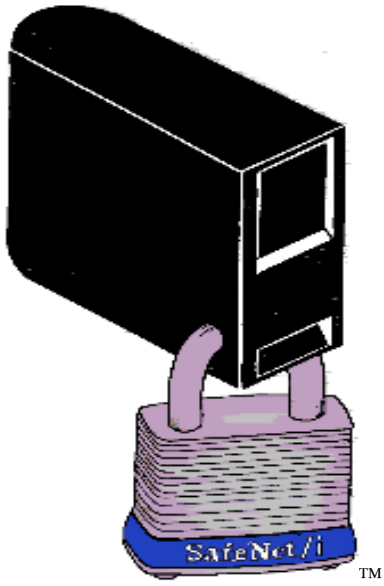
SafeNet/i

FOR IBM i

IMPLEMENTATION GUIDE

Version 12



™

How to contact us

Direct all inquiries to:

Kisco Systems LLC
54 Danbury Rd
Suite 439
Ridgefield, CT 06877

Phone: (518) 897-5002
Email: support@kisco.com

SafeNet/i Website:	www.safeneti.com
SafeNet/i Support Website:	https://www.kisco.com/safenet/support/index.html
Kisco Website:	https://www.kisco.com/

TABLE OF CONTENTS

Special Notices

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

IBM i	i OS
IBM i Access for Windows	PC Support/400
OS/2	IBM QRadar Security Intelligence Platform

The following terms are trademarks of Microsoft Corporation:

Microsoft Explorer	Microsoft Excel
ODBC	Microsoft Access
Windows XP	Microsoft Query
Windows Vista	Windows 7
Windows 8	Windows 10

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.

Log files can be specified as a system journal or a database file, or both.

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 by IP Address

SafeNet/i allows you to control access to certain servers by IP address.

See the **WRKSRV** command to determine which server functions can check for valid IP addresses.

Limit Access to Spooled Files

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

Profile Swapping

SafeNet/i can be configured to 'swap' user profile authorities when accessing the server via an exit point.

SafeNet/i allows you to select different SwapTo profiles for a user based on the Server Function they are using to access IBM i. (i.e., which Exit Point they are accessing)

By defining a User and Server ID-based SwapTo profile, you can attain a more granular security approach when utilizing the Swap Profile function of **SafeNet/i**. See the WRKSWPRF command for more information.

TCP Sockets

SafeNet/i can be configured to control all TCP sockets connections. TCP Listen, Accept and Connect actions can all be controlled, if required.

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 partial list:

- Windows XP
- Windows Vista
- Windows 7
- Windows 8
- Windows 10
- 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
- TCP sockets for any TCP application (Listen, Accept, Connect)

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 11 requires IBM i Version 7 Release 1 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.

Server Lookup Sequence

SafeNet/i supports group and supplemental profiles only if you purchased an unlimited user license of the product.

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

SERVER LOOKUPS

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

Object Lookup Sequences

SafeNet/i checks all possible authority and object/library combinations based upon settings within the CHGSPCSET command.

The object checking sequence is determined by the *OBJCHKSEQ* parameter

The object checking stop point is determined by the *OBJCHKSTOP* parameter

OBJECT LOOKUPS

System Settings for Object Lookup Process:

1. Use the following parameters in the CHGSPCSET command:

    a. **OBJCHKSEQ -** Object Checking Sequence
        i. ***STD** (See default sequence)
        ii. *ALT1 (See Alternate Seq#1)
        iii. *ALT2 (See Alternate Seq#2)
        iv. *ALT3 (See Alternate Seq#3)

    b. **OBJCHKSTOP -** When to stop object lookups.
        i. ***OnMatch** (like current, stops on any matching rule found)
        ii. *OnAccept (stop when accepted matching rule found)
        iii. *OnReject(stop when rejecting match found)
        iv. *AtEnd (stop only when all possible entries checked)

    c. **GENCHK** – Controls Generic Object Lookups. (i.e. QGPL/ABC*)
        i. *YES – Perform generic object searches.
        ii. *NO – Do not perform generic object searches.

STANDARD OBJECT LOOKUP SEQUENCE V8, V9, V10

*CHGSPCSET OBJCHKSEQ (*STD) - Default*

Lookup Sequence #	***Is the***	***authorized to***	
1	User	Library	Specific Object
2	Group/Supplemental Group	Library	Specific Object
3	User	Library	*ALL
4	User	Library	Generic Object
5	Group/Supplemental Group	Library	*ALL
6	Group/Supplemental Group	Library	Generic Object
7	User	*ALLLIB	*ALL
8	Group/Supplemental Group	*ALLLIB	*ALL

ALTERNATE OBJECT LOOKUP SEQUENCE #1

*CHGSPCSET OBJCHKSEQ (*ALT1)*

Lookup Sequence #	***Is the***	***authorized to***	
1	User	Library	Specific Object
2	User	Library	Generic Object
3	User	Library	*ALL
4	User	*ALLLIB	*ALL
5	Group/Supplemental Group	Library	Specific Object
6	Group/Supplemental Group	Library	Generic Object
7	Group/Supplemental Group	Library	*ALL
8	Group/Supplemental Group	*ALLLIB	*ALL

ALTERNATE OBJECT LOOKUP SEQUENCE #2

*CHGSPCSET OBJCHKSEQ (*ALT2)*

Lookup Sequence #	***Is the***	***authorized to***	
1	User	Library	Specific Object
2	Group/Supplemental Group	Library	Specific Object
3	User	Library	Generic Object
4	Group/Supplemental Group	Library	Generic Object
5	User	Library	*ALL
6	Group/Supplemental Group	Library	*ALL
7	User	*ALLLIB	*ALL
8	Group/Supplemental Group	*ALLLIB	*ALL

ALTERNATE OBJECT LOOKUP SEQUENCE #3

*CHGSPCSET OBJCHKSEQ (*ALT3)*

Lookup Sequence #	***Is the***	***authorized to***	
1	User	*ALLLIB	*ALL
2	User	Library	Specific Object
3	User	Library	Generic Object
4	User	Library	*ALL
5	Group/Supplemental Group	*ALLLIB	*ALL
6	Group/Supplemental Group	Library	Specific Object
7	Group/Supplemental Group	Library	Generic Object
8	Group/Supplemental Group	Library	*ALL

Special Considerations for Object Lookups

1. Exclusion Rules: Any matching Object Exclusion rule will STOP the lookup process regardless of above CHGSPCSET parameter settings. This is the current process and will remain.

2. QSYS.LIB path change: If *LEGACYPATH* parameter in CHGSPCSET is set to *NO, then any IFS Path request (*FileServer and *FTPServer) containing a /QSYS.LIB/ path will be processed as a normal object authority lookup as outline above.

   If the *LEGACYPATH* parameter is set to *YES, all /QSYS.LIB/ requests will be checked against the WrkUsrPth (long path) control entries.

   *(***YES** maintains existing SafeNet installation compatibility*)

Path Lookup Sequences

SafeNet/i checks all possible authority and path combinations based upon settings within the CHGSPCSET command.

The sequence to perform IFS path authority lookups is determined by the *PTHCHKSEQ* parameter

The *PTHCHKSTOP* parameter determines where IFS checking stops within **SafeNet/i**

PATH LOOKUPS

These new options are available **ONLY IF *LONG Path** type is **ACTIVE**. See the *PATHL* parameter on the CHGSPCSET command.

System Settings for Path Lookup Process:

1. Use the following parameters in the CHGSPCSET command:

    a. **PTHCHKSEQ** - IFS Path Checking Sequence
        i. ***STD** (See current sequence)
        ii. *ALT1 (See Alternate Seq#1)
        iii. *ALT2 (See Alternate Seq#2)
        iv. *ALT3 (See Alternate Seq#3)

    b. **PTHCHKSTOP** - When to stop path search/lookups.
        i. ***OnMatch** (like current, stops on any matching rule found)
        ii. *OnAccept (stop when accepted matching rule found)
        iii. *OnReject(stop when rejecting match found)
        iv. *AtEnd (stop only when all possible entries checked)

    c. **LEGACYPATH**– Maintains compatibility to current IFS Path searches/lookups for QSYS.LIB long path entries. *This is a temporary parameter to maintain backwards compatibility.*
    See Note below for further details.
        i. ***YES** – Check the long path file (WrkUsrPth) for QSYS.LIB type requests.
        ii. *NO – Treat all QSYS.LIB path requests as normal system objects. Use the normal object checking routines for these path types. (see WrkUsrObj) . Each request is broken down to Library and objects.
        i.e. a path of: /QSYS.LIB/QGPL.LIB/ABC.FILE = QGPL/ABC for object checking.

STANDARD IFS PATH LOOKUP SEQUENCE V8, V9, V10

CHGSPCSET PTHCHKSEQ (*STD) - Default

Lookup Sequence #	***Is the***	***authorized to***		
1	User	/*		
2	Group/Supplemental Group	/*		
3	User	Specific Path		
4	Group/Supplemental Group	Specific Path		
5	User	Generic Path		
6	Group/Supplemental Group	Generic Path		
7	User	*ALLFLR	*ALL	
8	Group/Supplemental Group	*ALLFLR	*ALL	

ALTERNATE IFS PATH LOOKUP SEQUENCE #1

CHGSPCSET PTHCHKSEQ (*ALT1)

Lookup Sequence #	***Is the***	***authorized to***		
1	User	Specific Path		
2	User	Generic Path		
3	User	/*		
4	User	*ALLFLR	*ALL	(WrkUsrObj entry)
5	Group/Supplemental Group	Specific Path		
6	Group/Supplemental Group	Generic Path		
7	Group/Supplemental Group	/*		
8	Group/Supplemental Group	*ALLFLR	*ALL	(WrkUsrObj entry)

ALTERNATE IFS PATH LOOKUP SEQUENCE #2

CHGSPCSET PTHCHKSEQ (*ALT2)

Lookup Sequence #	***Is the***	***authorized to***		
1	User	Specific Path		
2	Group/Supplemental Group	Specific Path		
3	User	Generic Path		
4	Group/Supplemental Group	Generic Path		
5	User	/*		
6	User	*ALLFLR	*ALL	(WrkUsrObj entry)
7	Group/Supplemental Group	/*		
8	Group/Supplemental Group	*ALLFLR	*ALL	(WrkUsrObj entry)

ALTERNATE IFS PATH LOOKUP SEQUENCE #3

CHGSPCSET PTHCHKSEQ (*ALT3)

Lookup Sequence #	***Is the***	***authorized to***		
1	User	/*		
2	User	*ALLFLR	*ALL	(WrkUsrObj entry)
3	User	Specific Path		
4	User	Generic Path		
5	Group/Supplemental Group	/*		
6	Group/Supplemental Group	*ALLFLR	*ALL	(WrkUsrObj entry)
7	Group/Supplemental Group	Specific Path		
8	Group/Supplemental Group	Generic Path		

*Special Considerations for Path Lookups (*File and *FTP Servers)*

1. Exclusion Rules: Any matching Object Exclusion rule will STOP the lookup process regardless of above CHGSPCSET parameter settings. This is the current process and will remain.

2. ***SHORT Path type is being deprecated as of this release.** *SHORT path support will be removed in a future release of **SafeNet/i**. (see CHGSPCSET *PATHL* parameter)

3. Note: **The parameter *LEGACYPATH* is temporary in nature.** The ability to have QSYS.LIB entries in the PCACCLNG file (WrkUsrPth) is being **deprecated** in this release and will be removed in a future release of **SafeNet/i**. This parameter will also be removed in a future release of **SafeNet/i**.

   If you currently have QSYS.LIB entries in WrkUsrPth, you should plan on moving required entries into WrkUsrObj. (Standard Object Control)

   Having this option set to ***YES** will cause the Path lookup sequence to continue checking the WrkUsrPth entries for any QSYS.LIB request.

   Having this option set to ***NO** will cause all QSYS.LIB paths to be treated as normal native DB requests and all object authority searches will be done exclusively against the WrkUsrObj entries.

   ***NO** will be the Default for new **SafeNet/i** installations.
   ***YES** is the default for upgrading customers.

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 - 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
- IP Addresses (Source and Target)

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 and Level 4)

For certain servers, you can limit access by setting up a simple address table. You can accept or reject specific IP addresses or ranges of addresses. You can also limit the amount of logging by using TCP/IP address controls.

See the WRKSRV command to determine which server functions can check for valid IP 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 1, 'First Time Installation' in the Install and Upgrade 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, 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. Determine which Object and Path lookup sequence you will use. (see 'Security Lookup Sequence' in the SafeNet/i Reference Guide or refer to the CHGSPCSET command)

3. 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)

4. Decide which of your users will have access to the servers.

5. Decide what authority the users will have to objects on the system.

6. Decide which SQL and FTP statements and CL commands your users will need.

7. Decide if you wish to use TCP/IP address controls.

8. Set up long path entries if required.

   Note: *SHORT path support is being deprecated.

9. Decide if you wish to use the Alert Notification feature of **SafeNet/i**.

10. Decide if you wish to use Profile Swapping.

    New with V10, you can specify swap profiles based on specific users and server combinations.

11. Authorize the users and/or *PUBLIC to the server functions.

12. Authorize users and/or *PUBLIC to objects, if necessary.

13. Authorize users and/or *PUBLIC to SQL, FTP statements, CL commands and TCP/IP tables, if necessary.

14. Enter exclusion rules, if any.

15. 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.

16. Change server Security Level settings to desired levels; flip Future and Current security settings. This activates all of the authority checking routines.

17. 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 Server*s 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 configuring **SafeNet/i** 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.

Note: All usage and security reports within **SafeNet/i** can be run against any archive file/member and library. For more information, see the section on archiving in Chapter 5, 'Reports' in the **SafeNet/i** Reference Guide.

New Option for Auto-Enrollment Reports

SafeNet/i has added the ability to include rejections for the auto enrollment reports.

By including rejections on the auto enrollment reports, you can see in advance all of the rejection possibilities for failing transaction, and this will help you create all of the access rules once rather than adopting a trial and error approach.

The INCREJ parameter only appears when you specify to run the auto enrollment reports. You will need to use the F10 key to see additional parameters. It is a *YES/*NO parameter and defaults to *NO.

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 4 - 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
```

Adding Additional Logging Jobs

When your system experiences an extremely high volume of network transactions, you can add additional logging jobs to **SafeNet/i**

To change the number of active **SafeNet/i** Transaction logging jobs:

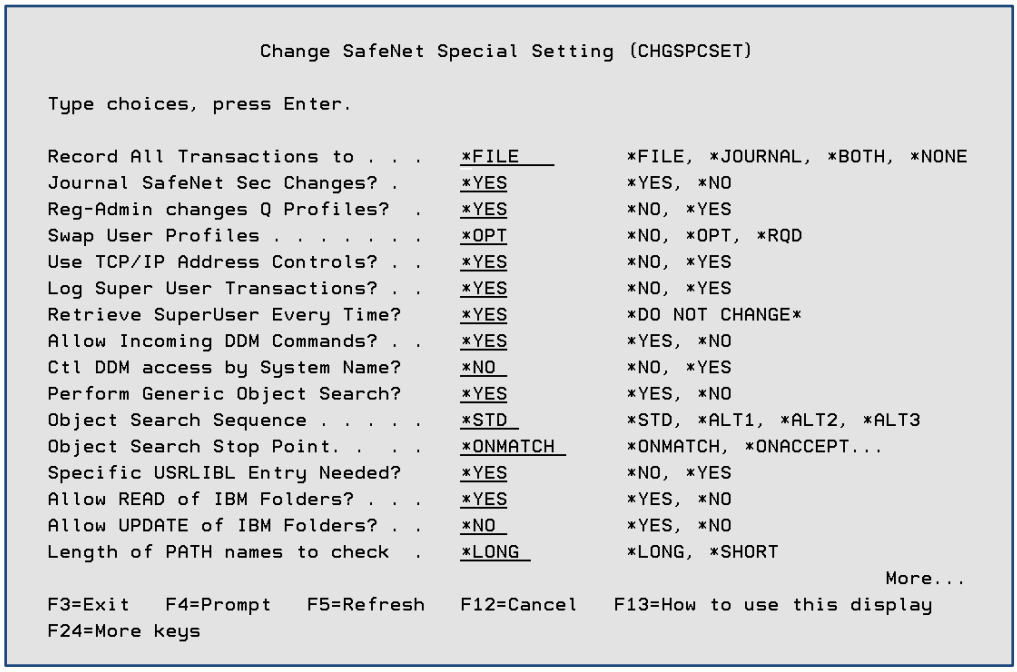
1. Issue the **ENDTRP** command to shut down the active logging job(s) in the SafeNet Subsystem
2. Use the **CHGSPCSET** command or use the SafeNet/i Main Menu (SN1), **Option 2 – Special SafetNet Settings**, to change parameter *DFTJOBS* to the desired value (1-9)
3. Issue the **STRTRP** command to reactivate the logging job(s)

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.



```
                  Change SafeNet Special Setting (CHGSPCSET)

Type choices, press Enter.

Record All Transactions to . . .   *FILE___       *FILE, *JOURNAL, *BOTH, *NONE
Journal SafeNet Sec Changes? .     *YES           *YES, *NO
Reg-Admin changes Q Profiles?  .   *YES           *NO, *YES
Swap User Profiles . . . . . .     *OPT           *NO, *OPT, *RQD
Use TCP/IP Address Controls? . .   *YES           *NO, *YES
Log Super User Transactions? . .   *YES           *NO, *YES
Retrieve SuperUser Every Time?     *YES           *DO NOT CHANGE*
Allow Incoming DDM Commands? . .   *YES           *YES, *NO
Ctl DDM access by System Name?     *NO            *NO, *YES
Perform Generic Object Search?     *YES           *YES, *NO
Object Search Sequence . . . . .   *STD           *STD, *ALT1, *ALT2, *ALT3
Object Search Stop Point. .  . .   *ONMATCH       *ONMATCH, *ONACCEPT...
Specific USRLIBL Entry Needed?     *YES           *NO, *YES
Allow READ of IBM Folders? . . .   *YES           *YES, *NO
Allow UPDATE of IBM Folders? . .   *NO            *YES, *NO
Length of PATH names to check  .   *LONG          *LONG, *SHORT
                                                                    More...
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

CHGSPCSET Command

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

Parameter	Screen Selections	Value	Description
LOGALL	Record All Transactions	****FILE*** *JOURNAL *BOTH *NONE	Specifies whether or not all network requests are logged: • *FILE logs all network requests into PCSECLIB/TRAPOD physical file • *JOURNAL logs all network requests into the TRAPJRN Journal • *BOTH logs all network requests into both the 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 SAFENET journal
QPROFS	Reg-Admin changes Q Profiles?	****NO*** *YES	Specifies whether to allow a regular SafeNet admin to change IBM supplied Q profile authorities and work with *ALLIB/ *ALLFLR security entries: • *YES allows regular administrators to change Q profile authorities and work with *ALLLIB/ *ALLFLR security entries • *NO allows only Super-Admins to change Q profile and *ALLLIB/ *ALLFLR authorities
SWAPU	Swap User Profiles	*NO ****OPT*** *RQD	Specifies whether to allow or require a swapping profile to be used within **SafeNet/i**.
LOGSUSR	Log Super User Transactions	****YES*** *NO	Indicates whether or not to log super user requests
SUSRCHK	Retrieve SuperUser Every Time	****YES*** *NO	Specifies whether to retrieve the list of Super-Users every time a transaction is processed or only at program initialization time. • *YES retrieves the list of Super-Users every transaction • *NO loads the Super-User list at program initialization time ONLY

			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. 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.**
ALWDDM	Allow Incoming DDM Commands	***YES*** *NO	Specifies whether commands received over the *DDM or *RMTSRV servers should be processed or rejected. 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 ALL incoming command processing by the *Distributed Data Management* and the *Remote Command Program Call* 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.
DDM	Use system name for DDM requests	*YES ***NO***	Specifies 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/i** for the system name to DDM server, and the objects, commands, etc. that the 'sourcesystem-name' will access. **SafeNet/i** allows you to add profiles to the setup even if no IBM i profile exists; in this case, use the source

			system name.
GENCHK	Perform Generic Object Search?	***YES*** *NO	Specifies whether generic object checking is performed as part of the user to object authority checking sequence. If you use generic object entries in WRKUSROBJ, this must be *YES. For performance, this can be set to *OFF if you do not use Library/OBJ* (generic object) entries. Default is *YES.
OBJCHKSEQ	Object Search Sequence	***STD*** *ALT1 *ALT2 *ALT3	Determines the sequence to perform object authority lookups within **SafeNet/i**. For compatibility with existing installations (V10 and earlier), the default entry is *STD. Changing this setting may affect user access via the network server points. Make sure you have analyzed the impact by using the on-line transaction tester (PCTESTR) or the Security Report (PRTSECRPT). Use these programs to test how changing this setting will affect your installation. See additional parameters on those programs for usage. DO NOT change this setting unless you know exactly what to expect. For specifics regarding these settings, see 'Security look up routines' in this manual.
OBJCHKSTOP	Object Search Stop Point	***ONMATCH*** *ONACCEPT *ONREJECT *ATEND	Determines the point where object checking stops within **SafeNet/i**. For compatibility with existing installations (V10 and earlier), the default entry is *ONMATCH. Changing this setting may affect user access via the network server points. Make sure you have analyzed the impact by using the on-line transaction tester (PCTESTR) or the Security Report (PRTSECRPT). Use these programs to test how changing this setting will affect your installation. See additional parameters on those programs for usage. DO NOT change this setting unless you know exactly what to expect. • *ONMATCH stops the Object Authority

			Lookup upon finding the first matching user to object entry, regardless of whether the entry is ACCEPTED or REJECTED • *ONACCEPT stops the Object Authority Lookup upon finding the first ACCEPTED matching user to object entry. • *ONREJECT Object Authority Lookup stops upon the first REJECTED matching user to object entry. • *ATEND stops the Object Authority Lookup upon exhausting all possible user to object entries. The status of the last matching record will be returned. (ACCEPT or REJECT)
USRLIBL	Specific USRLIBL Entry Needed	*YES ***NO***	Specifies whether a specific *USRLIBL entry is required in the SafeNet control file (WRKUSROBJ) when transactions are received with unqualified object names. Action to take when no library is specified in a request: • *YES REQUIRES that a *USRLIBL entry exist in WRKUSROBJ • *NO ACCEPTS all unqualified object requests WITHOUT checking for a corresponding *USRLIBL entry in WRKUSROBJ. *NO is a potential SECURITY RISK
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 list is contained in file IBMFLR. You may add additional entries as required to this file. Add entries using UPDDTA. • *YES allows READ of IBM Folders • *NO rejects all READ attempts to IBM folders. (Can be overridden at the user to object level) 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 *File Server* function is set to Level 4, this parameter is in effect. 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.
UPDTIBM	Allow UPDATE of IBM Folders	***YES*** *****NO	This option controls automatic Write/ Update authority to IBM supplied folders. Whenever the **SafeNet/i** Security Level for the *File Server* function is set to Level 4, this parameter is in effect. Initially **SafeNet/i** sets this to *YES. *NO rejects all UPDATE attempts to IBM folders. (Can be overridden at the user to object level)
PATHL	Length of PATH names to check	***LONG*** *****SHORT	Specifies whether to check the Long mixed case or standard 10 position upper case PATH Lengths in the FTP and FILESRV servers. *LONG Path is the default beginning V10 of **SafeNet/i**. *SHORT Path support is being deprecated with this release update.
PTHCHKSEQ	Path Search Sequence	***STD*** *ALT1 *ALT2 *ALT3	Determines the sequence to perform IFS Path authority lookups within **SafeNet/i**. For compatibility with existing installations (V10 and earlier), the default entry is *STD. Changing this setting may affect user access via the network server points. This parameter is only available when PATHL parameter is set to *LONG path support. Make sure you have analyzed the impact by using the on-line transaction tester

			(PCTESTR) or the Security Report (PRTSECRPT). Use these programs to test how changing this setting will affect your installation. See additional parameters on those programs for usage. DO NOT change this setting unless you know exactly what to expect. For specifics regarding these settings, see 'Security look up routines' in this manual.
PTHCHKSTOP	Path Search Stop Point	***ONMATCH*** *ONACCEPT *ONREJECT *ATEND	Determines the point where IFS Path checking STOPS within **SafeNet/i**. For compatibility with existing installations (V10 and earlier), the default entry is *ONMATCH. Changing this setting may affect user access via the network server points. This parameter is only available when PATHL parameter is set to *LONG path support. Make sure you have analyzed the impact by using the on-line transaction tester (PCTESTR) or the Security Report (PRTSECRPT). Use these programs to test how changing this setting will affect your installation. See additional parameters on those programs for usage. DO NOT change this setting unless you know exactly what to expect. • *ONMATCH stops the IFS Path Authority Lookup upon finding the first matching user (or group) to path entry(WRKUSRPTH), regardless if entry is ACCEPTED or REJECTED. • *ONACCEPT stops the IFS Path Authority Lookup upon finding the first ACCEPTED matching user (or group) to path entry. • *ONREJECT stops the IFS Path Authority Lookup upon finding the first REJECTED matching user (or group) to

			path entry. • *ATEND stops the IFS Path Authority Lookup after exhausting all possible user (or group) to path entries. The status of the last matching record will be returned (ACCEPTED or REJECTED).
GENPTH	Generic Path LTR or RTL?	*LTR ***RTL***	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. This parameter only affects systems set to *LONG path support.
LEGACYPATH	Legacy QSYS.LIB Path Support? Existing Installs New Installs	 ***YES*** *NO *YES ***NO***	This parameter allows you continue using the legacy SafeNet QSYS.LIB path search/ lookup support. This parameter, when set to *YES will continue to check the user to IFS Path entries (WRKUSRPTH) when any transaction that contains a Native DB path directory like: "/QSYS.LIB/xxx.file/ xxx. mbr". If this parameter is set to *NO, all requests that are paths to QSYS.LIB will use the standard User to Object authentication entries (WRKUSROBJ). This parameter is only available when PATHL parameter is set to *LONG path support. • *NO Any request for a QSYS.LIB Path name will use **SafeNet/i** standard User to Object searches for authentication (WRKUSROBJ). • *YES When set to *YES, any request for a QSYS.LIB path name will use SafeNet's legacy lookup/search method against the User to Path entries. (WRKUSRPTH) This value maintains compatibility to

			early V10 and prior SafeNet installations. This lookup method is being deprecated. This method will be removed from SafeNet support in a future release. Please convert any QSYS.LIB path entries in WRKUSRPTH into standard SafeNet User to Object entries (WRKUSROBJ).
DFTJOBS	Default Number of Logging Jobs to Start	# of jobs **1 (one)**	Specifies the number of SAFELOGING transaction log jobs that are started by default. 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. Number of logging jobs to autostart with the STRTRP command
TCPIPS	Use TCP/IP address controls?	***NO** *YES	This is a global setting. You must set this to *YES if you intend to use any IP address controls

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.

See the WRKSRV command, option F18 for more exclusion and user exit program options.

SAP users: Please see the reference guide for further instructions and options for co-existence.

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.

Support for SAP Exit Point

SafeNet/i includes temporary support for customers who are running SAP on their IBM i platform and have registered the SAP exit point. When **SafeNet/i** registers an exit point, if it finds a point already registered, it will normally flag the point with a level 5 and not register the actual **SafeNet/i** program. When this happens, the existing exit program stays in place and the **SafeNet/i** program does not enforce security for that exit point.

When an SAP customer registers their exit program on the *SQL exit pint (Database Server – entry), **SafeNet/i** will not function. Since the SAP exit program is not enforcing security, customers will want to have **SafeNet/i** active for this exit point. SAP has a provision for this with their product that involves registering the **SafeNet/i** program in a file in the IFS. The specific **SafeNet/i** program that should be registered is named SAFENET in library PCSECLIB. See the SAP user's guide for specific instruction on how to do this registration.

When the **SafeNet/i** exit point registration is done, **SafeNet/i** has now been modified to specifically look for the SAP exit program. When it is found, rather than flagging the point at Level 5, it will process it as a normal registration. It is the customer's responsibility to make sure that the correct program is registered to SAP in the IFS file.

SafeNet/i Integration with IBM QRadar

SafeNet/i can now integrate with IBM's QRadar Network Anomaly Detection product. An additional documentation manual is now available for this feature for customers wanting to implement this integration.

Chapter 5 - SAFENET/i CHANGES BY RELEASE

To see the latest updates and enhancements to SafeNet/i visit the support pages:

https://www.kisco.com/safenet/support/snupdats.html

NEW Version 11 Enhancements

1. TCP *Sockets controls have been added. **SafeNet/i** will now log and/or control all TCP/IP connections. You can monitor TCP Accept, Listen and Connect requests. You can also set up controls by user, server and IP address.

2. A new “Advanced View” is now available for customers with an unlimited user license when using any of the WRKUSRXXX commands. This view will display any user entries (Groups and Public) that affect the current user being maintained through the WRKUSRXXX commands.

3. Added a User Notes field to all IP control entries for user documentation purposes.

4. Logging can now be controlled by specific user even at Level 1. Simply use the WRKUSRSRV command to enroll the user or group profile, and set the override logging level.

5. Changes can now be made directly to file PCACCESU (User to Server Authorizations). In prior releases, file maintenance had to be done via the WRKUSRSRV command exclusively to correctly update application user indexes and that caused issues for customers using replication software. SafeNet now utilizes a trigger program so direct file maintenance is now possible.

6. By default, **SafeNet/i** will always allow access to the new Access Client 5250 Emulator QSYS/QSYCKUFU program. This allows access to the new 5250 client without specific SafeNet authorization entries.

INDEX