. You would mark them accordingly with the name of the month of the year. At the end of every month, you would then make a complete backup of your data files again.

This allows you to then go back several months at a time, if necessary, to review information or to print historically dated information. Of course, the last set of files created should be the yearly set of files done at the end of each fiscal year for archiving purposes. It is also highly recommended that all report model detail be run at this time for hard copy backup.

As an additional protection for those users with tape backup systems, it is still highly recommended that if you have a floppy disk drive on your computer that a floppy disk backup be made occasionally ***(at least monthly)*** in case a problem were to develop on the tape drive that you are using. Normally, you would not find out there is a problem until you needed to restore information, and that may be too late.

This all may sound like a considerable amount of work and inconvenience, but consider the investment involved. The largest true cost of a hardware failure or loss of information is not the loss of programs, disks, or even computers. The largest cost is that of labor and management's time. This can literally represent thousands of man hours over time. This is a large investment that should be safeguarded at all times. This program is designed for implementing security throughout the system creating and generating reports. Unfortunately, there is limited ability to protect the information created. That is entirely up to you, the user and manager, to protect your investment.

This page intentionally left blank.

CHAPTER 3 ERROR CODES

This chapter covers the **"Error Codes"** that a user may receive during the course of normal processing when the **Advanced Security Administrator** module is activated.

Error Code	Description	Resolution
Error -1	This error message will appear if the company you have accessed is not found in the company directory file. Therefore, no permissions are available.	Update and Enable Company Rights for this company.
Error -2	(Company rights not set for system-wide permissions group "_PERMALL."). This error message will appear only if the _PERMALL group has been added and has not been entirely set up.	This will require permissions to be set by the *System Manager*.
Error -3	(Option ID not found in the company permissions file.) This error message will appear when the Option ID ***(menu option or custom object)*** entered is not found in the active company's permissions file.	This will require the appropriate **Menu File** or **Custom Objects** file to be loaded using the **"Update Company Permissions"** option.
Error -4	(Access to this option denied because the permissions flag in the **"_PERMALL"** group is set to **"N"**.) This error message will appear if this option does not have access rights under the _PERMALL group.	Update the _PERMALL group to allow access to this option *(all group members will then have access)* **NOTE:** The User ID permissions do not override the **_PERMALL** group permissions.
Error -5	(Company rights not set for company wide permissions group "_PERMCO.") This error message will appear only if the **_PERMCO** group has been added and has not been entirely set up.	This will require permissions to be set by the *System Manager*.
Error -6	(Access to this option denied because the permissions flag in the "_PERMCO" group is set to "N".) This error message will appear if the active User ID is part of the _PERMCO group and this group does not have access to this option.	Update the _PERMCO group to allow access to this option *(all group members will then have access).* **NOTE:** The User ID permissions do not override the **_PERMALL** group permissions.
Error -7	(Unable to open company permissions file). This error message will appear when the Advanced Security Administrator module can not access the active company's permission file.	Verify that the active company's permission file has been created. If it has not yet been created, select the options to ***"Create Company Rights"*** and ***"Enable Company Rights."***

Error Code	Description	Resolution
Error -8	(User ID not found.) This message will appear if the User ID used to log into the system is not found.	***System Manager*** will need to add this User ID and assign rights so that this user may access the system.
Error -9	(User not enabled.) This error message will appear if the User ID used to log into the system has not yet been enabled.	***System Manager*** will need to enable this User ID.
Error -10	(User does not have access rights to this option.) This error message will appear if the active User ID does not have access rights to the option they have selected	***System Manager*** will ascertain whether this User ID requires access to said option and should change access rights accordingly.
Error -11	(Authority ID Invalid or Not Found.) This error message will appear when a user accesses an option that requires an "Authority ID" and password to continue to access said option and the Authority ID entered is not found, or the Authority is not yet set up, or the Authority's password is incorrect, or the Authority is not yet enabled.	Enter the correct Authority ID or have the ***System Manager*** create a new Authority ID.
Error -999	(Other Error.) For any other error not defined herein. If you receive an error not listed here, please contact Data Pro Accounting Software Technical Support and keep track of the events that were happening when the error occurred.	

CHAPTER 4 PRINT REPORTS

This section includes a description and sample of each report generated by the **Advanced Security Administrator** module. The reports included here reflect sample information input into the sample company and only reflect an example of the way a company may utilize certain features within this module. All modules are designed to be extremely flexible in the way you may organize data and print the corresponding reports accordingly.

Do not assume that these reports reflect the only way they may either be structured or the fashion in which they may be printed. These reports may be used as a cross reference to determine which reports you should be using in your daily activities or when trying to locate specific types of information.

STANDARD FEATURES FOR REPORTS

Here is a listing of some standard features, which can be utilized with all reports:

CTRL + O (Output Options)
Destination - Printer Choice, E-Mail or Display
Report Titles
E-mail Settings - Recipient and Subject
Range of Accounts
Data Record Retrieval
Cancel the Print Job

CTRL + O (Output Options)

You are able to change your Output Options ***(printing preference)*** at any time when you are within the **Infinity POWER** programs. By Pressing **CTRL O**, an overlay screen will appear with your available output options. You may choose to print to a Printer, send the report as an e-mail, or display the report on the screen.

If you select **"Printer,"** this will cause the output to be generated to whichever printer device you currently have as ***"active"*** in the **Windows** operating system. You may choose to change printers by <clicking> on the **"Print Options"** button and select another printer that you have set up in your Windows program. Also, by choosing **"Printer,"** you have the capability of changing the title of the report you will be printing. The standard report name will be shown, however, if you wish to overwrite it with another title, you may do so. If you select **"E-Mail,"** this will cause the output to generate an e-mail to a specific recipient. On the Output Options screen, you will need to define the recipient of the e-mail in the **"To"** field. Make sure to enter their e-mail address and not just their name. The **"Subject"** field is automatically assigned the name of the report you will be generating, however, if you wish to overwrite it with another subject, you may do so.

Be sure you have defined your **"E-Mail Host"** in the Output section of the Configuration Settings, otherwise, this feature will not be operational. Your name should be your e-mail address, not your actual name. If you select **"Display,"** this will cause the output to generate the report to the screen. All reports are generally created in an **80** or **132** column format. You may size your output window both larger and smaller to allow you to view as much of the report on the screen at once as possible.

If you are used to using the **Windows Character-based** or **UNIX/Linux** version of **Infinity POWER**, you realize that you may also send reports to a **"text"** file for a myriad of uses. You may do the same in Windows, however, you must set up a **"printer"** type in Windows that will direct the output to the file. Once this is done, any time you want to direct reports to a file, you simply select the new printer definition under Windows.

The principal applies if you want to print any report or form as a **FAX** document. Define the FAX software as a printer in Windows and simply redirect your output to that specific printer.

Range of Accounts

When asked to define the range of account numbers to report on, place your cursor on the ***"Beginning Account #"*** field and <click> the **Down Arrow *(F2 by default)*** to gain access to the account listing. You may choose to search for accounts by account number or description. Once you have selected the Beginning Account Number, <click> on the Ending Account Number field and then <click> the **Down Arrow *(F2 by default)*** to gain access to the account listing to choose your ending number.

Data Record Retrieval

This function can be done on any indexed field in the currently active system or a field the current system is integrated with. When the right mouse button is <clicked> in the field, the system will display the choices of data record retrieval.

This feature is available in most options throughout the **Infinity POWER** system. It will simplify your retrieval of records when printing reports. The data record retrieval choices are listed below.

First Record	This option will allow you to select the first record in the requested file.
Next Record	This option will allow you to retrieve the next sequential record in the file, assuming you have already selected a record.
Current Record	This option will allow you to select the last record that was accessed.
Scroll View	This option will display a scrolling screen with all records in the accessed file. You may scroll through the records and select the one of your choice. You may also change the sorting preference and search for the record in a variety of ways.
Previous Record	This option will allow you to retrieve the previous sequential record in the file, assuming you have already selected a record.
Last Record	This option will allow you to select the last record in the requested file.

Cancel the Print Job

<Clicking> on the **"Cancel"** button during the printing of a report will cancel the print job. However, keep in mind, some of the report may still be in the printer buffer at the time of cancellation.

PRINT USERS (SSA0104)

Use this option to print a profile for one or more users. This is a reporting option that allows you to see the configuration that has been set up for a single user or a range of users. When you select this option, you will be prompted to enter the beginning User ID and the ending User ID. Make your selection and prompt which sort method the report should use in printing. This report will only include information for the company that is currently loaded and active. The information included on the report includes the following fields and a sample is shown on the following page.

Fields:

- User ID
- Description
- User #
- Enabled Status (Y/N)
- Rights Set (Y/N)
- Password Established (Y/N)
- Authorities Assigned (Y/N)
- Password Change Date
- Last Password Change (Date/Time)
- Last Login (Date/Time)
- Last Logout (Date/Time)

Print Users Report

Infinity POWER Sample Company, Inc. Page 1
User Listing for Company "ins" (4) 04/28/2006

User ID	Description	User#	Enab	Rights Set	PW Auth		Next PW Change		Last PW Change		Last Login		Last Logout	
Betty	Betty Howard	4	Y	Y	Y	N	08/31/2006	12:59	04/02/2005	11:45	04/02/2005	11:52	04/02/2005	11:53
BILLJ	Bill Johnson	6	Y	Y	Y	N	12/31/2006	12:59	04/02/2005	11:46	04/02/2005	11:54	04/02/2005	11:54
JEFFK	Jeff Killinger	10	Y	Y	Y	N	09/30/2006	12:59	04/02/2005	11:47	04/02/2005	11:53	04/02/2005	11:53
JORGE	Jorge Gonzales	7	Y	Y	Y	N	04/30/2006	12:58	04/02/2005	11:46	04/02/2005	11:54	04/02/2005	11:54
LEON	Leon Hernandez	8	Y	Y	Y	N	05/31/2006	12:58	04/02/2005	11:47	04/02/2005	11:54	04/02/2005	11:54
LILLY	Lillian Rodriguez	11	Y	Y	Y	N	05/15/2006	12:58	04/02/2005	11:48	04/02/2005	11:53	04/02/2005	11:53
Mary M	Mary McArther	3	Y	Y	Y	N	07/31/2006	12:58	04/02/2005	11:44	04/02/2005	11:54	04/02/2005	11:55
PATW	Pat Williams	9	Y	Y	Y	N	05/31/2006	12:58	04/02/2005	11:47	04/02/2005	11:53	04/02/2005	11:54
SCOTT	Scott Thompson	1	Y	Y	Y	N	06/30/2006	12:58	04/02/2005	11:43	04/02/2005	11:14	04/02/2005	11:15
SCOTT2	Scott Robinson	2	Y	Y	Y	N	01/31/2006	12:57	04/02/2005	11:44	03/18/2005	12:49	03/21/2005	09:08
SYSADM	System Administrator	0	Y	N	Y	N	07/31/2006	12:57			04/02/2005	12:01	04/02/2005	11:52
TERRYD	Terry Diaz	12	Y	Y	Y	N	04/30/2006	12:57	04/02/2005	11:48	04/02/2005	11:55	04/02/2005	11:55
TONY	Tony Hampton	5	Y	Y	Y	N	04/30/2006	12:56	04/02/2005	11:45	04/02/2005	11:55	04/02/2005	12:01

PRINT A GROUP (SSA0204)

Use this option to print a profile for one or more groups. This is a reporting option that allows you to see the configuration that has been set up for a single group or a range of groups. When you select this option, you will be prompted to enter the beginning Group ID and the ending Group ID. Make your selection and prompt for which sort method the report should use in printing. This report will only include information for the company that is currently loaded and active. The information included on the report includes the following fields and a sample is shown on the following page.

Fields:

- Group ID
- Description
- Group #
- Enabled Status (Y/N)
- Rights Set (Y/N)

Print A Group

Infinity POWER Sample Company, Inc. Page 1
Group Listing for Company "ins" (4) 04/28/2006

Group ID	Description	Group #	Enabled?	Rights Set?
Accounting	Accounting Department	0	Y	Y
Executive	Executive Management	2	Y	Y
Manufact	Manufacturing Department	4	Y	Y
Marketing	Marketing Department	3	Y	Y
Sales	Sales Department	1	Y	Y
Shipping	Shipping Department	5	Y	Y

PRINT AN AUTHORITY (SSA0706)

This option allows you to print information about your authorities. By selecting this option, you will be able to print out the specific data on each authority set up in the system. This may include all authorities that have been set up throughout the entire system or just authorities set up for a specific User ID. When you select this option, seven **(7)** data items will appear on the screen.

Data Item	Description
Type of Report	The choices for this report are: **By Authority** or **By Option.** This provides you with the two major criteria in which to run the report. If you are looking for a listing of the options that have been assigned to an authority, then choose **"By Authority."** If you are looking to find which authorities have been assigned to a specific option or all options, then choose **"By Option."**
All Authorities	By <clicking> on this check box, you will be telling the system to print all authorities based on the way you respond to the following prompts. If you only want to print a single or a few authorities in the currently loaded company, you should make sure this check box is un-checked.
User ID	If you have left the check box blank in the data item above, the system will then prompt you in this field for the User ID that you want to print authorities for. You must type in a valid **User ID** or leave the field blank to proceed. If you have checked the check box in the data item above, the system will skip by this field during this process.
All Options	<Click> on this checkbox if your desire is to print all authorities either for all options or for the user specified in data item #2. If this is not what you want to do, then make sure to un-check this check box.
System	This data item allows you to specify which system or accounting modules should be included for printing by this option. You may leave the field blank which will include all systems or specify the two or three character **System ID** representing the specific **Infinity POWER** module. For example, use **"GL"** for the General Ledger module.
Option ID	If you want to print for a specific **Option ID**, you must specify it in this field. This data item does not have the scroll search near match window, therefore, your entry must be specific ***(i.e., GL0101)***.
All Companies	This data item allows you to specify whether the print function should include only the currently loaded company or all companies where the authorities have been assigned. Enter your choice accordingly.

When you <click> on the **"Start"** button to validate this screen, the system will print the authorities based on the criteria entered on this screen. You will then be at the same screen again where you can proceed to print additional authorities as desired. When you are done, <click> on the **"Close"** button to exit to the menu. The information included on the report includes the following fields and a sample is shown on the following page.

Fields:

- User ID
- Enabled (Y/N)
- Company
- System
- Option ID

Print an Authority

Infinity POWER Sample Company, Inc. — Page 1
Authority Listing — (4) 04/28/2006
By Authority -- Company "ins"

User ID	Co	Sys	Option ID	Enabled?
Betty	ins	SO	CREDIT LIMIT	Y
JORGE	ins	SO	CHANGE HOLD	Y

LIST LOGGED-IN USERS (SSA0610)

Use this option to display a list of all users currently logged-in to your system. By simply selecting this option, the system will automatically generate a report to the printer of all of the users that are currently logged-in to the system.

The list will include all of the User IDs and their login time on the system.

Logged In Users

Infinity POWER Sample Company, Inc. Page 1
Logged-In Users (4) 04/28/2006

User ID	Login Time
SYSADM	12:01:51

* Number of records printed: 1

PRINT ACTIVITY LOG (SSA0615)

This option allows you to display a history of events reflecting access to your system. To produce an activity log, you must first have **Activity Tracking** turned on in the Security Configuration. If it is set to be on, you will be prompted for a beginning and ending **Date/Time** range to include in this report. The number that will be prompted for is in the following format.

Year/Month/Day/Hour/Minute/Second
or
040917171528

The format illustrated here would represent September 17, 2004 followed by 5:15:28 P.M. All time is calculated in military time format. When you select this beginning or ending range, you may press enter to use the near match scroll search to find the exact reference to include on this report. Therefore, you may print this report in a wide variety of ranges including months, weeks, days or hours. The results that print on the report will vary depending on how you have the Security Configuration set. It may, however, contain a variety of data if you have changed the configuration over a period of time.

In the configuration, you may choose to implement Activity Logging at three **(3)** levels. These levels include the following choices:

- **Successful Login**
- **Login Attempts**
- **Option Selection**

Based on the system being configured for either **"Successful Login"** or **"Login Attempts,"** the report will print the Date, Time, User ID, Event ***(Login or Logout)*** and its Code. Codes are numbers such as **"0"** for a normal occurrence such as a normal login or logout. Code **"1"** illustrates that the login attempt was unsuccessful.

If you have the system configured for ***"Successful Login,"*** the only information that will print on the report will be those logins where the user was successful in getting into the system. If the system is configured for ***"Login Attempts,"*** the report will include both successful logins as well as those attempts where the user was unsuccessful in getting into the system. The ***System Manager*** may want to set this flag occasionally just to verify who is attempting to access the system and is failing.

By setting the system to **"Option Selection,"** the system will be tracked at all possible levels. This includes all logins and logouts, successful or not, and once logged in, which options the user selected and whether they encountered any errors or not.

This is the ideal report variance for System Managers who want to see clearly everything that all users are doing in their system. However, this can become a disk intensive option to have turned on. Therefore, occasional purging of files may be required to free up additional disk space.

When this option is selected the event code will go beyond whether the user logged in or not, it will show the specific **System** and **Option ID** that the user accessed. It will also include the company that was affected. You may print this option as often as desired. When the report is completed, you will be automatically returned to the menu. The following page shows a sample of the report with the **Activity Logging Level** set in the Security Configuration to **"Option Selection."**

The information included on the report includes the following fields.

Fields:

- Date
- Time
- User ID
- Event *(System, Option ID, Login/Logout)*
- Company
- Code

Activity Log

Infinity POWER Sample Company, Inc.
Activity Log

Page 1
(4) 04/28/2006

Date	Time	User ID	Event		Code
04/02/2005	13:29:05	BETTY	Login		0
04/02/2005	13:29:05	SYSADM	Logout		0
04/02/2005	13:29:11	BETTY	GL GL0101	ins	0
04/02/2005	13:29:49	BETTY	GL GL0201	ins	0
04/02/2005	13:29:58	BETTY	GL GL0400	ins	0
04/02/2005	13:30:10	BETTY	GL GL0202	ins	0
04/02/2005	13:30:25	JORGE	Login		0
04/02/2005	13:30:25	BETTY	Logout		0
04/02/2005	13:30:30	JORGE	SO SO0100	ins	0
04/02/2005	13:31:09	JORGE	SO SO0105	ins	0
04/02/2005	13:31:51	JORGE	SO SO0202	ins	0
04/02/2005	13:32:15	JORGE	SO SO0209	ins	0
04/02/2005	13:32:31	JORGE	SO AR0400	ins	0
04/02/2005	13:32:40	JORGE	SO IM0100	ins	0
04/02/2005	13:32:52	PATW	Login		0
04/02/2005	13:32:52	JORGE	Logout		0
04/02/2005	13:32:58	PATW	AP AP0201	ins	0
04/02/2005	13:33:16	PATW	PO PO0100	ins	0
04/02/2005	13:33:22	PATW	PO PO0201	ins	0
04/02/2005	13:33:45	PATW	JC JC0107	ins	0
04/02/2005	13:34:09	PATW	JC JC0400	ins	0
04/02/2005	13:34:21	SYSADM	Login		0
04/02/2005	13:34:21	PATW	Logout		0
04/02/2005	13:34:28	SYSADM	SSA SSA0615	ins	0

This page intentionally left blank.

INDEX

A

Access Rights 1-8, 1-9, 1-11, 1-12, 2-14, 2-36
Activity Log 2-35
Activity Log File 1-6
Activity logging enabled? 2-33
Activity logging level 2-33
Add a Group 2-14
Add An Authority 2-26
All Authorities 2-28, 2-29, 2-31
All Authorities? 2-27, 2-28, 4-6
All companies 2-31
All Companies 2-18, 2-27, 2-28, 2-29, 2-30
All companies? 2-27, 2-28, 2-30, 4-6
All Options 2-27, 2-28, 2-29, 2-30, 2-31
All Options? 2-27, 2-28, 2-30, 4-6
Assign Rights? 2-14
Assign Users To Groups 2-23
ASSIGN USERS TO GROUPS 2-23
Authorizations 1-5

C

Change a Group 2-21
Change a User 2-13, 2-21
Change An Authority 2-27
Change password attempts 2-33
Company 2-24, 2-28, 2-29, 2-31
Confirm access denied? 2-33
Control File 1-6
Copy a Group 2-14
Copy An Authority 2-28, 2-29
Copy Rights From? 2-14
Create Company Rights 2-23
Custom Object File 1-6
Custom security objects 2-25

D

Data Backups 2-38
Data File Descriptions 1-6
Delete a Group 2-14
Delete An Authority 2-27
Delete Company Rights 2-25
Description 2-4, 2-12, 2-15, 2-21
Disable All Authorities? 2-14
Disable All Permissions? 2-14
Disable Auth? 2-14
Disable Perm? 2-14
Display Disabled Menu Options? 1-8, 2-33

E

Enable All Authorities? 2-14
Enable All Permissions? 2-14

Enable Auth? 2-14
Enable Company Rights 2-25
Enable Perm? 2-14
Enabled 2-4, 2-5, 2-8, 2-12, 2-27
Enabled? 2-14
Error 3-1, 3-2
Error Codes 3-1

F

Force Password Change 1-8
FORCE PASSWORD CHANGE 2-33

G

Group 1-6, 1-7
Group ID 2-15, 2-17, 2-18, 2-20

I

Introduction 1-1

L

List Logged 4-8
List Logged-In Users 4-8
Login attempts 2-33
Login Control 1-8
Login enabled 2-33

M

Maintain Data Files 2-37
Make Complete Data Backups 2-38

N

New User ID 2-30

O

Old User ID 2-30
Option ID 2-27, 2-28, 2-29, 2-30, 2-31, 4-6
Overview Of A Typical Configuration 1-8

P

Password 2-4, 2-5, 2-7, 2-8, 2-11
Password Aging 2-33
Password aging enabled? 2-33
Password Change Date 2-4, 2-8
Password Change Time 2-5
Password Control 2-35
Password required? 2-33
Permall 1-8
Permco 1-8
Print A Group 4-4
Print a User 4-2
Print Activity Log 4-10
Print An Authority 4-6

Print Users 4-2

R

Replace An Authority 2-30

S

Security Configuration 2-33, 2-37
Security Configuration File 1-6
Security Objects 1-3
Set All Companies? 2-14
Set Up And Maintenance 2-1
Set Up Authorities 1-12
Set Up Groups 1-8, 2-14, 2-16
Set Up Users 1-8, 2-1
Special Groups 1-9
STANDARD FEATURES FOR REPORTS 4-1
Standard menu options 2-24
SET UP USERS;Add a User;Description;Enabled?;Password Change Date;Password Change Time;Enable All Permissions?;Disable All Permissions?;Enable All Authorities?;Disable All Authorities?;Set All Companies?;Copy Rights From?;Set Password?;Assign Rights?;System;Enable Perm?;Enable Auth?;Disable Auth?;Display Group Info?;Change a User;Delete a User 2-1
System 2-3, 2-4, 2-5, 2-6, 2-7, 2-8, 2-9, 2-10, 2-10, 2-11, 2-12, 2-13, 2-14, 2-15, 2-16, 2-17, 2-18, 2-19, 2-19, 2-20, 2-21, 2-22, 2-26, 2-27, 2-27, 2-28, 2-29, 2-30, 2-31, 2-32, 4-6
System Configuration 1-9, 2-36
System Integration 1-6
System Manager 1-11, 2-36

T

Type of Report? 4-6

U

Update Company Rights 2-24
Update custom security objects? 2-24
Update standard menu options? 2-24
Update using custom menu in directory 2-24
Use access rights from company 2-24
Use default company? 2-33
User 2-1, 2-3, 2-4, 2-6, 2-7, 2-7, 2-8, 2-8, 2-10, 2-11, 2-12, 2-13, 2-14, 2-21, 2-23
User ID 2-3, 2-4, 2-6, 2-7, 2-8, 2-11, 2-14, 2-23, 2-26, 2-28, 2-29, 2-31, 4-6
User Info 2-14
User Logging 1-5

V

Vendor Inquiry 2-14