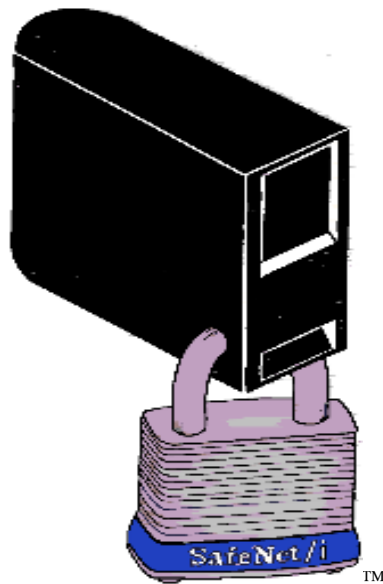


SAFENET/i

FOR IBM i

IMPLEMENTATION GUIDE

Version 10



How to contact us



Información del Distribuidor

Via Laietana 20
08003 Barcelona, Spain
93 319 16 12
www.att.es
email: att@att.es

Direct all inquiries to:

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

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

Kisco Website:

www.kisco.com/safenet
www.kisco.com/safenet/support

SafeNet/i Website:

www.safeneti.com

SafeNet/i Support Website:

www.safeneti.com/safenet/support

TABLE OF CONTENTS

- Chapter 1 OVERVIEW1.1**
 - SafeNet/i Features..... 1.3*
 - System Requirements..... 1.6*
- Chapter 2 PLANNING FOR SECURITY1.1**
- Chapter 3 SAFENET QUICKSTART3.1**
 - Navigating within SafeNet/i 3.8*
 - SafeNet Administrator..... 3.9*
- CHAPTER 4 IMPLEMENTATION.....4.1**
 - Deciding how to use SafeNet/i 4.1*
 - Planning for SafeNet/i Settings 4.3*
 - Steps to set up SafeNet/i..... 4.4*
 - Example of User Setup..... 4.6*
 - Automatic Enrollment 4.8*
 - Post Automatic Enrollment 4.10*
- CHAPTER 5 SPECIAL SAFENET TECHNICAL CONSIDERATIONS5.1**
 - Insuring network requests are logged..... 5.1*
 - Changing Special SafeNet/i Settings..... 5.2*
 - Exit Point Exclusion Option..... 5.7*

Special Notices

The following terms are trademarks of the International Business Machines Corporation:

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

The following terms are trademarks of Microsoft Corporation:

Windows XP	Microsoft Excel
Microsoft Explorer	Microsoft Access
ODBC	Microsoft Query
Windows Vista	Windows 2000
Windows 7	

SafeNet/i Implementation Guide

Chapter 1 - OVERVIEW

What is SafeNet/i?

SafeNet/i is a powerful yet easy to use tool for the IBM i that enables you to exercise full control over users who access your system via network connections. These network connections can be through any device that has access to your IBM i, whether through a LAN, WAN, the Internet, etc.

SafeNet/i provides the means to secure functions and objects on your IBM i, 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/i is non-invasive to your existing IBM i security. **SafeNet/i** does not change any of your existing security settings or object level authorities other than exit point program registrations.

SafeNet/i 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 IBM i Security sufficient?

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

However, when these same users are entering your IBM i 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 IBM i, 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 IBM i, they can copy it, add to it, or even delete it. **SafeNet/i** can help you control this.

Who should use SafeNet/i?

SafeNet/i is designed for any installation where intelligent network devices communicate with the IBM i. These devices have access to the data on the IBM i whether they connect to the system through a LAN, WAN or the Internet, whether they are local or remote, or whether there is a single IBM i or multiple systems in the network.

How does SafeNet/i work?

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

You establish the rules for your IBM i and use **SafeNet/i** 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/i** 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/i Reference Guide](#) for detailed information on the transaction logging features of **SafeNet/i**.

SafeNet/i Features

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

Generate Audit Reports

SafeNet/i tracks each request coming from a client into the IBM i. It stores this information in a log that you can review. The log indicates who is accessing your system, which server function on the IBM i 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/i can be set up to limit access to specific server functions on the IBM i based on the individual's user profile.

Exclude Users from Server Functions

SafeNet/i allows you to turn off individual server functions. For example, you can completely exclude the file transfer function for all users on your IBM i 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/i gives you the ability to implement object level security over clients that are accessing the various server functions on the IBM i. 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/i allows you to define specific IP addresses or ranges of IP addresses to control access to *FTP server*, *FTP client* or *TELNET*.

Limit Access to Spooled Files

SafeNet/i can be configured to control access to spooled files in individual output queues.

What is a Server Function?

With IBM i 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 IBM i 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 IBM i (the server).

The IBM i has several specialized **server functions** that are included as part of IBM i, and each request from a client uses one of these server functions on the IBM i.

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

Server support provided with IBM i 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 IBM i:

- Transfer function server for transferring files between personal computers and IBM i
- 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 IBM i through DDM

Optimized Support

Optimized clients:

- Windows95 (32 bit applications)
- Windows NT
- Windows 2000
- Windows XP
- Windows Vista
- Windows 7
- 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 IBM i 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
- Sign-on 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 IBM i servers are included in the Host Server option of the operating system. These servers are used by IBM i Access for Windows but are designed so that other client products can use them also.

System Requirements

SafeNet/i V10 requires IBM i Version 5 Release 4 and above.

PTFs

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

System Library List Entries

Library QSYS2 is required by **SafeNet/i** to gain access to necessary IBM i operating system 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 IBM i, there are features available to you within the operating system 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 IBM i.

However, when these same users are accessing your IBM i, 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 IBM i, that PC spreadsheet program can upload data, download data, add or delete data on your IBM i.

This is where **SafeNet/i** can assist you. **SafeNet/i** 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/i** Security Level settings, you can restrict server functions and establish specific authority to objects.

SafeNet/i and IBM i Security

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

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

SafeNet/i Object Authorities

SafeNet/i uses Data Rights and Existence Rights similar to those used by IBM i 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 - update records

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/i**. The unlimited user license allows you to define *PUBLIC and group profiles within **SafeNet/i**. This significantly reduces the complexity of **SafeNet/i** administration.

SafeNet/i 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 IBM i user profile
2. **SafeNet/i** will mix or combine individual authorities with group authorities.

If **SafeNet/i** finds that an individual is authorized to a particular server, but not the object, **SafeNet/i** will then check to see if a group profile is authorized to the object. **SafeNet/i** 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/i** 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 authority entries, comparable to IBM i, that simplify administration.

Security look up routines

SafeNet/i 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/i** will no longer continue examining name combinations.

To incorporate *PUBLIC authorities and exclusions, **SafeNet/i** 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

Important: When you install your copy of SafeNet/i the license type is set to a default Unlimited User level. If you do not plan on purchasing an unlimited user license, you may want to avoid using Group and/or Supplemental profiles and *PUBLIC during your evaluation, since this support is available only with an unlimited user license.

The base license of SafeNet/i provides support for up to 25 network users on your system. At the unlimited level, there are additional features and controls that you can use to protect your system and simplify maintenance of your rules.

Chapter 3 - SafeNet/i QuickStart

Quickstart will enable you to begin using **SafeNet/i** immediately to track client/server activity on your IBM i, 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/i** 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/i Reference Guide](#) for detailed information on how to review the information that is being logged.

Trial Versions of SafeNet/i

If you are performing this Quickstart with an evaluation copy of SafeNet/i, be aware that your trial license expires thirty (30) days after installation. To check the status of your trial, use **Option 2 – Display Installation Status** on the INSTALL menu; if you need more time to complete your evaluation, please contact support.

Quickstart is made up of the following steps:

1. Install SafeNet/i, modify your startup program to start the SafeNet/i logging job upon IPL
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/i (for unlimited user licenses)
8. Set up group authorities other than *PUBLIC in SafeNet/i (for unlimited user licenses)
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 (SN2), **Option 4 - On-line Transaction Testing**.
12. Make changes to SafeNet/i settings as required based on results of PCTESTR
13. TEST, TEST, TEST
14. Flip the 'Future' and 'Current' settings (Use 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/i** management options, see 'SafeNet Administrator' in Chapter 3 of this guide.

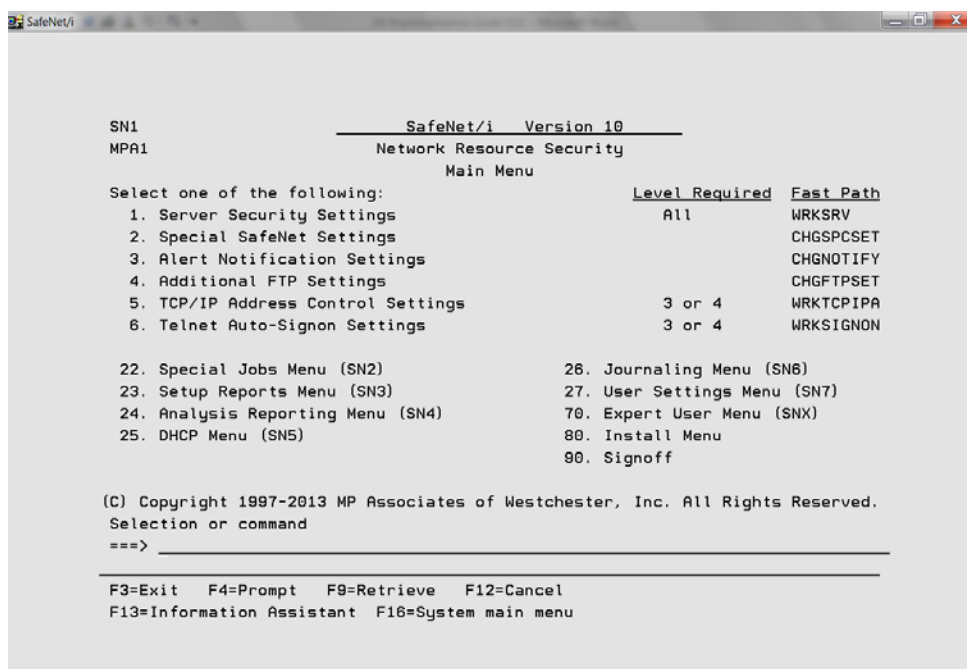
If the SafeNet/i Main Menu is not displayed, type

GO PCSECLIB/SN1

Follow these steps to begin logging requests:

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

From the SafeNet/i Main Menu (SN1) select **Option 1 - Server Security Settings** or use **WRKSRV** command



```
SafeNet/i
-----
SN1
MPA1
SafeNet/i Version 10
Network Resource Security
Main Menu

Select one of the following:
1. Server Security Settings           Level Required: All      Fast Path: WRKSRV
2. Special SafeNet Settings          Level Required: All      Fast Path: CHGSPCSET
3. Alert Notification Settings        Level Required: All      Fast Path: CHGNOTIFY
4. Additional FTP Settings            Level Required: All      Fast Path: CHGFTPSET
5. TCP/IP Address Control Settings    Level Required: 3 or 4   Fast Path: WRKTCPIPA
6. Telnet Auto-Signon Settings        Level Required: 3 or 4   Fast Path: WRKSIGNON

22. Special Jobs Menu (SN2)
23. Setup Reports Menu (SN3)
24. Analysis Reporting Menu (SN4)
25. DHCP Menu (SN5)
26. Journaling Menu (SN6)
27. User Settings Menu (SN7)
70. Expert User Menu (SNX)
80. Install Menu
90. Signoff

(C) Copyright 1997-2013 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
```

The *Maintain Server Security* screen is displayed.

```

SafeNet/i
-----
WRKREG2R                               4/06/13
MPA1                                     13:25:04
          SafeNet/i  V10
Maintain Server Security

Security Levels:
1=Unlimited Access  2=No Access  3=Limited by User  4=Limited by User & Object
5=Not Supported/User Program Detected

Logging Levels:          TOD=Time of Day Checking:
A=Log All  N=No Logging  R=Log Rejected          Y=Yes  N=No

|--Current--| Future  Max.      Server
Sec.  Log  TOD  Sec.  Lvl.  Description
3     A    N    4     4   Distributed Data Management      *DDM
3     A    Y    3     3   DRDA DB2 Database Access Rqst    *DRDA
4     A    N    1     4   Original Data Queue Server       *DQSRV  100
1     A    N    1     3   Original License Mgmt Server     *LMSRV  100
1     A    N    1     3   Original Message Server         *MSGFCL 100
1     R    N    1     3   Network Print Server - entry     QNPSERV 100
1     A    N    1     4   Network Print Server - spool file QNPSERV 100
3     A    N    4     4   File Server                     *FILESRV 100
4     A    N    4     4   Original Remote SQL Server       *RQSRV  100
1     A    N    1     4   Spooled File Security            *SPLAUT 100
                                     More...

F3=Exit  HELP      F18=User Exit Programs  F22=Flip Future & Current Settings
Pageup/Pagedown      (c) Copyright 1997 MP Assoc., Inc.

```

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.)

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.

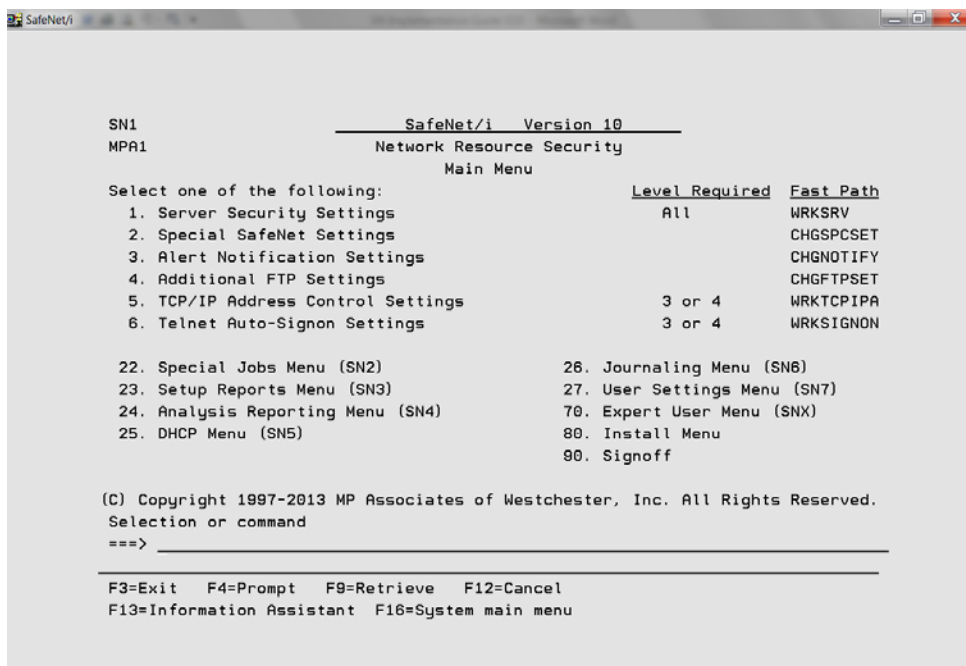
Note: The server functions are listed on multiple screens. **PageDown** to ensure you enter a security and logging level for all the servers.

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

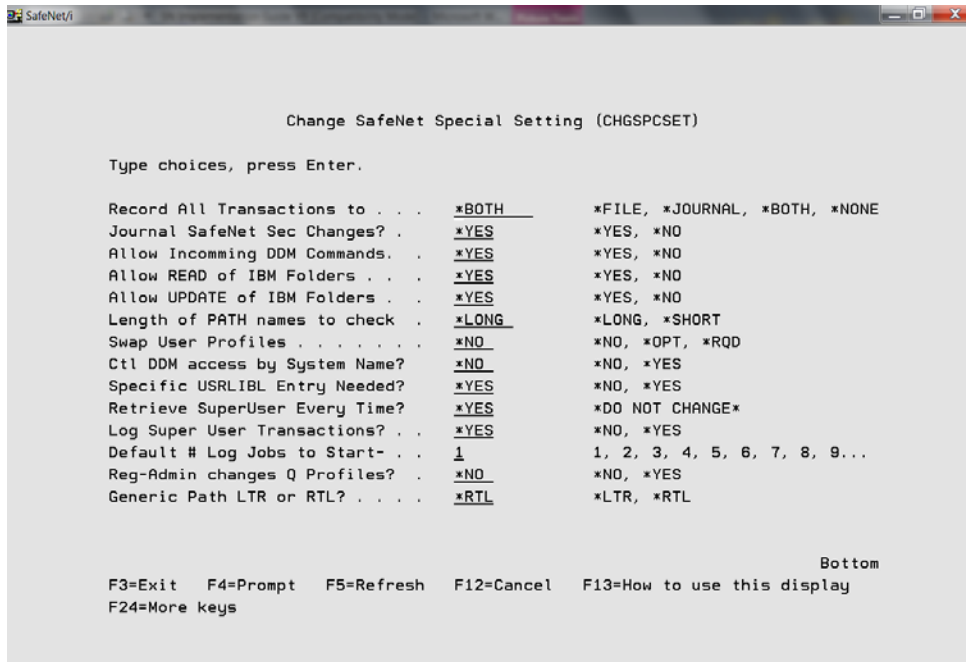
Due to a potentially high transaction rate and logging overhead, you will probably want to limit logging on several of the servers after you have become familiar with their transactions. Some of the servers where you can safely limit transaction logging are:

License Management Servers Network Print
Data Queue Servers Message Servers

3. Press **F3** to return to the SafeNet/i Main Menu.
4. Select **Option 2 - Special SafeNet Settings** or use CHGSPCSET command



The *Change SafeNet Special Setting* screen appears.



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

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

6. **F3** to return to the SafeNet/i Main Menu.
7. 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: Some functions of SafeNet/i will begin working right away. But, because IBM i allocates exit programs at startup (IPL) only, once you have installed **SafeNet/i** 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/i's** processes.

Transaction Logging Subsystem (SAFELOGING)

In Step 7 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/i** data queue can become full and cause network response issues.

SafeNet/i 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 Chapter 5 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/i**.
- 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 the Special Jobs Menu (SN2), **Option 3 - On-line Transaction Review** or the **PCREVIEW** command to view the TRAPOD log file.

- Collect your data for 2-4 weeks.

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

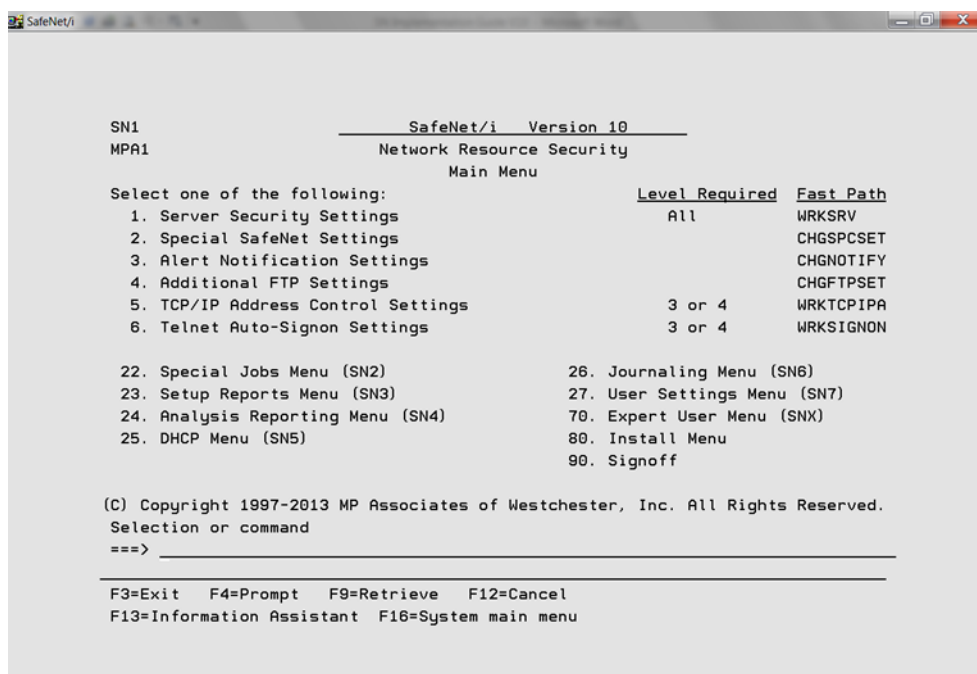
Navigating within SafeNet/i

Starting SafeNet/i

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

GO PCSECLIB/SN1, then press ENTER

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



```
SafeNet/i
-----
SN1
MPA1
SafeNet/i Version 10
Network Resource Security
Main Menu

Select one of the following:
1. Server Security Settings
2. Special SafeNet Settings
3. Alert Notification Settings
4. Additional FTP Settings
5. TCP/IP Address Control Settings
6. Telnet Auto-Signon Settings

22. Special Jobs Menu (SN2)
23. Setup Reports Menu (SN3)
24. Analysis Reporting Menu (SN4)
25. DHCP Menu (SN5)

26. Journaling Menu (SN6)
27. User Settings Menu (SN7)
70. Expert User Menu (SNX)
80. Install Menu
90. Signoff

Level Required Fast Path
All WRKSRV
CHGSPCSET
CHGNOTIFY
CHGFTPSET
3 or 4 WRKTCPIPA
3 or 4 WRKSIGNON

(C) Copyright 1997-2013 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
```

From this menu you can access all of the **SafeNet/i** functions and sub-menus.

Sub-menus are accessed using Options 22 through 27, and Options 70 and 80. These options are available from every menu, even if the options are not listed on the menu.

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 SafeNet/i User Settings (SN7) by selecting **Option 8 – Work with SafeNet Administrators.**

SafeNet/i the IBM-supplied settings in SafeNet/i user or administrator
ALWAYS SafeNet/i. Uby default to suit your purposes

Chapter 4 - IMPLEMENTATION

Deciding how to use SafeNet/i

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

For a complete description of **SafeNet/i** Security Level settings, see Chapter 2, 'Setting Up Servers' in the [SafeNet/i Reference Guide](#).

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

The logging feature of **SafeNet/i** traps each request that is made to the individual server functions on the IBM i. 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/i** security settings and **SafeNet/i** parameters are logged. Using **SafeNet/i** 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 (Client and Server requests)
- TELNET Requests
- CL command RUN requests

Multiple reports are available to you in **SafeNet/i**, enabling you to look at the log data in various ways. You can find the [Analysis Reports Menu](#) through the [SafeNet/i Main Menu \(SN1\)](#), *Option 24* or use the **SN4** command.

2. Limiting Server Functions

SafeNet/i'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/i** Level 2 to completely disable the Message Server function. Or, if you want to make sure only particular users can send messages, use **SafeNet/i** Level 3 for the server function. Then, give only those individuals who will be permitted to send messages authority to the Message Server.

At Security Levels 3 and 4, **SafeNet/i** 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/i** security levels and user access to your server functions, you can use **SafeNet/i** 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 TELNET, FTP Client and 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/i Settings

As you are deciding how to set up **SafeNet/i**, keep in mind that there are many different ways to access the same objects on the IBM i through the various client applications. For example, the file transfer facility in IBM i Access for Windows uses the Data Base Access Server functions on the IBM i, while Microsoft Explorer* uses the File Server function of IBM i 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/i**. See Chapter 3, 'SafeNet/i 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/i 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/i

These are the basic steps to set up SafeNet/i:

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 IBM i 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/i**.

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/i Reference Guide](#).

Decide how to control FTP access and Anonymous FTP (see 'Server Function Descriptions' and 'Setting up FTP' in the [SafeNet/i 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/i**.
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. Change server Security Level settings to desired levels; flip Future and Current security settings. This activates all of the authority checking routines.
16. Monitor your system

Example of User Setup

For this example, assume you have a user who needs to transfer a file from a PC spreadsheet program to an IBM i 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 IBM i. The PAYROLL file has already been created on the IBM i 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 IBM i Access for Windows on their client and doing the same transfer as the example scenario.

Since the client is a PC with IBM i 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. This assumes that all *Database Servers* are set to their highest available SafeNet security settings, either Level 3 or Level 4.

At this level, the user must be authorized to the server functions and objects.

1. Authorize the user to the *Database Server - Entry* server function. (User Settings Menu (SN7) Option 1 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. Set up Data Rights (User Settings Menu (SN7) Option 2 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/i**. 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/i**.

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

1. Run and review the usage reports on SafeNet/i 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 on SafeNet/i 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 *Print Security Report by User* on Menu SN4 - **Option 1**, 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. From Menu SN1, select **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/i TECHNICAL CONSIDERATIONS

Insuring network requests are logged

After **SafeNet/i** is installed, a new subsystem, called SAFELOGING, will be active on your IBM i. 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:

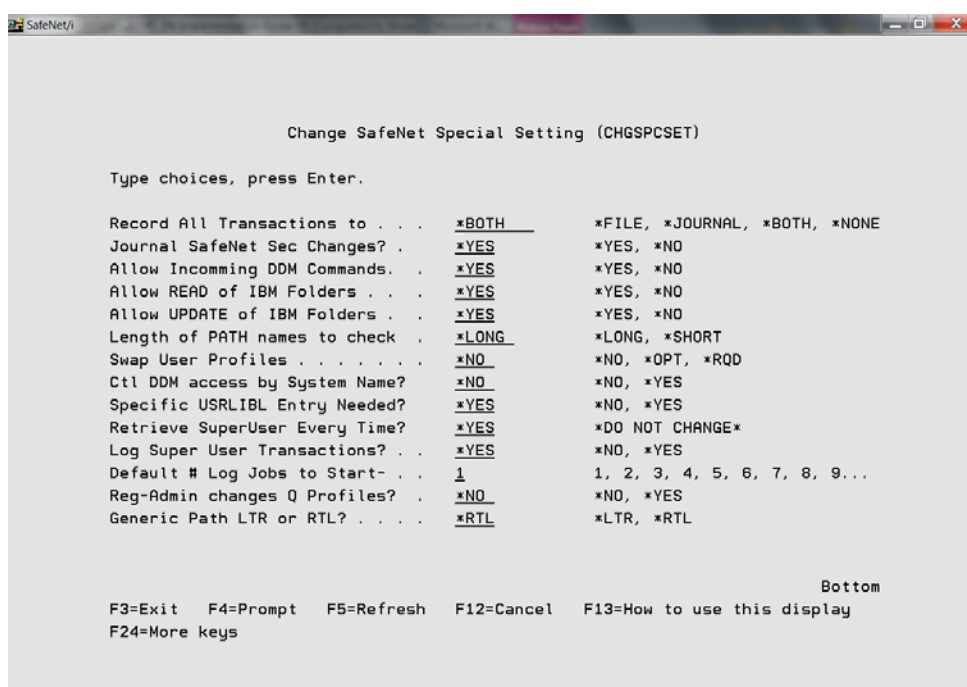
```
PCSECLIB/ENDTRP  
MONMSG CPF0000
```

Changing Special SafeNet/i Settings

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

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

From the SafeNet/i Main Menu select **Option 2 – Special SafeNet Settings** or use the **CHGSPCSET** command.



CHGSPCSET Command

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

Parameter	Screen Selections	Value	Description
LOGALL	Record All Transactions	* FILE *JOURNAL *BOTH *NONE	Specifies whether or not all network requests are logged: <ul style="list-style-type: none"> *FILE logs all network requests into PCSECLIB/TRAPOD physical file *JOURNAL logs all network requests into the PCSECJRN/TRAPJRN Journal *BOTH logs all network requests into both the PCSECJRN/TRAPJRN Journal and the PCSECDTA/TRAPOD Physical File Specify *NONE not to log the requests at all
JRNSEC	Journal SafeNet Sec Changes?	*YES * NO	Specifies whether changes made to the SafeNet security control files should be written to the PCSECJRN/SAFENET journal
ALWDDM	Allow Incoming DDM Commands	* YES *NO	Specifies whether commands received over the *DDM or *RMTSRV servers should be processed or rejected. <p>This option controls whether or not incoming commands are processed. If the server function Security Level setting within SafeNet/i 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.</p> <p>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.</p>
READIBM	Allow READ of IBM Folders	* YES *NO	Specifies whether to allow automatic read authority to IBM folders over the file server Exit point. The default IBM folder

			<p>list is contained in file IBMFLR. You may add additional entries as required to this file. Add entries using UPDDTA.</p> <ul style="list-style-type: none"> • *YES allows READ of IBM Folders • *NO rejects all READ attempts to IBM folders. (Can be overridden at the user to object level) <p>This option controls automatic authorities to IBM-supplied folders. SafeNet/i is initially installed with Read as *YES. Whenever the SafeNet/i Security Level for the <i>File Server</i> function is set to Level 4, this parameter is in effect.</p>
UPDTIBM	Allow UPDATE of IBM Folders	*YES *NO	<p>This option controls automatic Write/Update authority to IBM supplied folders. Whenever the SafeNet/i Security Level for the <i>File Server</i> function is set to Level 4, this parameter is in effect.</p> <p>Initially SafeNet/i sets this to *YES.</p> <p>*NO rejects all UPDATE attempts to IBM folders. (Can be overridden at the user to object level)</p>
PATHL	Length of PATH names to check	*LONG *SHORT	<p>Specifies whether to check the Long mixed case or standard 10 position upper case PATH Lengths in the FTP and FILESRV servers.</p> <p>Long Path is the default beginning in of SafeNet/i.</p>
SWAPU	Swap User Profiles	*NO *OPT *RQD	<p>Specifies whether to allow or require a swapping profile to be used within SafeNet/i.</p>
			SafeNet/ie- SafeNet/iIBM i
USRLIBL	Specific USRLIBL Entry Needed	*YES *NO	<p>Specifies whether a specific *USRLIBL entry is required in the SafeNet control file (WRKUSROBJ) when transactions are received with unqualified object names.</p> <p>Action to take when no library is specified in a request:</p> <ul style="list-style-type: none"> • *YES REQUIRES that a *USRLIBL

			<p>entry exist in WRKUSROBJ</p> <ul style="list-style-type: none"> *NO ACCEPTS all unqualified object requests WITHOUT checking for a corresponding *USRLIBL entry in WRKUSROBJ. *NO is a potential SECURITY RISK
SUSRCHK	Retrieve SuperUser Every Time	*YES *NO	<p>Specifies whether to retrieve the list of Super-Users every time a transaction is processed or only at program initialization time.</p> <ul style="list-style-type: none"> *YES retrieves the list of Super-Users every transaction *NO loads the Super-User list at program initialization time ONLY <p>If this is set to *NO, and you modify the Super-User list, that change may not take effect until after the next system IPL. This is a performance setting.</p> <p>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.</p>
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)	<p>Specifies the number of SAFELOGGING transaction log jobs that are started by default.</p> <p>For high network traffic systems, you may want to increase this number to a maximum of 9 jobs. For normal or low traffic systems, you can probably leave this as 1. Under normal circumstances, SafeNet/i will automatically activate additional logging jobs as required if the data queue fills to maximum size.</p> <p>Number of logging jobs to autostart with the STRTRP command</p>
QPROFS	Reg-Admin changes	*NO	Specifies whether to allow a regular

	Q Profiles?	*YES	<p>SafeNet admin to change IBM supplied Q profile authorities and work with *ALLIB/ *ALLFLR security entries:</p> <ul style="list-style-type: none"> • *YES allows regular administrators to change Q profile authorities and work with *ALLIB/ *ALLFLR security entries • *NO allows only Super-Admins to change Q profile and *ALLIB/ *ALLFLR authorities
GENPTH	Generic Path LTR or RTL?	*LTR *RTL	<p>Specifies whether to build generic path look-ups from left-to-right or right-to-left. This parameter affects the *FILESRV and *FTPSERVER generic path lookup processes.</p> <p>This parameter only affects systems set to *LONG path support.</p>

Most IBM i installations utilizing PC Support/400 or IBM i Access for Windows require access to the shared folders on the IBM i. Leaving the setting *READIBM* *YES allows network clients Read Only access to all IBM-supplied folders for the purpose of IBM i Access operations.

Exit Point Exclusion Option

This version of **SafeNet/i** includes the ability for you to flag a specific exit point so that it is always excluded from **SafeNet/i** 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/i** be excluded on their system.

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

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

```
ADDLIBLE PCSECLIB  
ADDLIBLE 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/i** by running option 50 from the Install menu.
6. When **SafeNet/i** is deactivated, you can then immediately reactivate it using the same option 50 from the Install 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/i** product.

If, at some point in the future, you decide that you want to have **SafeNet/i** 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/i** 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

Administrator..... 3.3, 3.9
Alert Notification 4.5, 4.10, 5.1
Anonymous Logon 4.4
Audit 1.3, 4.1
Automatic Enrollment..... 4.8, 4.10

C

CHGSPCSET..... 5.2, 5.3, *See also Settings, Special*

E

ENDTRP..... 5.1
Exclusions..... 1.3, 2.4, 2.5
Exit points..... 1.1
 Excluding from SafeNet..... 5.7

H

History file..... 5.1

L

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

O

Object Authorities..... 2.3

P

PTF 1.6

Q

Quickstart..... 3.1

S

SAFELOGGING Subsystem 3.7
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 Up..... 4.4
Settings
 Future 4.10
 Special 3.5

T

Transaction Logging 3.7
TRAPOD 4.8

U

User Profiles
 *PUBLIC 2.4, 2.5, 2.6, 4.4, 4.5
 Group..... 2.4, 2.5, 2.6
 Supplemental..... 2.4, 2.5, 2.6
 Swapping 5.4



Información del Distribuidor

Via Laietana 20
08003 Barcelona, Spain
93 319 16 12
www.att.es
email: att@att.es