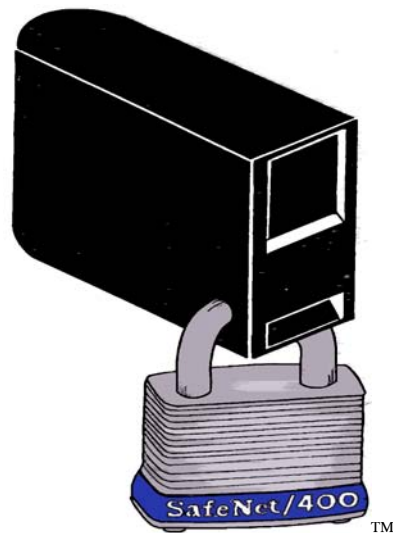


SAFENET/400

FOR THE IBM SYSTEM i5

IMPLEMENTATION GUIDE

Version 8.50



How to contact us

Direct all inquiries to:

Kisco Information Systems
89 Church Street
Saranac Lake, New York 12983

Phone: (518) 897-5002
Fax: (518) 897-5003

SafeNet/400 Website: <http://www.kisco.com/safenet>

SafeNet/400 Support Website: <http://www.kisco.com/safenet/support>

Visit the SafeNet/400 Web Site at [HTTP://WWW.KISCO.COM/SAFENET](http://www.kisco.com/safenet)

TABLE OF CONTENTS

CHAPTER 1 - OVERVIEW	1.1
<i>SAFENET/400 FEATURES</i>	<i>1.3</i>
<i>SYSTEM REQUIREMENTS</i>	<i>1.6</i>
CHAPTER 2 - PLANNING FOR SECURITY	2.1
CHAPTER 3 - SAFENET/400 QUICKSTART	3.1
<i>ADDITIONAL INITIAL STEPS</i>	<i>3.9</i>
<i>SAFENET ADMINISTRATOR</i>	<i>3.10</i>
CHAPTER 4 - IMPLEMENTATION	4.1
<i>DECIDING HOW TO USE SAFENET/400</i>	<i>4.1</i>
<i>PLANNING FOR SAFENET/400 SETTINGS</i>	<i>4.3</i>
<i>STEPS TO SET UP SAFENET/400</i>	<i>4.4</i>
<i>EXAMPLE OF USER SETUP</i>	<i>4.6</i>
<i>AUTOMATIC ENROLLMENT</i>	<i>4.8</i>
<i>POST AUTOMATIC ENROLLMENT</i>	<i>4.10</i>
CHAPTER 5 - SPECIAL SAFENET/400 TECHNICAL CONSIDERATIONS	5.1
<i>INSURING NETWORK REQUESTS ARE LOGGED</i>	<i>5.1</i>
<i>CHANGING SPECIAL SAFENET/400 SETTINGS</i>	<i>5.2</i>
<i>EXIT POINT EXCLUSION OPTION</i>	<i>5.6</i>

Special Notices

The following terms, which are denoted by TM in this publication, are trademarks of the International Business Machines Corporation:

System i5	OS/2	DB2 for System i5
iSeries	PC5250	DB2 for OS/390
OS/400	DRDA	DB2 Connect
PC Support/400		iSeries Access for Windows

The following terms, which are denoted by an asterisk (*) in this publication, are trademarks of Microsoft Corporation:

Windows XP	Microsoft Excel
Microsoft Explorer	Microsoft Access
ODBC	Microsoft Query
Windows Vista	Windows 2000

The following terms, which are denoted by a double asterisk (**) in this publication, are trademarks of other companies:

ShowCase Strategy (Showcase Corporation)

SafeNet/400 Implementation Guide

Chapter 1 - OVERVIEW

What is SafeNet/400?

SafeNet/400 is a powerful yet easy to use tool for the IBM System i5™ that enables you to exercise full control over users who access your system via network connections. These network connections can be through personal computers that are attached to the System i5 over twinax, or LAN, WAN, Ethernet, etc.

SafeNet/400 provides the means to secure functions and objects on your System i5, using IBM-provided APIs and exit points, without having to write your own programs. Its flexibility gives you the power to tailor it precisely to the needs of your installation.

SafeNet/400 is non-invasive to your existing System i5 security. **SafeNet/400** does not change any of your existing security settings or object level authorities other than exit point program registrations.

SafeNet/400 never impacts the performance of your “green screen” applications. It only operates with network traffic accessing your database outside of normal “green screens”.

Isn't System i5 Security sufficient?

When users gain entry to the System i5 through a 5250 emulation session on a PC, or network client, access to objects on the system can be controlled by OS/400™ system values, individual user profiles and your own menu security.

However, when these same users are entering your System i5 through a spreadsheet or data base program on the client, your menu security and some user profile settings are circumvented. Unless you have established strict object-level security on your System i5, and use adopted authority, your system and all its data is available to those programs on the PC.

This means users can not only see data on your System i5, they can copy it, add to it, or even delete it. **SafeNet/400** can help you control this.

Who should use SafeNet/400?

SafeNet/400 is designed for any installation where intelligent clients (PCs) communicate with a System i5. These clients have access to the data on the System i5 whether they connect to the system through a LAN or twinax, whether they are local or remote, or whether there is a single System i5 or multiple systems in the network.

How does SafeNet/400 work?

SafeNet/400 captures every incoming request from clients who attempt to access server functions of OS/400, such as SQL, ODBC and PC file transfers. It looks at each request, then acts on each one, depending on the level of security that you have defined.

You establish the rules for your System i5 and use **SafeNet/400** Security Level settings and object authority to enforce them. The rules are checked, and when a request is received, those that are permitted are accepted and those that are not are rejected.

Which servers are being accessed by the clients and where are the requests coming from?

With so many different software packages in use on the desktop, it has become very difficult to determine which server functions are being used by each program.

The logging features of **SafeNet/400** give you the ability to determine the server function and data that is being accessed, along with a record of where the requests are coming from. You can then use this information to set up the server functions, user profiles and data authorities.

See the chapters on 'Reports' and 'Testing your Security Settings' in the [SafeNet/400 Reference Guide](#) for detailed information on the transaction logging features of **SafeNet/400**.

SafeNet/400 Features

The following features of **SafeNet/400** give you the ability to implement client/server security on your System i5, from simply logging activity to completely restricting access to system functions and data. **SafeNet/400** lets you:

Generate Audit Reports

SafeNet/400 tracks each request coming from a client into the System i5. It stores this information in a log that you can review. The log indicates who is accessing your system, which server function on the System i5 they are requesting, what data or objects they are using, and whether the request was accepted or rejected.

Limit Access to Server Functions, Based on User Profile

SafeNet/400 can be set up to limit access to specific server functions on the System i5 based on the individual's user profile.

Exclude Users from Server Functions

SafeNet/400 allows you to turn off individual server functions. For example, you can completely exclude the file transfer function for all users on your System i5 if you wish.

You can also exclude users from specific servers, or all servers, based on the time of day or day of the week.

Limit Access to Objects within Server Functions, Based on User Profile

SafeNet/400 gives you the ability to implement object level security over clients that are accessing the various server functions on the System i5. Authority is granted by user profile to the individual servers, then each user is granted authority to objects on the system.

Limit Access to FTP, TELNET

SafeNet/400 allows you to define specific IP addresses or ranges of IP addresses to control access to *FTP* or *TELNET*.

What is a Server Function?

With iSeries Access for Windows, IBM provides many basic client/server functions such as file transfer, virtual printing and file serving through Network Neighborhood operations.

Each function in iSeries Access for Windows uses both client and server programs. For instance, the file transfer process uses a program on the PC (the client) to request a file from the System i5 (the server).

The System i5 has several specialized **server functions** that are included as part of OS/400, and each request from a client uses one of these server functions on the System i5.

Server support provided with PC Support/400 was **original** support and was designed for original clients.

Server support provided with iSeries Access for Windows, beginning with OS/400 Version 3 Release 1, is called **optimized** support and is for optimized clients.

Original Support

Original clients:

- DOS
- DOS Extended
- OS/2*

Original servers in OS/400:

- Transfer function server for transferring files between personal computers and System i5
- Remote SQL server for remote data base access
- Data queue server for client/server application development
- Message function server for sending and receiving messages
- License management server to help manage client application licenses
- Virtual print server for remote print support
- Shared folder server for file serving
- Remote command server to submit remote commands to System i5 through DDM

Optimized Support

Optimized clients:

- Windows95* (32 bit applications)
- WindowsNT*
- Windows 2000*
- Windows XP*
- Windows Vista*
- Linux

Optimized servers:

- File server that replaces shared folders servers
- Data base server for file transfer and remote SQL functions
- Network print server to provide same functions as virtual print server, plus additional print management functions
- Data queue server
- Remote command/program call server to provide ability for personal computer applications to issue commands and call programs on System i5 and pass results back to client
- Central server that provides services such as license management and other client management functions
- APPC password management server that provides password management functions for host servers with APPC support
- Signon server that provides password management functions for host servers with sockets support
- Server mapper that provides current server port number to client on a connection request

Most OS/400 servers are included in the Host Server option of OS/400. These servers are used by iSeries Access for Windows but are designed so that other client products can use them also.

System Requirements

SafeNet/400 is supported for OS/400 Version 2 Release 3 and later.

SafeNet/400 V8.0 requires OS/400 Version 5 Release 2 and above.

PTFs

- There are specific minimum cumulative PTF levels required for **SafeNet/400** to work properly with the various server functions. Make sure you check the current PTF information at <http://www.kisco.com/snptfs.htm>.
- It is also recommended that you stay current with your MS Windows and iSeries Access for Windows Service Packs.

System Library List Entries

Library QSYS2 is required by **SafeNet/400** to gain access to necessary IBM OS/400 APIs. Please make sure your QSYSLIBL system value contains an entry for **QSYS2**.

Chapter 2 - PLANNING FOR SECURITY

Why do clients require special security planning?

When planning for security for your System i5, there are features available to you as part of OS/400 that work well for users connecting to your system via terminals or 5250 emulation sessions. These features include:

- User class and special authorities
- Allowing access to applications through menus only
- Setting LIMIT CAPABILITIES parameter to *YES to eliminate the command line
- RVKOBJAUT and GRTOBJAUT commands

Simply using menu security and selecting the appropriate user class can satisfy most of the issues you have in regard to users who are working with data on your System i5.

However, when these same users are accessing your System i5, not through menus that you have set up, but through a spreadsheet application running on an intelligent client, you could have a security exposure. Unless you have implemented full object-level security and use adopted authority for everything on your System i5, that PC spreadsheet program can upload data, download data, add or delete data on your System i5.

This is where **SafeNet/400** can assist you. **SafeNet/400** gives you the power to plan for and implement the same high level of security for your clients as you currently have for your “green screen” users. By using **SafeNet/400** Security Level settings, you can restrict server functions and establish specific authority to objects.

SafeNet/400 and OS/400 Security

SafeNet/400 co-exists with all the built-in features of OS/400 security. Whether your system security level is set at 10, 20, 30, 40 or above, **SafeNet/400** will perform authority checking accordingly.

SafeNet/400 does not replace or override OS/400 security. It works on top of OS/400. If you allow a user the right to delete a file through **SafeNet/400**, but OS/400 does not allow the same authority, the request will be rejected. If OS/400 allows data deletion rights and **SafeNet/400** does not, the request will also be rejected.

SafeNet/400 Object Authorities

SafeNet/400 uses Data Rights and Existence Rights similar to those used by OS/400 to check authority.

Data Rights

READ - a user can:

- Display contents of an object, such as viewing records in a file
- Run a program
- Access the objects in a library

WRITE - a user can:

- Add - add entries to an object, such as adding records to a file
- Update - change entries in an object, such as changing records in a file

DELETE - a user can:

- Remove entries from an object, such as deleting records from a file

Existence Rights/Management Rights

A user can:

- Delete the object
- Transfer ownership of the object
- Move the object
- Create a new object
- Remove/add members

Group and Supplemental Profile Support

It is highly recommended that for simplicity of setup, you purchase an unlimited user license of **SafeNet/400**. The unlimited user license allows you to define *PUBLIC and group profiles within **SafeNet/400**. This significantly reduces the complexity of **SafeNet/400** administration.

SafeNet/400 supports group and supplemental profiles only if you purchased an unlimited user license of the product. If you need group profile support, please contact technical support for information on how to order a user license upgrade.

If you use group profiles, please be aware of the following:

1. The group profile name is retrieved from the OS/400 user profile
2. **SafeNet/400** will mix or combine individual authorities with group authorities.

If **SafeNet/400** finds that an individual is authorized to a particular server, but not the object, **SafeNet/400** will then check to see if a group profile is authorized to the object. **SafeNet/400** allows a profile to use objects or servers based on combined authority of individual and group profiles.

****PUBLIC Authority***

If you have purchased an unlimited **SafeNet/400** license, you can use *PUBLIC authority. With *PUBLIC you can assign servers, objects, SQL, FTP and path names that the general public will have authority to. Used in conjunction with exclusions, this provides powerful OS/400-like authority entries that simplify administration.

Security look up routines

SafeNet/400 checks all possible authority and object/library combinations.

As soon as a match is found, the acceptance or rejection will be processed and returned at that point. All authority checking routines will stop and **SafeNet/400** will no longer continue examining name combinations.

To incorporate *PUBLIC authorities and exclusions, **SafeNet/400** will perform the authority checking according to the following sequence:

Server Lookups

<i>Is the</i>	<i>authorized to</i>
User	Specific Server *ALL Servers
Group/Supplemental	Specific Server *ALL Servers
*PUBLIC	Specific Server *ALL Servers

Object Lookups

<i>Is the</i>	<i>authorized to</i>	
User	Library	Specific Object
Group	Library	Specific Object
Supplemental Group	Library	Specific Object
*PUBLIC	Library	Specific Object
User	Library	Generic Object
Group	Library	Generic Object
Supplemental Group	Library	Generic Object
*PUBLIC	Library	Generic Object
User	Library	*ALL
Group	Library	*ALL
Supplemental Group	Library	*ALL
*PUBLIC	Library	*ALL

<i>Is the</i>	<i>authorized to</i>	
User	*ALLLIB	*ALL
Group	*ALLLIB	*ALL
Supplemental Group	*ALLLIB	*ALL
*PUBLIC	*ALLLIB	*ALL

Reminder: Remember that the base license of **SafeNet/400** provides support for up to 25 network users on your system. If you wish to have support for Group and/or Supplemental profiles and *PUBLIC, you must purchase a license for an unlimited number of users. At the unlimited level, there are additional features and controls that you can use to protect your system and simplify maintenance of your rules. If you would like to test running **SafeNet/400** at the unlimited user level, please contact our technical support staff to request an authorization for an unlimited user test.

Chapter 3 - SAFENET/400 QUICKSTART

Quickstart will enable you to begin using **SafeNet/400** immediately to track client/server activity on your System i5, without affecting any of your current users.

Quickstart involves turning on Security Level 1 - Unlimited Access, Logging Level A (ALL) to permit full access to the server functions while logging all requests, for a minimum of two weeks. During that time you can review the log to see which clients are accessing the various server functions. At the end of the two-week period you should have enough information to help you decide how to configure **SafeNet/400** for your installation.

You may wish to collect more data for a longer period of time based on your particular installation. Do your best to capture all the types of transactions and network activity at your site.

See the chapters on 'Reports' and 'Testing your Security Settings' in the [SafeNet/400 Reference Guide](#) for detailed information on how to review the information that is being logged.

Quickstart is made up of the following steps:

1. Install SafeNet/400, modify your startup program for logging
2. Ensure logging is active; you will want to collect 2-4 weeks of data
3. Set up SafeNet Admin and Super Admin profiles
4. Set Future Security Settings
5. Reduce non-critical logging (Telnet, data queues, virtual printers, etc.)
6. Develop your *PUBLIC policy and group profile assignments (for unlimited user licenses)
7. Set up *PUBLIC user to Server, to Object, to FTP, to SQL, etc. in SafeNet/400 (for unlimited user licenses)
8. Set up group authorities other than *PUBLIC in SafeNet/400
9. Set up any 'Super Trusted Users' in SafeNet
10. Set up Alert notifications
11. Use PCTESTR to test all the historical transactions against Future Settings and display only 'Rejected' transactions. You will find PCTESTR on the Special Jobs Menu, **Option 10 – On-line Transaction Testing**.
12. Make changes to SafeNet/400 settings as required based on results of PCTESTR
13. TEST, TEST, TEST
14. Flip the 'Future' and 'Current' settings (User F22 in the WRKSRV command)

These steps are described in detail on the following pages.

Begin Quickstart

Set up Administrative profiles

If you wish to use a profile other than SAFENET or QSECOFR, or wish to allow limited users to access some of the **SafeNet/400** management options, see 'SafeNet Administrator' on page 3.10 of this guide.

If the SafeNet/400 Main Menu is not displayed, type

GO PCSECLIB/SN1

Follow these steps to begin logging requests:

1. Sign on as SAFENET or QSECOFR, or another SafeNet/400 Super Admin profile.

From the SafeNet/400 Main Menu select **Option 1 - Work with Server Security Settings** or use **WRKSRV** command

```
SafeNet/400
File Edit View Communication Actions Window Help
-----
SN1
MPR400
SafeNet/400 Version 8
Network Resource Security
Main Menu

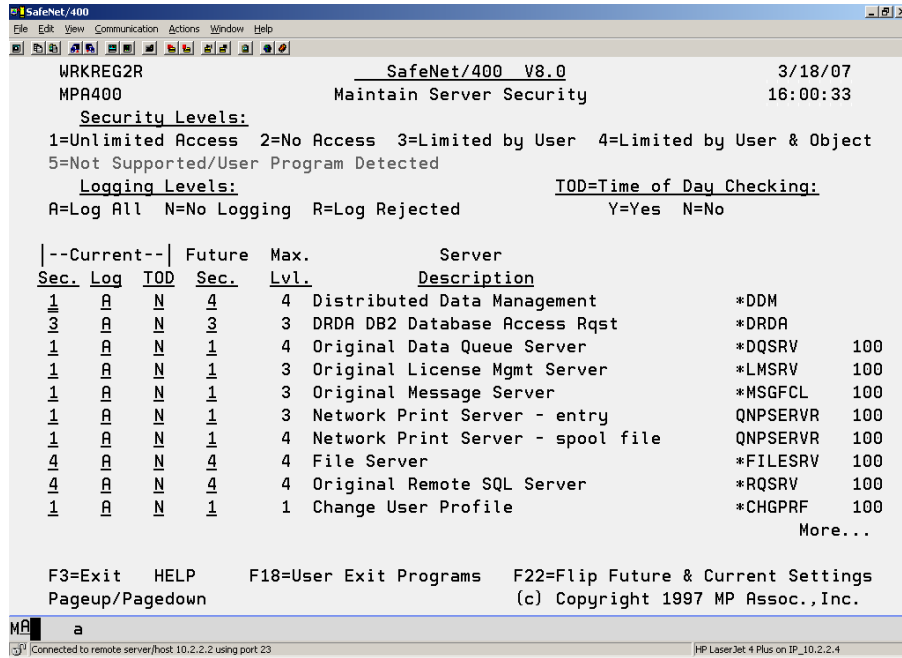
Select one of the following:
Level Required Fast Path
1. Work with Server Security Settings All WRKSRV
2. Work with User to Server Security 3 or 4 WRKUSRSRV
3. Work with User to Object Level Security 4 WRKUSROBJ
4. Work with User to SQL Statement Security 4 WRKUSRSQL
5. Work with User to FTP Statement Security 4 WRKUSRFTP
6. Work with User to CL Command Security 4 WRKUSRCMD
7. Work with User to Long Path Names 4 WRKUSRPTH
8. Work with TCP/IP Address Security 3 or 4 WRKTCPIPA
9. Work with TELNET Auto-Signon Security 3 or 4 WRKSIGNON
10. Go to Special Jobs/Setup Menu (SN2)
11. Go to Setup Reports Menu (SN3)
12. Go to Analysis Reports Menu (SN4) 80. Install Menu
13. Go to DHCP Menu (SN6) 90. Signoff

(C) Copyright 1997-2005 MP Associates of Westchester, Inc. All Rights Reserved.
Selection or command
===>

F3=Exit F4=Prompt F9=Retrieve F12=Cancel
F13=Information Assistant F16=System main menu

MB a
Connected to remote server/host: 10.2.2.2 using port 23 HP LaserJet 4 Plus on IP_10.2.2.4
```

The *Maintain Server Security* screen is displayed.



2. In the *Sec* column, **type 1** (Unlimited Access) and in the *Log* column **type A** (Log All) for all the servers. (This should already be done as the default during the installation process.)

Leave TOD (Time of Day) set to N. Use this option carefully. A change to this value is effective immediately.

Don't change anything in the *Future Settings* column at this time. It will be set to the recommended Server Level by default.

Note: The server functions are listed on multiple screens. **PageDown** to ensure you enter a security and logging level for all the servers.

When you have finished setting up all the servers, press **ENTER**.

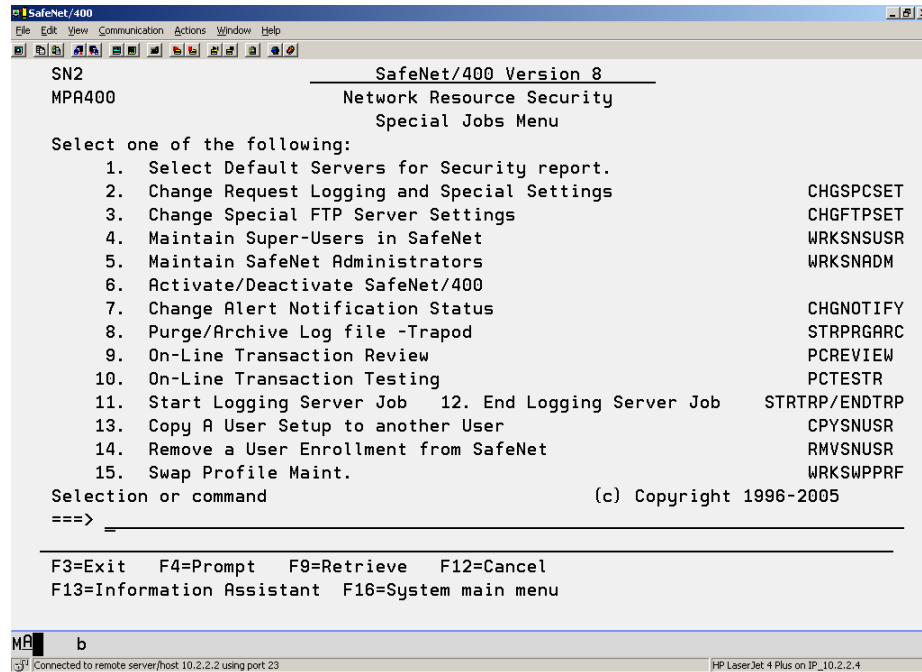
Due to a potentially high transaction rate and logging overhead, you will probably want to limit logging on several of the servers after you have become familiar with their transactions. Some of the servers where you can safely limit transaction logging are:

Telnet	Network Print
Signon Server	Message Servers
License Management Servers	Data Queue Servers

3. **Press F3** to return to the SafeNet/400 Main Menu.

4. Select **Option 10 - Go to Special Jobs/Setup Menu** or use **GO SN2** command

The Special Jobs Menu is displayed.



The screenshot shows a terminal window titled 'SafeNet/400' with a menu of 15 options. The window has a menu bar with 'File', 'Edit', 'View', 'Communication', 'Actions', 'Window', and 'Help'. The main content area displays the following text:

```
SN2                               SafeNet/400 Version 8
MPA400                            Network Resource Security
                                   Special Jobs Menu

Select one of the following:
  1. Select Default Servers for Security report.
  2. Change Request Logging and Special Settings           CHGSPCSET
  3. Change Special FTP Server Settings                   CHGFTPSET
  4. Maintain Super-Users in SafeNet                     WRKSNSUSR
  5. Maintain SafeNet Administrators                     WRKSNADM
  6. Activate/Deactivate SafeNet/400
  7. Change Alert Notification Status                     CHGNOTIFY
  8. Purge/Archive Log file -Trapod                      STRPRGARC
  9. On-Line Transaction Review                          PCREVIEW
 10. On-Line Transaction Testing                          PCTESTR
 11. Start Logging Server Job   12. End Logging Server Job  STRTRP/ENDTRP
 13. Copy A User Setup to another User                   CPYSNUSR
 14. Remove a User Enrollment from SafeNet               RMVSNUSR
 15. Swap Profile Maint.                                 WRKSWPPRF

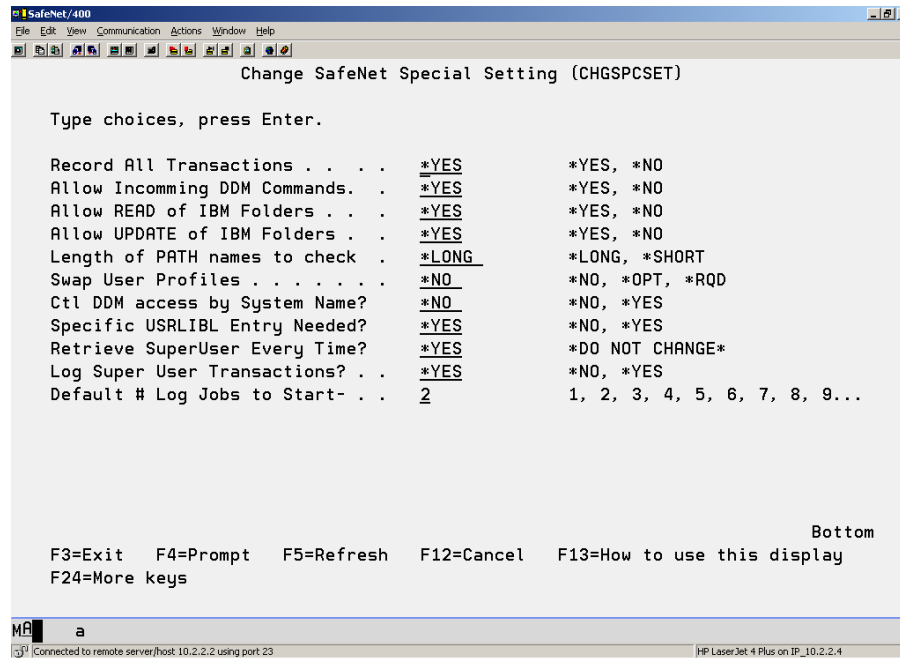
Selection or command                                     (c) Copyright 1996-2005
===> _____

F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel
F13=Information Assistant  F16=System main menu
```

At the bottom of the window, there is a status bar with 'MPA b' on the left and 'HP LaserJet 4 Plus on IP_10.2.2.4' on the right. A small icon and text 'Connected to remote server/host: 10.2.2.2 using port 23' are visible in the bottom left corner.

5. Select **Option 2 - Change Request Logging and Special Settings** or use **CHGSPCSET** command

The *Change SafeNet Special Setting* screen appears.



6. Make sure the first parameter (Record all Transactions) is set to ***YES (Logging Function On)** or use the command **CHGSPCSET LOGALL(*YES)**

Accept the defaults on the remaining options, and **ENTER**.

7. **F3** to return to the SafeNet/400 Main Menu.
8. Modify your STARTUP Program

You must issue the STRTRP command to activate the SAFELOGING subsystem at system startup time. Modify your system startup program to issue this command: **PCSECLIB/STRTRP**

You can also issue this command from any command line

Reminder: Because OS/400 allocates exit programs at startup (IPL) only, once you have installed **SafeNet/400** and have completed the Quickstart, at the earliest opportunity you should perform an IPL or end your system to a restricted state, then restart the system. This will "turn on" all of **SafeNet/400's** processes.

Transaction Logging Subsystem (SAFELOGING)

In Step 8 above, it is recommended that you change your start up program to automatically start the log recording subsystem at IPL. If you do not make these changes, the **SafeNet/400** data queue can become full and cause network response issues.

SafeNet/400 includes a function that senses when the queue is full and forces the log recording subsystem to start. However, this should not be relied upon as a normal startup method.

If you are unfamiliar with this requirement, please see the section on 'Insuring network requests are logged' in Appendix A of this manual.

You have now performed all of the steps necessary to complete QuickStart.

Review

- Now is the time to make sure your system has been restarted since the installation of **SafeNet/400**.
- Make sure your startup program has been modified and that the Safeloging subsystem is up and running. There should be one or more active safeloging jobs in the subsystem and you should see transactions being recorded in the TRAPOD file in library PCSECDTA. Use PCREVIEW to view this file.
- Collect your data for 2-4 weeks.

Now continue with the detailed configuration of **SafeNet/400**, outlined in this guide and the SafeNet/400 Reference Guide.

Additional Initial Steps

Starting SafeNet/400

- Sign on as SAFENET or with a user profile that has a user class of *SECOFR.
- On the System i5 command line type

GO PCSECLIB/SN1, then press ENTER

- This brings you to the SafeNet/400 Main Menu.

```
SafeNet/400
File Edit View Communication Actions Window Help
-----
SN1
MPA400
SafeNet/400 Version 8
Network Resource Security
Main Menu

Select one of the following:
Level Required Fast Path
1. Work with Server Security Settings All WRKSRV
2. Work with User to Server Security 3 or 4 WRKUSRSRV
3. Work with User to Object Level Security 4 WRKUSROBJ
4. Work with User to SQL Statement Security 4 WRKUSRSQL
5. Work with User to FTP Statement Security 4 WRKUSRFTP
6. Work with User to CL Command Security 4 WRKUSRCMD
7. Work with User to Long Path Names 4 WRKUSRPTH
8. Work with TCP/IP Address Security 3 or 4 WRKTCPIPA
9. Work with TELNET Auto-Signon Security 3 or 4 WRKSIGNON
10. Go to Special Jobs/Setup Menu (SN2)
11. Go to Setup Reports Menu (SN3)
12. Go to Analysis Reports Menu (SN4) 80. Install Menu
13. Go to DHCP Menu (SN6) 90. Signoff

(C) Copyright 1997-2005 MP Associates of Westchester, Inc. All Rights Reserved.
Selection or command
===>

F3=Exit F4=Prompt F9=Retrieve F12=Cancel
F13=Information Assistant F16=System main menu

MP a
[Connected to remote server/host: 10.2.2.2 using port 23] [Implementation Guide.rtf - Microsoft Word] [HP LaserJet 4 Plus on IP_10.2.2.4]
```

From this menu you can access all of the **SafeNet/400** functions.

You can use the menu options or you can use the commands that are listed to the right of the options.

Note: To use the commands provided, remember to first add PCSECLIB to your library list.

SafeNet Administrator

You can set up a SafeNet/400 Administrator, or 'Super Admin' from the [SafeNet/400 Special Jobs Menu](#) or by using the WRKSNADM command. This can also be found on the [Special Jobs Menu](#), **Option 5 – Maintain SafeNet Administrators**.

The WRKSNADM command can be executed by a user with *SECADM or *SECOFR authority.

A user profile must be set up as a SafeNet/400 'Super Admin' to perform the following:

- Activate or deactivate SafeNet/400
- Change/copy/remove the IBM-supplied Q profiles settings in SafeNet/400
- Use the WRKSRV, CHGSPCSET, CHGFTPSET commands

A regular SafeNet/400 user or administrator does not have authority to the above functions.

Unless specifically changed, QSECOFR is ALWAYS a SafeNet/400 Super Admin. User profile SAFENET is a Super Admin; this status can be changed or removed to suit your purposes.

Chapter 4 - IMPLEMENTATION

Deciding how to use SafeNet/400

There are several methods to choose from when deciding how to implement **SafeNet/400** for your location. Below you will find three ways to use **SafeNet/400**.

For a complete description of **SafeNet/400** Security Level settings, see Chapter 2, 'Setting Up Servers' in the SafeNet/400 Reference Guide.

1. **SafeNet/400 as an Auditing Tool**

The logging feature of **SafeNet/400** traps each request that is made to the individual server functions on the System i5. This information can be useful in determining who is accessing which server function and what data, if any they are attempting to use. In addition, changes to both SafeNet/400 security settings and SafeNet/400 parameters are logged. Using **SafeNet/400** in this manner has no affect on any users accessing your system. For each request the log contains information on:

- User Profile
- Description of the server function being accessed
- Current server Security Level setting
- Date and time
- Data being accessed, if any
- SQL statements being utilized, if any
- If the request was accepted or rejected
- The reason the request was rejected
- Directory paths
- Program/command calls
- FTP Requests
- TELNET Requests
- CL command RUN requests

Multiple reports are available to you in **SafeNet/400**, enabling you to look at the log data in various ways. You can find the Analysis Reports Menu through the SafeNet/400 Main Menu, *Option 12* or use **GO SN4** command.

2. Limiting Server Functions

SafeNet/400's Security Level settings give you the ability to turn off specific server functions for all users, or for only certain users, if desired.

For example, if you don't want any of your clients to be able to send messages, you can use **SafeNet/400** Level 2 to completely disable the Message Server function. Or, if you want to make sure only particular users can send messages, use **SafeNet/400** Level 3 for the server function. Then, give those only individuals who will be permitted to send messages authority to the Message Server.

At Security Levels 3 and 4, **SafeNet/400** will check authority for each user who attempts to access the Server function and will accept only requests from authorized users. All others will be rejected.

The logging level indicates which network requests you wish to log:

- A = all requests
- N = no requests
- R = only rejections

3. Restricting access to objects based on user profile (Security Level 4)

Once you have set up **SafeNet/400** security levels and user access to your server functions, you can use **SafeNet/400** to control which objects each user has access to, what Data Rights they have to the objects, and whether they have Existence Rights to the objects.

In addition, you can specify SQL and/or FTP statements or CL commands that individual user profiles have authority to use.

4. Restricting access to servers based on IP address (Security Level 3)

For FTP and TELNET, and the FTP server, you can limit access by setting up a simple address table. You can accept or reject specific IP addresses or ranges of addresses.

Planning for SafeNet/400 Settings

As you are deciding how to set up **SafeNet/400**, keep in mind that there are many different ways to access the same objects on the System i5 through the various client applications. For example, the file transfer facility in System i5 Access for Windows uses the Data Base Access Server functions on the System i5, while Microsoft Explorer* uses the File Server function of OS/400 to access the same data.

This means that if you don't set up both of these server functions properly, you may be giving users authority to data without intending to do so.

You need to make sure you know which server functions your client applications are using, and set up your servers, and your users, accordingly. The easiest way to do this is to turn on logging as soon as you install **SafeNet/400**. See Chapter 3, 'SafeNet/400 Quickstart' in this guide for more information.

Next, run the analysis reports to identify the servers and objects that users are accessing. See the chapter on 'Reports' in the [SafeNet/400 Reference Guide](#).

For additional information on server functions and the clients that use them, see the IBM manual, [TCP/IP Configuration and Reference Guide](#) or specific licensed program manual.

Steps to set up SafeNet/400

These are the basic steps to set up **SafeNet/400**:

1. Determine the Future Server settings
2. Authorize users to servers that will be set to Security Level 3 or 4
3. Authorize users to objects for those users accessing the iSeries through servers that are set to Level 4
4. Authorize users to SQL and FTP statements, CL commands, TCP/IP tables and long path names if required. These are required if any of the above servers will be set to Level 4.
5. Change server Security Level and Logging Level settings

A more detailed explanation of the steps follows:

1. Install the product, perform **Quickstart**, IPL and turn on logging for 2-4 weeks.

Review reports to see which server functions are being used, which data is being accessed and by which users. Run the whole series of usage reports available from the Analysis Reports menu (SN4).
2. Decide how the server functions should be set up and secured for your location, and if you will use *PUBLIC or group profile entries in **SafeNet/400**.

Examine your logs for DDM command requests, Remote Program Call or FTP commands.

Note: See special notes on disabling the Remote Program Call and DDM Command Server in 'Server Function Descriptions' in the SafeNet/400 Reference Guide.

Decide how to control FTP access and Anonymous FTP (see 'Server Function Descriptions' and 'Setting up FTP' in the SafeNet/400 Reference Guide)

3. Decide which of your users will have access to the servers.
4. Decide what authority the users will have to objects on the system.

5. Decide which SQL and FTP statements and CL commands your users will need.
6. Decide if you wish to use TCP/IP address control for FTP or TELNET.
7. Decide if you need to set up long path names.
8. Decide if you wish to use the Alert Notification feature of **SafeNet/400**.
9. Decide if you wish to use Profile Swapping.
10. Authorize the users and/or *PUBLIC to the server functions.
11. Authorize users and/or *PUBLIC to objects, if necessary.
12. Authorize users and/or *PUBLIC to SQL, FTP statements, CL commands and TCP/IP tables, if necessary.
13. Enter exclusion rules, if any.
14. Use Future Settings to test your settings with the *On-Line Transaction Testing* or the *Batch Transaction Test Report* program prior to changing server Security Level settings.
15. Activate **SafeNet/400**
16. Change server Security Level settings to desired levels. This activates all of the authority checking routines.

Example of User Setup

For this example, assume you have a user who needs to transfer a file from a PC spreadsheet program to a System i5 database file. This example is based on the following scenario:

Every month this user transfers employee expense data from a Microsoft Excel* spreadsheet into a payroll file on the System i5. The PAYROLL file has already been created on the System i5 in library PERSONNEL and each month a member in the PAYROLL file is replaced with the new data.

File Transfer from a Windows Client

The user is running iSeries Access for Windows on their client and doing the same transfer as the example scenario.

Since the client is a PC with iSeries Access for Windows, there are multiple server functions that may be used: *Database Server - Entry*; *Database Server - Object Information*; and *Database Server - SQL*.

The following steps outline the procedure to give this user proper access. The **SafeNet/400** Security Level for the *Database Server - Entry* server function is set to Level 4.

At this level, the user must be authorized to the server function.

1. Authorize the user to the *Database Server - Entry* server function. (Main Menu Option 2 or **WRKUSRSRV** command)
2. If the other Database Servers (SQL, RTVOBJINF, etc.) are set to **Level 3 or 4** also, authorize the user to the required servers.
3. No specific Data Rights are required to access the library, file or member. At Level 3, only the user profile's authority to the server function itself is checked.
4. Set up Data Rights (Main Menu Option 3 or **WRKUSROBJ** command) so this user has Write and Delete data authorities to the PERSONNEL library and the PAYROLL file. See Scenario at the beginning of this section.

Even though member authority is not checked, since the member is to be replaced as part of the transfer process, this user will need DELETE data rights to the file to clear the member and WRITE data rights to add new records to it.

Note: If the PAYROLL file does not already exist in the PERSONNEL library, the user will also need Existence Rights so the file can be created during the transfer process.

Important: The other database servers, *Object Information* and *SQL*, are used by various file attribute and SQL statement processing. It is your responsibility to review the server request logs to determine which servers are required.

Automatic Enrollment

Use Automatic Enrollment to simplify the administration and set up of **SafeNet/400**. The auto-enrollment process uses the transactions that have been logged in the TRAPOD file to automatically set up your users with the proper access to server functions, commands, SQL statements, etc.

We advise that you use Automatic Enrollment only if you have an excessive number of users to enroll in **SafeNet/400**.

Important: Backups are recommended prior to performing these steps because auto-enrollment updates **are not** automatically reversible. Make sure you ALWAYS review the 'Preliminary Reports' before finalizing the Automatic Enrollment.

After performing **SafeNet/400 Quickstart** and logging requests for a minimum of two weeks, you should be ready to auto-enroll your users in **SafeNet/400**.

1. Run and review the usage reports on **SafeNet/400** Menu SN4.
2. Set the 'Future Settings' for each server to your desired level.
3. Decide if you want to use *PUBLIC authorities, group or supplemental authorities.
4. Set up the initial control files for generic access (for example, set up the *PUBLIC settings for servers, objects, SQL, FTP and long paths).
5. Set up the users/groups using *ALL objects, libraries, commands, FTP, etc.
6. Run the usage reports (Menu SN4) and select the parameter to run the auto-enrollment reports, but do not actually perform the auto-enrollment updates.

Note: When printing the *User to Server Usage* report, you can perform auto-enrollment checks against the *Current* or *Future* server settings. Change the *Enrollment Basis - Curr/Future* parameter to either *C* or *F*, then run the report. When running the report here for the auto-enrollment process, use 'F' for Future settings.

If the Current or Future server setting is a level that does not require enrollment, the transactions will not be enrolled.

7. Review the auto-enrollment reports and perform any additional manual entries into the control files for specific users.
8. Re-run and review the auto-enrollment reports until you are satisfied with the results
9. Back up the PCSECDTA library.
10. Re-run the usage reports, this time changing the *Perform Enrollment Updates* parameter to *YES to perform the auto enrollment updates and print the reports.
11. Run the *User to Security Settings* report and review all the entries
12. Run the *Batch Security Report by User* (Menu SN4), select to test future settings, printing only rejections. If all the control file settings are correct you should receive no output.

If you receive rejections on the report, review the security control files, make the appropriate corrections and run the security report again. Continue this process until the report generates no output or until all rejections on the report are valid.

Post Automatic Enrollment

Turning on your Future Settings

If you have successfully set up all the security files, enrolled users or run the auto-enrollment, reviewed the batch transaction test report and set your future server settings and logging levels, you are now ready to turn on the new future settings.

1. Use the **CHGNOTIFY** command to turn on Alert Notification so you will receive immediate messages about rejections
2. **GO SN1**, *Option 1* (WRKSRV) then use **F22** to toggle between current and future settings. This will activate the server setting you wish to use.

At any time you may use F22 to switch between current and future settings.

Chapter 5 - SPECIAL SAFENET/400 TECHNICAL CONSIDERATIONS

Insuring network requests are logged

After **SafeNet/400** is installed, a new subsystem, called SAFELOGING, will be active on your System i5. The subsystem may contain up to two different pre-start jobs. One job, ALERTWATCH, will be active if you are using Alert Notification in Summarized Mode. The other job, SAFELOGING, must be active for network requests to be logged to the history file.

To make sure this job is active at all times, change your system start up job or procedure to include the following lines:

```
PCSECLIB/STRTRP /* Starts logging */  
MONMSG CPF0000
```

This command will start the SAFELOGING subsystem and the SAFELOGING pre-start job.

Important: You must activate this feature for transaction logging to occur.

To insure proper shutdown of these programs, your system power down procedure should include the following commands:

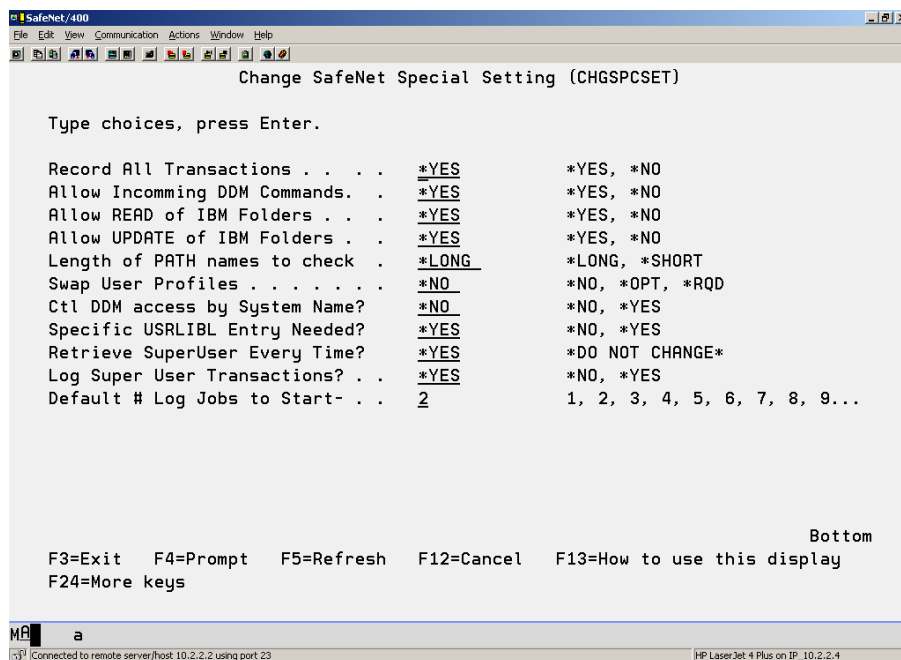
```
PCSECLIB/ENDTRP  
MONMSG CPF0000  
DLYJOB 10 /*For orderly shutdown*/  
ENDSBS SAFELOGING *IMMED
```

Changing Special SafeNet/400 Settings

Use the CHGSPCSET command to change **SafeNet/400** settings.

A detailed explanation of each parameter is on the following pages.

From the Special Jobs Menu select **Option 2 - Change Request Logging Level and Special Settings** or use the **CHGSPCSET** command.



```
SafeNet/400
File Edit View Communication Actions Window Help
Change SafeNet Special Setting (CHGSPCSET)

Type choices, press Enter.

Record All Transactions . . . . *YES          *YES, *NO
Allow Incoming DDM Commands. . *YES          *YES, *NO
Allow READ of IBM Folders . . . *YES          *YES, *NO
Allow UPDATE of IBM Folders . . *YES          *YES, *NO
Length of PATH names to check . *LONG         *LONG, *SHORT
Swap User Profiles . . . . . *NO           *NO, *OPT, *RQD
Ctl DDM access by System Name? *NO           *NO, *YES
Specific USRLIBL Entry Needed? *YES          *NO, *YES
Retrieve SuperUser Every Time? *YES          *DO NOT CHANGE*
Log Super User Transactions? . . *YES          *NO, *YES
Default # Log Jobs to Start- . . 2             1, 2, 3, 4, 5, 6, 7, 8, 9...

Bottom
F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys

MR a
Connected to remote server/host: 10.2.2.2 using port 23
HP LaserJet 4 Plus on IP_10.2.2.4
```

CHGSPCSET Command

The default value is highlighted in **bold**.

Parameter	Screen Selections	Value	Description
LOGALL	Record All Transactions	* YES *NO	This setting can be changed so that requests are not logged. It recommended that this setting be left at the default *YES.
ALWDDM	Allow Incoming DDM Commands	* YES *NO	This option controls whether or not incoming commands are processed. If the server function Security Level setting within SafeNet/400 is set to Level 3 or higher, setting this option to *NO shuts off <u>ALL</u> incoming command processing by the <i>Distributed Data Management</i> and the <i>Remote Command Program Call</i> server functions. If this option is left at the default of *YES, and the DDM or Remote Command Program Call server function is set to Level 3 or 4, the user submitting the incoming command must be authorized to the server. If set to Level 4, the user must be authorized to the command being issued.
READIBM	Allow READ of IBM Folders	* YES *NO	This option controls automatic authorities to IBM-supplied folders. SafeNet/400 is initially installed with Read as *YES. Whenever the SafeNet/400 Security Level for the <i>File Server</i> function is set to Level 4, this parameter is in effect.
UPDTIBM	Allow UPDATE of IBM Folders	* YES *NO	This option controls automatic Write/Update authority to IBM supplied folders. Initially SafeNet/400 sets this to *YES. Whenever the SafeNet/400 Security Level for the <i>File Server</i> function is set to Level 4, this parameter is in effect.
PATHL	Length of PATH names to check	* LONG *SHORT	Indicates if you are using standard 10-character paths or long path names
SWAPU	Swap User Profiles	*NO * OPT *RQD	Specifies whether to allow or require a swapping profile to be used within SafeNet/400 .
DDM	Use system name for DDM requests	*YES * NO	Specifies whether when the system gets a DDM request, whether the system name is

			used for security checking or the incoming user profile. When set to *YES the system name replaces the user seen at the target DDM system during a DDM connection. (Typically QUSER) It is not necessary to have a user profile on the target DDM server that matches the requester from the source. You do need to have entries in SafeNet/400 for the system name to DDM server, and the objects, commands, etc. that the 'sourcesystemname' will access. SafeNet/400 allows you to add profiles to the setup even if no OS/400 profile exists; in this case, use the source system name.
USRLIBL	Specific USRLIBL Entry Needed	*YES *NO	Determines whether specific *USRLIBL entries are required in WRKUSROBJ
SUSRCHK	Retrieve SuperUser Every Time	*YES *NO	Indicates whether or not to look up the SUSER data every cycle. DO NOT CHANGE THIS VALUE UNLESS INSTRUCTED TO DO SO BY SAFENET SUPPORT.
LOGSUSR	Log Super User Transactions	*YES *NO	Indicates whether or not to log super user requests
DFTJOBS	Default Number of Logging Jobs to Start	# of jobs 1 (one)	Number of logging jobs to autostart with the STRTRP command

Most System i5 installations utilizing PC Support/400 or iSeries Access for Windows require access to the shared folders on the System i5. Leaving the setting *READIBM* *YES allows network clients Read Only access to all IBM-supplied folders for the purpose of PC Support operations, update function, I: drive activity, etc.

Important: If *File Server* function is set to Level 4 and this option is set to *READIBM* *NO you will have to add the folder authority required for each user who needs access to the folders for PC Support/400 or iSeries Access for Windows.

Example: PC Support/400 with Extended DOS user who runs from their I: drive or uses the update function will require an entry in user-to-object security as follows:

Network Path Request = /QDLS/QIWSFL2/.....

<u>Library</u>	<u>Object</u>	<u>Read</u>	<u>Write</u>	<u>Delete</u>
QDLS	QIWSFL2	X		
QIWSFL2	*ALL	X		

Setting *Write/Update (UPDTIBM)* set to **NO* prevents users from changing or adding to the contents of any IBM-supplied folder. This parameter is only effect when the *File Server* function security setting is to Level 4.

Exit Point Exclusion Option

This version of **SafeNet/400** includes the ability for you to flag a specific exit point so that it is always excluded from **SafeNet/400** processing. Use of this option will open up a security exposure on your system, so we do not recommend that you use this without consulting first with Kisco support staff. Some customers, however, may find that their system requires that a specific exit program from **SafeNet/400** be excluded on their system.

To set an exit point to be excluded from **SafeNet/400**, you need to follow these exact steps:

1. At the command line, run the following commands:

```
ADDLIB PCSECLIB  
ADDLIB PCSECDTA
```

2. Update the exit point exclusion code by running a new file maintenance program. You can run this program by entering the following call at the command line:

```
CALL ACTEPXCL
```

3. Find the exit point on the list that is displayed and place a 2 next to it. On the detail screen that follows, code the exclusion code with the letter X and press ENTER.
4. Next, go to your system console and bring your system to restricted state by ending all subsystems.
5. When the system reaches restricted state, deactivate **SafeNet/400** by running option #6 from the SN2 menu.
6. When **SafeNet/400** is deactivated, you can then immediately reactivate it using the same option #6 from the SN2 menu.
7. Resume normal processing by starting your controlling subsystem.

At this point, the selected exit point will no longer be linked to the **SafeNet/400** product.

If, at some point in the future, you decide that you want to have **SafeNet/400** process transactions at the exit point that has been excluded, you can do so by following the exact same procedure as outlined above with the exception that at step #3, instead of entering the letter X, you should change the existing letter X to a blank.

When you finish step 7 above, **SafeNet/400** will now be connected to the exit point in question. Go to the SN1 menu and run option #1 to check the level setting for the exit point. You will find that it has been reset to 1 and may need to be reset to the level you prefer.

INDEX

A

Administrator3.3, 3.10
Alert Notification.....4.5, 4.10, 5.1
Anonymous Logon.....4.4
Audit1.3, 4.1
Automatic Enrollment.....4.8, 4.10

C

CHGSPCSET5.2, 5.3. See also Settings, Special

E

ENDTRP.....5.1
Exclusions.....1.3, 2.4, 2.5
Exit points.....1.1
 Excluding from SafeNet.....5.6

H

History file.....5.1

L

Limit Transaction Logging.....3.5
Long path name.....4.4, 4.5
Look up routines.....2.5

O

Object Authorities.....2.3

P

PTF.....1.6

Q

Quickstart3.1

S

SAFELOGING Subsystem3.8
Server Function ...1.2, 1.3, 1.4, 1.6, 2.1, 3.1, 3.4,
 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.8, 5.3
Set Up4.4
Settings
 Future4.9, 4.10
 Special3.6, 5.2
System Requirements1.6

T

Transaction Logging3.8
TRAPOD.....4.8

U

User Profiles
 **PUBLIC*2.4, 2.5, 2.6, 4.4, 4.5, 4.8
 Group.....2.4, 2.5, 2.6
 Supplemental2.4, 2.5, 2.6
 Swapping5.3