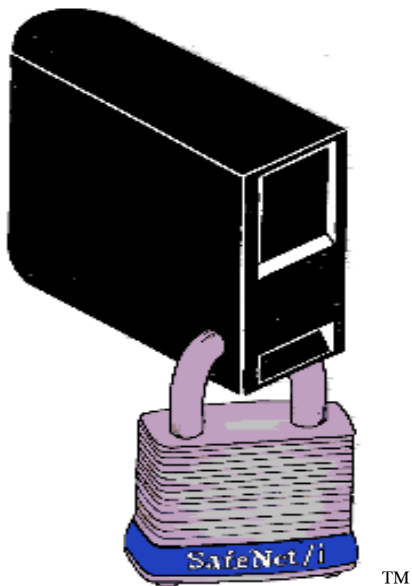


SAFENET/i

REFERENCE GUIDE

Version 10



© 2013 MP Associates of Westchester, Inc.

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 - SETTING UP USERS.....	1.1
<i>Super User Control – Trusted Users</i>	<i>1.5</i>
<i>Setting the User Logging Levels</i>	<i>1.6</i>
<i>Entering User Security Levels</i>	<i>1.7</i>
<i>Entering User Authorities to Objects.....</i>	<i>1.9</i>
<i>Entering User Authorities to SQL Statements</i>	<i>1.14</i>
<i>Entering User Authorities to FTP Statements</i>	<i>1.16</i>
<i>Entering User Authorities to CL Commands.....</i>	<i>1.20</i>
<i>Entering Long Path Names.....</i>	<i>1.22</i>
<i>Copying an Existing User to Set Up a New User in SafeNet/i.....</i>	<i>1.24</i>
<i>Removing a User from SafeNet/i.....</i>	<i>1.24</i>
<i>Removing Unknown Users from SafeNet/i.....</i>	<i>1.25</i>
<i>Removing Administrators from SafeNet/i</i>	<i>1.25</i>
<i>Maintain all Security for a User</i>	<i>1.26</i>
<i>Setting up Time of Day Controls.....</i>	<i>1.27</i>
CHAPTER 2 - SETTING UP SERVERS	2.1
<i>Recommended Server Settings</i>	<i>2.6</i>
<i>Entering Server Function Security Levels</i>	<i>2.9</i>
<i>Customer Exit Programs.....</i>	<i>2.11</i>
CHAPTER 3 - TELNET, TCP/IP ADDRESS CONTROLS	3.1
<i>Setting up TELNET.....</i>	<i>3.1</i>
<i>Kerberos.....</i>	<i>3.4</i>
<i>Setting up TCP/IP Address Controls</i>	<i>3.7</i>
CHAPTER 4 - SETTING UP FTP	4.1
<i>Setting up for Normal User IDs and FTP Servers.....</i>	<i>4.1</i>
<i>Setting up for ANONYMOUS FTP.....</i>	<i>4.6</i>
<i>Object Level Security for FTP Client Sessions.....</i>	<i>4.8</i>
CHAPTER 5 - REPORTS.....	5.1
<i>Setup Reports</i>	<i>5.2</i>
<i>Usage Reports.....</i>	<i>5.4</i>
<i>Run Security Report by User from Archive.....</i>	<i>5.6</i>
CHAPTER 6 - TESTING YOUR SECURITY SETTINGS	6.1
<i>Testing SafeNet/i settings based on your historical data.....</i>	<i>6.2</i>
<i>Batch Transaction Test Review/Report – Security Report by User</i>	<i>6.7</i>
<i>Recommended approach to testing</i>	<i>6.10</i>
<i>PCREVIEW.....</i>	<i>6.11</i>

CHAPTER 7 - BACKUPS AND PURGES.....	7.1
<i>Log file Purge</i>	<i>7.1</i>
<i>Automating the log file purge</i>	<i>7.4</i>
<i>Automating the One Step Security Report</i>	<i>7.4</i>
<i>Automating and Running the Security Report and the Log File Purge Together.....</i>	<i>7.5</i>
<i>Daily Backup Procedure.....</i>	<i>7.7</i>
CHAPTER 8 - JOURNALING SAFENET ACTIVITY	8.1
<i>Journaling Security Files and Network Transactions</i>	<i>8.1</i>
<i>Verify or Delete Journal Receivers – STRPRGARC command</i>	<i>8.3</i>
<i>Convert and Print SafeNet/i Security Journals – CVTSECJRN command.....</i>	<i>8.4</i>
<i>Convert Network Transactions Journal Receivers – CVTTRNJRN command</i>	<i>8.6</i>
CHAPTER 9 - SPECIAL SAFENET CONSIDERATIONS	9.1
<i>Excluding an Exit Point from SafeNet/i Checking.....</i>	<i>9.1</i>
<i>Resetting Level 5 within SafeNet/i</i>	<i>9.3</i>
<i>Pre-Power Down Program Point</i>	<i>9.4</i>
<i>Profile Swapping.....</i>	<i>9.5</i>
<i>Files Contained in SafeNet/i</i>	<i>9.7</i>
<i>Extra Security for TRAPOD.....</i>	<i>9.8</i>
<i>SafeNet/i Commands.....</i>	<i>9.9</i>
<i>Print Commands</i>	<i>9.11</i>
CHAPTER 10 - USING AUTOMATIC ALERT NOTIFICATION.....	10.1
<i>Activating SafeNet/i Alert Notification</i>	<i>10.2</i>
CHAPTER 11 - DHCP CONTROLS AND REPORTING	11.1
<i>Current DHCP Activity.....</i>	<i>11.3</i>
<i>Maintaining MAC Addresses</i>	<i>11.5</i>
<i>Fixed IP Addresses</i>	<i>11.6</i>
<i>Purging Expired DHCP Lease Information</i>	<i>11.7</i>
<i>Ping Checker.....</i>	<i>11.8</i>
CHAPTER 12 - PROBLEM DETERMINATION	12.1
<i>Error Message Received on the IBM i.....</i>	<i>12.1</i>
<i>Error Message Received on the Client</i>	<i>12.3</i>
<i>Examples of Client Error Messages</i>	<i>12.6</i>
<i>Error Codes which Appear in the Log.....</i>	<i>12.8</i>
<i>Additional Troubleshooting Tips</i>	<i>12.10</i>
CHAPTER 13 - DE-ACTIVATING AND REMOVING SAFENET.....	13.1
<i>De-activating SafeNet/i.....</i>	<i>13.1</i>
<i>Removing SafeNet/i from your system</i>	<i>13.3</i>
APPENDIX A - SERVER FUNCTION DESCRIPTIONS	A.1
<i>Original Servers.....</i>	<i>A.1</i>
<i>Optimized Servers</i>	<i>A.12</i>

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:

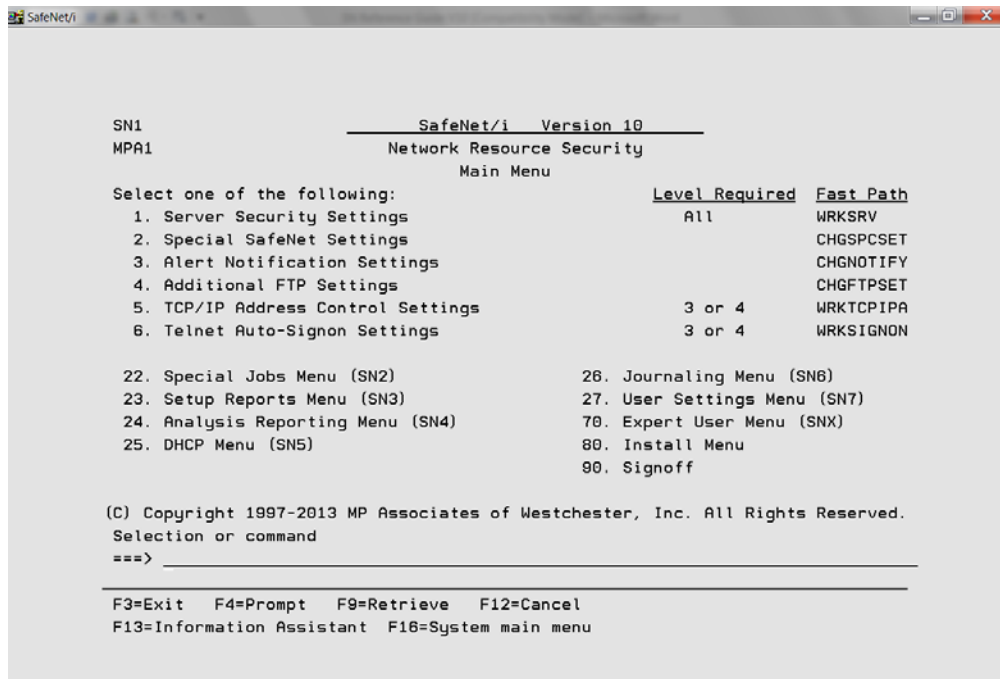
Windows XP	Microsoft Excel
Microsoft Explorer	Microsoft Access
ODBC	Microsoft Query
Windows Vista	Windows 2000
Windows 7	

SafeNet/i Reference Guide

Chapter 1 - SETTING UP USERS

Navigating through the screens and menus

You can perform each of the steps outlined in this chapter by using the corresponding option on the SafeNet/i Main Menu, SN1.



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

On any menu you can use the menu options or you can use the Fast Path commands that are listed to the right of the options.

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.

To navigate among the sub-menus you can type the menu option number or you can type the menu name on the command line.

Menu Option	Menu Description	Menu Name
21	Main Menu	SN1
22	Special Jobs Menu	SN2
23	Reports Menu	SN3
24	Analysis Reporting Menu	SN4
25	DHCP Menu	SN5
26	Journaling Menu	SN6
27	User Settings Menu	SN7

Option 21 will always take you back to the Main Menu (SN1).

Navigating User Setup Screens

When using the WRKUSRxxx maintenance screens the following command keys provide navigation within SafeNet/i.

F2	Display list of defined SafeNet/i users
F3	Exit
F6	Add new entries
F7	Toggle between the group profile* settings and the user profile settings when working with the user setting maintenance screens in SafeNet/i
F8	Display all the user profiles within the group*
F9	Advance to next user setting screen
F12	Cancel
HELP	Additional HELP displays

Note: To use Group Profiles, you must have an unlimited user license.

SafeNet/i using **Option 8 – Work with SafeNet Administrators** on SafeNet/i User Settings (SN7), SafeNet/i the IBM-supplied settings in SafeNet/i (see note below) SafeNet/i user or administrator ALWAYS SafeNet/i. U to suit your purposes.

Alternate Administrative Security

Beginning with SafeNet/i Version 10, you can change the way administrative security for SafeNet/i is handled on your system. You can now:

- Permit regular SafeNet/i Administrators to copy or remove rules from SafeNet/i and assign *ALL entries
- Authorize only a Super Admin to change the LOGALL parameter in the Change SafeNet Special Setting (CHGSPCSET) command
- Allow regular Administrators to work with or modify user profiles that start with the letter Q

The QPROFS parameter on the CHGSPCSET command controls this function.

From the Main Menu (SN1) use **Option 2 – Special SafeNet Settings** or the CHGSPCSET command to change the QPROFS parameter to *YES or *NO.

See Chapter 5 in the *SafeNet/i Implementation Guide* for more details on the CHGSPCSET command.

Important Note

Prior to this change, a regular SafeNet/i Administrator or a Super Admin was allowed to use the Change SafeNet Special Settings command, CHGSPCSET. With this release, you must be a Super Admin to access this command.

THIS CAN CREATE A PROBLEM if you have included this command in your system SAVE process to stop transaction logging during the backup.

We recommend that you remove this from your SAVE procedure now and use the IBM save-while-active process instead from this point on.

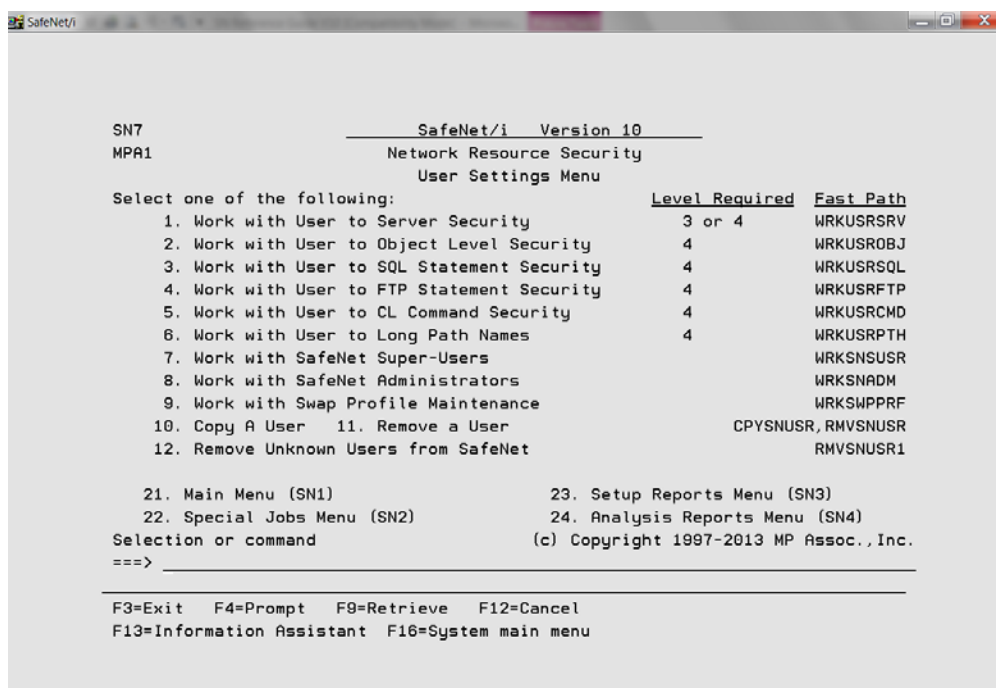
Group Profile as SafeNet/i Administrator

You can enroll group profiles as SafeNet/i Administrators. When you enroll a group profile as an administrator, every member of the group will be considered to be an administrator by SafeNet/i.

Super User Control – Trusted Users

Under special circumstances it may be necessary to have a user that should not be checked through all the **SafeNet/i** security routines. Transactions from these users can bypass the traditional **SafeNet/i** security routines; you can choose to log the Super User transactions or not log these transactions.

To maintain these users, select **Option 7 – Work with SafeNet Super Users** from the User Settings Menu



Note: You can turn logging on or off for Super Users by using the CHGSPCSET command and changing the LOGUSER parameter to *YES or *NO. See Chapter 5 in the *SafeNet/i Implementation Guide* for more details on the CHGSPCSET command.

This should only be used under conditions when you want **NONE** of the specified users' transactions to be checked through **SafeNet/i** security routines. This is a global setting for all Super Users.

Setting the User Logging Levels

The valid logging levels are:

Logging Level A	Log all transactions
Logging Level R	Log only rejected requests
Logging Level N	No logging

As you set up your user logging levels, please keep in mind the following:

- If you set the logging level on the Server Function (WRKSRV) to *NO LOGGING* or *REJECTIONS*, the Server Function (WRKSRV) setting will override the individual user logging level.
- If you set the logging level on the Server Function to *ALL*, the individual user logging level will override the Server Function logging level.

To make sure you are logging transactions correctly, we recommend that when you initially set up **SafeNet/i** you set the Server Functions to log *ALL* and set the User to Server logging levels to either *ALL* or *REJECTIONS*.

Then, after you have had some experience with checking the logs and interpreting the results, you may want to make changes for specific user and server combinations.

An example of this might include certain "trusted" user profiles. If you trust the user in question and are concerned about the size and amount of logging activity, you might choose to only record rejected transactions for that user.

Another example might be a known client server application that is clearly defined and does not need to be monitored. For these applications you might choose to stop logging altogether. We have found several fax applications that fall into this category. They generate a large number of entries that are really not needed for your purposes in controlling access security.

Entering User Security Levels

If you plan on setting any of the Server Functions to Level 3 or Level 4, and anticipate doing anything other than simply logging all requests, the first step in configuring **SafeNet/i** is to give the users authority to any Server Functions they require.

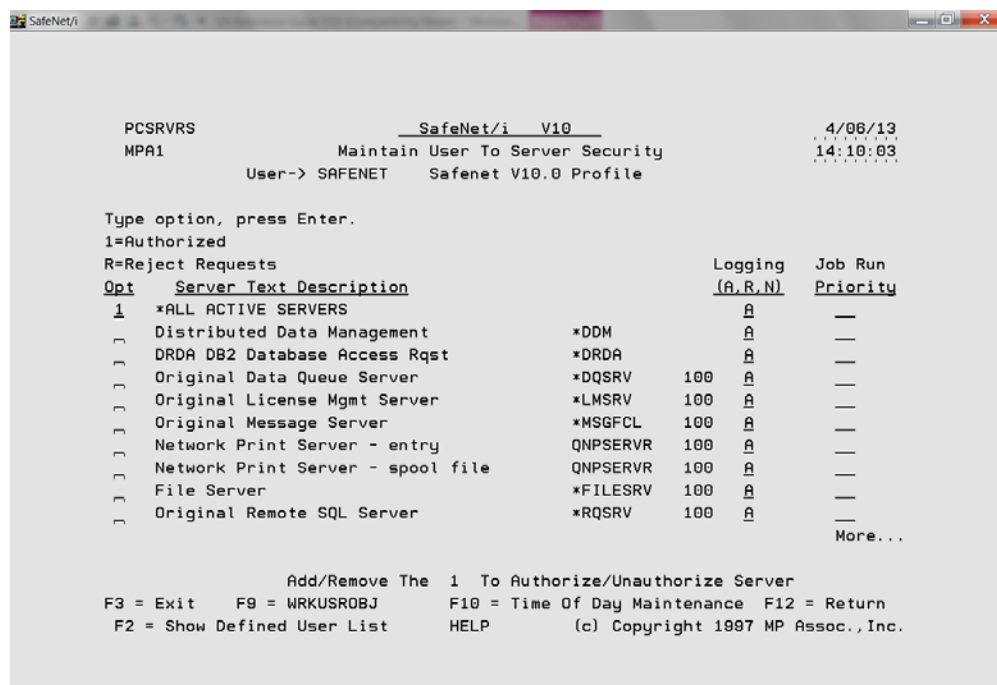
1. From the SafeNet/i User Settings Menu (SN7) select **Option 1 - Work with User to Server Security** or use **WRKUSRSRV** command

The *Work User to Server Security Enter User Profile* screen appears.

2. **Type the user profile** you will be setting up, or ***PUBLIC**, then **ENTER**.

If you would like a list of all user profiles on the system, press **F4** or type ***ALL**.

To see a list of users already defined within **SafeNet/i** type ***ALLDFN**.



The *Maintain User to Server Security* screen appears.

A list of all the servers is displayed.

3. If you would like to see the list of all users who have been defined within **SafeNet/i**, press **F2**.

Type 1 in the *Option* column in front of each server this user will have access to.

If they will have access to all the server functions, **select**

***ALL ACTIVE SERVERS**

To remove access to a particular server, remove the '1' and leave the *Option* column blank for that server.

4. **Enter** the *Logging Level* for each server.

A = All

R = Rejections only

N = No logging

When you have finished setting up servers for this user, press **ENTER**.

5. Enter the *Job Run Priority* for each server. Do this if you choose to override the operating system job priority defaults.

The job priority will be set when the user accesses this server. Valid job priorities are 00 (the default) through 99. A value of 00 indicates no change to the default job priority.

6. **Press F9** to continue to the next step - setting up user authorities to objects.

Entering User Authorities to Objects

Once you have given the user access to the servers, the next step is to enter the level of authority the user has to objects on the IBM i if you plan on setting any of the servers to Level 4.

1. If you used F9 from the previous screen, skip to Step 4.
2. If you are currently on the SafeNet/i User Settings Menu (SN7), select **Option 2 - Work with User to Object Level Security** or use **WRKUSROBJ** command

The *Work User to Object Security* screen is displayed.

3. Type **the user profile name, the Group** or ***PUBLIC**, then **ENTER**.

To list all of the user profiles on the system, press **F4** or type ***ALL**.

To see a list of users already defined within **SafeNet/i** type ***ALLDFN**.

PCACCSO SafeNet/i V10 4/06/13
MPA1 Maintain Authorized Objects By User 14:11:09
User-> SAFENET Safenet V10.0 Profile

Type option, press Enter.
4=Delete

Option	Library or Folder	Object or Sub-Flr	Read	Write	Delete	Existence-- Rights
-	*ALLFLR	*ALL	X	X	X	X
-	PCSECDTA	*ALL	X	X	X	X
-	PCSECLIB	*ALL	X	X	X	X
-	GRADENETC	*ALL	X	X	X	X
-	PCSECD80	*ALL	X	X	X	X
-	*ALLLIB	*ALL	X	X	X	X

Bottom

F2 = Show Defined SafeNet Users F3 = Exit F6 = Add
F9 = WRKUSRSQL F12 = Return HELP (c) Copyright 1997 MP Assoc., Inc

The *Add New Object Authorization* screen appears.

If you would like to see the list of all users who have been defined within **SafeNet/i**, press **F2**.

Note: If this user has already been set up in **SafeNet/i**, the *Maintain Authorized Objects by User* screen is displayed. Press **F6** to add new objects and authorities for this user.

4. In the *Library or Folder* column, **enter the name** of the library or folder, then **TAB** to the *Object or Sub-Flr* column and **type in the name** of the object or sub-folder.

Note: Allowed entries for **Library** or **Folder**

- *ALLLIB
- *ALLFLR
- Specific library name

When setting up a **library**, you must enter the **complete library name**. Generic library names are not allowed.

Allowed entries for **Object**

- *ALL
- Specific object
- Generic data/program or IBM i object name followed by * (FIL*)

NOT ALLOWED for object

- Long file or folder names - 10 position maximum (names over 10 are truncated)
- Generic sub-folder names (FOLD*)
- Generic folder content names

NOT ALLOWED for library

- Long folder names
- Generic folder names
- Generic library names
- *ALL

If granting rights to multiple objects in one library, you must list the library name multiple times or use a generic object name. For example:

<u>LIBRARY</u>	<u>OBJECT</u>
QUSRSYS	PAY1
QUSRSYS	PROJECT
QUSRSYS	PRT*

5. For *Data Rights*, **type an X** under the appropriate level of authority. Place an X for each data right that applies.
6. For *Existence Rights*, **type an X** if this user will be able to create, delete or move an object.

To assign EXCLUSIONS to objects and/or libraries, give the user no rights by leaving the *Data Rights* and *Existence Rights* columns blank.

7. Repeat these steps for each object or group of objects for this user profile.

PageDown to the next screen if you need more lines.

ENTER when you have finished keying in all necessary objects and rights.

The *Maintain Authorized Objects by User* screen is refreshed and all the information you just entered is displayed.

Press F9 to continue to the next step - setting up user authorities to SQL statements.

Reminder:

If you have already entered objects for a particular user, and you are updating their user to object level security, a list of existing object authorities will be displayed. To add more, **press F6**. To delete an existing entry, **type 4** in the *Option* column, then **ENTER**.

Exclusions

To give all users read access to all objects in all libraries, but exclude them from any objects in the PAYROLL library, give *PUBLIC READ authority to the library and exclude *PUBLIC from the PAYROLL library.

```
SafeNet/i

PCACCSO          SafeNet/i  V10          4/06/13
MPA1             Maintain Authorized Objects By User  14:14:26
                User-> *PUBLIC  *Public Authorities

Type option, press Enter.
4=Delete

Option  Library  Object  |-----Data Rights-----|Existence--|
Option  or Folder or Sub-Flr  Read  Write  Delete  Rights
-       -       -       -       -       -       -
-       QSRVAGT  *ALL    -       -       -       *EXCLUSION*
-       PAYROLL  *ALL    -       -       -       *EXCLUSION*
-       *ALLLIB  *ALL    X       -       -       -

Bottom

F2 = Show Defined SafeNet Users  F3 = Exit  F6 = Add
F9 = WRKUSRSQ  F12 = Return  HELP  (c) Copyright 1997 MP Assoc., Inc
```

If the PAYDEPT profile needs to use objects in the PAYROLL library, grant user profile PAYDEPT READ authority to the PAYROLL library.

```

SafeNet/i

PCACCSO          SafeNet/i  V10          4/06/13
MPA1             Maintain Authorized Objects By User  14:17:11
                User-> PAYDEPT

Type option, press Enter.
4=Delete

Option      Library      Object      |-----Data Rights-----|Existence--|
Option      or Folder    or Sub-Flr  Read  Write  Delete  Rights
-           PAYROLL      *ALL        X    -    -    -

Bottom

F2 = Show Defined SafeNet Users      F3 = Exit  F6 = Add
F9 = WRKUSRSQL      F12 = Return  HELP      (c) Copyright 1997 MP Assoc., Inc

```

This individual authority overrides the *PUBLIC authority.

Entering User Authorities to SQL Statements

If you are going to set the *SQL* servers to Level 4, the next step is to authorize users to the *SQL* Statements they may need.

1. If you used F9 from the previous screen, skip to Step 4.
2. If you are currently on the SafeNet/i User Settings Menu (SN7), select **Option 3 - Work with User to SQL Statement Security** or use **WRKUSRSQL** command

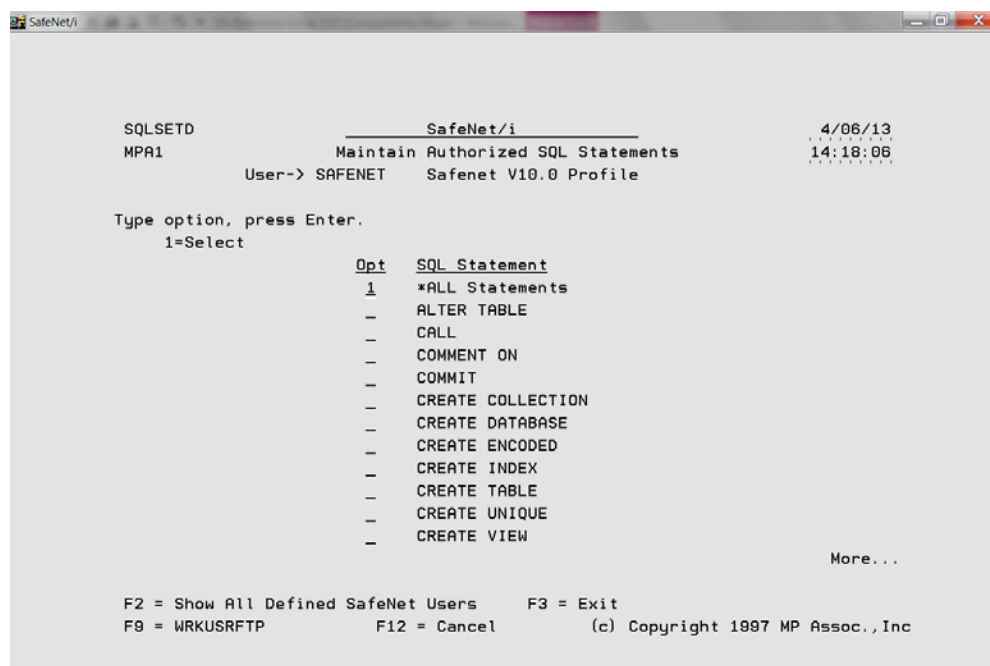
The *Work User to SQL Statements* screen is displayed.

3. **Type the user profile, the Group or *PUBLIC, then ENTER.**

If you would like a list of all user profiles on the system, press **F4** or type ***ALL**.

To see a list of users already defined within **SafeNet/i** type ***ALLDFN**.

The *Maintain Authorized SQL Statements* screen appears.



4. **Type 1** in front of each *SQL* statement that this user is permitted to use.

Selecting ***ALL Statements** authorizes the use to all *SQL* statements

To remove authorization to a selection, remove the 1.

If you would like to see the list of all users who have been defined within **SafeNet/i**, press **F2**.

5. When finished making all your selections, **ENTER**.
6. **Press F9** to advance to the next step - setting up user authorities to FTP statements.

Entering User Authorities to FTP Statements

Next you must authorize users to the FTP Statements they may need if you are going to set the *FTP Server* or *FTP Client* to Level 4.

1. If you used F9 from the previous screen, continue with Step 4.
2. If you are on the SafeNet/i User Settings Menu (SN7), select **Option 4 - Work with User to FTP Statement Security** or use **WRKUSRFTP** command

The *Work User to FTP Statements, Enter User ID* screen is displayed.

3. **Type the user profile** or ***PUBLIC** then **ENTER**.

If you would like a list of all user profiles on the system, press **F4** or type ***ALL**.

To see a list of users already defined within **SafeNet/i** type ***ALLDFN**.

The *Work with Authorized FTP Statements* screen appears.

SafeNet/i

FTPSETD
MPA1

SafeNet/i
Work With Authorized FTP Statements
User-> SAFENET Safenet V10.0 Profile

4/06/13
14:19:06

Type option, press Enter.
1=Select

Opt	FTP Operation	Associated FTP Command
1	Directory/Lib Create	MKDIR, XMKD
1	Directory/Lib Delete	RMD, XRMD
1	Set Current Dir	LCD, CWD, CDUP, XCWD
1	List Files	LIST, NLIST
1	File Deletion	DELE
1	Receiving Files	GET, MGET
1	Sending Of Files	PUT, APPEND, MPUT
1	Renaming Files	RNFR, RNTD
1	Execute CL Commands	Any CL - SYSCMD

Bottom

F2=Show Defined Users F3=Exit F4=Additional Settings F7=Alt Profiles
F9 = WRKUSRCMD F12 = Cancel (c) Copyright 1997 MP Assoc., Inc

4. **Type 1** in front of each FTP statement that this user is permitted to use.

To remove authorization to a statement, remove the 1.

If you would like to see the list of all users who have been defined within **SafeNet/i**, press **F2**.

5. Press F4 to display the *Maintain Special FTP Settings for Users* screen

Note: Special FTP settings for a user are allowed only when your system is at OS/400 V5R1 or higher. If you are at a previous operating system level, these settings have no effect.

```
FTPSET2D                               SafeNet/i                               4/06/13
                                         Maintain Special FTP Settings for Users      14:20:08

User->  SAFENET      Safenet V10.0 Profile

Initial Name Format->  *LIB              (*LIB, *PATH)
Initial List Format->  *DFT              (*DFT, *UNIX)
Initial Library----->  QGPL              Name, *USRPRF
Encrypted FTP Connection-->  0 (0=Allowed,1=Not Allowed,2=Required)

Initial Home Directory Path  Name of Path or *USRPRF
/
_____
_____
_____

CCSID of Initial Path--->  000000 (0 - 85533) 0=Default

F3 = Exit
F12=Return                                HELP      (c) Copyright 2001 MP Assoc., Inc
```

For this user, the initial Name Format and List Format will override the settings established by the *i OS Change FTP Server Attributes* command (CHGFTPA).

Select the parameters as follows:

Encrypted

- For SSL connections this should be set to 0 or 2
- For regular or non-SSL connections, leave this set to 0 or 1

PATH

- This field is in effect only when Name Format is set to *UNIX. The field should point to an actual IFS directory on the IBM i.

Name Format

- *LIB indicates that the user sees standard Library/Object IBM i style names
- *PATH displays PC or *UNIX style file and directory names.

List Format

- *DFT user sees standard IBM i CHGFTP server settings
- *UNIX user sees UNIX style directory listings

6. When finished making all your selections, **ENTER**.
7. **Press F9** to continue to the next step - setting up user authorities to CL commands.

Important Note:

When the FTP Client point is set to Level 4, only the GET and PUT FTP sub-commands are required. The other commands, when using the FTP Client, are for the TARGET SYSTEM ONLY (sent to/run on the target system).

When authorizing users to the GET/PUT sub-commands, the assumed object authority is reversed from authorities required for the FTP Server point and the same objects.

See the following examples.

Using FTP Client:

- Sending an object to a remote system
An FTP PUT of object ABC in an FTP Client session requires *READ authority to object ABC on the local machine.
- Get an object from a remote system
An FTP GET of object ABC in an FTP Client session requires *OBJMGT authority to the object ABC on the local machine.

Using FTP Server:

- Send an object to local system
An FTP PUT of object ABC in an FTP Server session requires *OBJMGT authority to the object ABC on the LOCAL machine.
- Get an object from the local system

An FTP GET of object ABC in an FTP Server session requires *READ authority to the object ABC on the LOCAL machine.

Entering User Authorities to CL Commands

Next, if you plan on setting the *FTP*, *DDM* or *Remote Command Servers* to Level 4, you must authorize users to the CL commands they may need.

1. If you used F9 from the previous screen, continue with Step 4.
2. From the SafeNet/i User Settings Menu, select **Option 5 - Work with User to CL Command Security** or use **WRKUSRCMD** command

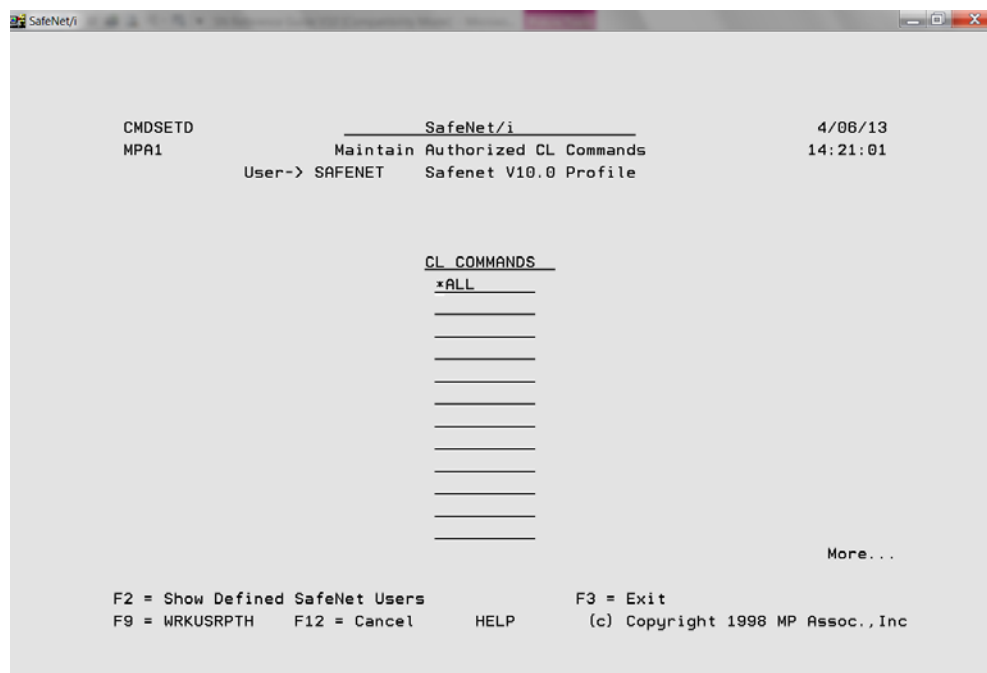
The *Work User to CL Commands, Enter User ID* screen is displayed.

3. **Type the user profile or *PUBLIC then ENTER.**

If you would like a list of all user profiles on the system, press **F4** or type ***ALL**.

To see a list of users already defined within **SafeNet/i** type ***ALLDFN**.

The *Maintain Authorized CL Commands* screen appears.



4. **Type each CL command that this user is permitted to use.**

If you want the user to have access to all CL commands, **type *ALL** in the first available space.

To remove authorization to a command, **FIELD EXIT** through the line to blank it out.

If you would like to see the list of all users who have been defined within **SafeNet/i**, press **F2**.

5. When finished typing all the required CL commands for this user, press **ENTER**.
6. **Press F9** to continue with setting up path names.

Entering Long Path Names

The default **SafeNet/i** setting is to use long path names.

If you choose to not use long path name support, you must first change the **SafeNet/i** default setting. Use the **CHGSPCSET** command to set the *PATHL* parameter to **SHORT*.

Follow these steps to authorize the user to the paths.

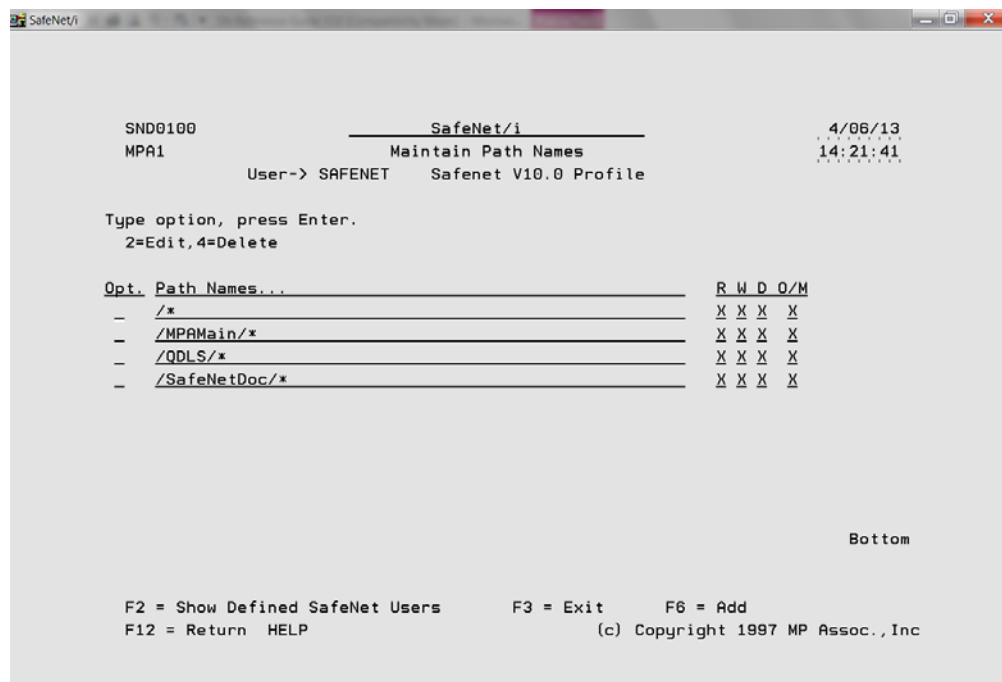
1. If you used F9 from the previous screen, continue with Step 4.
2. From the SafeNet/i User Settings Menu (SN7), select **Option 6 - Work with User to Long Path Names** or use **WRKUSRPTH** command

The *Work with User to Path Names, Enter User ID* screen is displayed.

3. **Type the user profile or *PUBLIC then ENTER.**

If you would like a list of all user profiles on the system, press **F4** or type ***ALL**.

To see a list of users already defined within **SafeNet/i** type ***ALLDFN**.



The *Maintain Path Names* screen appears.

If you would like to see the list of all users who have been defined within **SafeNet/i**, press **F2**.

4. Enter the paths that the user is authorized to.

Paths can be entered up to 512 positions in length, although only the first 60 positions are shown on the display. To enter and/or view a path over 60 positions long, **enter 2** in the option column.

Use /* to give authority to all folders/paths

End the path with * to allow access to all items in subfolders.

5. When finished typing all the paths for this user, press **ENTER**.

New in Version 9 - Building Generic Path Names for Lookups

Prior to Version 9, if you used generic path matching lookups the lookup/matching was performed as follows (*RTL):

1. Check for full path match in WRKUSRPTH
2. Remove one character at end of string, add an asterisk (*) wildcard character
3. Check for a match in WRKUSRPTH
4. Repeat 2-3 until matched, or beginning of string

Since the introduction of Version 9, you have a choice

- Use the normal Right-to-Left lookup routine (*RTL) as outlined above

OR

- Use the new Left-to-Right lookup routine. (*LTR) described below

The new *LTR routine works in this manner:

1. Check for full path match in WRKUSRPTH
2. Start building the lookup string with /a* where a = the first character of requested path
3. Check for a match in WRKUSRPTH
4. Add one more character to lookup string from requested path (/ab*)
5. Repeat 3-4 until all possibilities are exhausted

Use the CHGSPCSET command to set the *GENPTH* parameter to **LTR* or **RTL*.

Copying an Existing User to Set Up a New User in SafeNet/i

This will allow you to copy the authorities and settings from one user to another within **SafeNet/i**. The new user profile must already exist in i OS.

1. From the User Settings Menu (SN7), select **Option 10 – Copy a User Setup to Another User** or use the **CPYSNUSR** command.

The *Copy SafeNet User/Authorities* screen is displayed.

2. **Type the user profile** you are copying from, then **the new profile(s)** to add.
3. When finished entering all the new profiles, press **ENTER**.

This will set up the new profile in **SafeNet/i** and return you to the User Settings Menu (SN7).

Removing a User from SafeNet/i

This option allows you to remove a user's authorities and settings from **SafeNet/i**.

1. From the User Settings Menu (SN7), select **Option 11 – Remove a User Enrollment from SafeNet** or use the **RMVSNUSR** command

The *Remove Users from SafeNet* screen appears.

2. **Type the user profile(s)** to remove, then press **ENTER**.

This will remove the user from **SafeNet/i** and return you to the Special Jobs Menu.

Removing Unknown Users from SafeNet/i

Use the **RMVSNUSR1** command to remove user entries in SafeNet/i if the referenced user profile does NOT exist in the IBM i.

1. From the User Settings Menu (SN7), select **Option 12 – Remove Unknown Users from SafeNet** or use the **RMVSNUSR1** command

The *Remove Unknown Users SafeNet/i* is displayed.

2. **Type any user profiles that you want to OMIT** from the removal process.

This process will remove entries from the SafeNet/i control files if the user is unknown to the system and will return you to the User Settings Menu (SN7).

Removing Administrators from SafeNet/i

- From the User Settings Menu (SN7), select **Option 8 – Work with SafeNet Administrators** or use command **WRKSNADM**. Use *Option 4* to delete an Administrator.

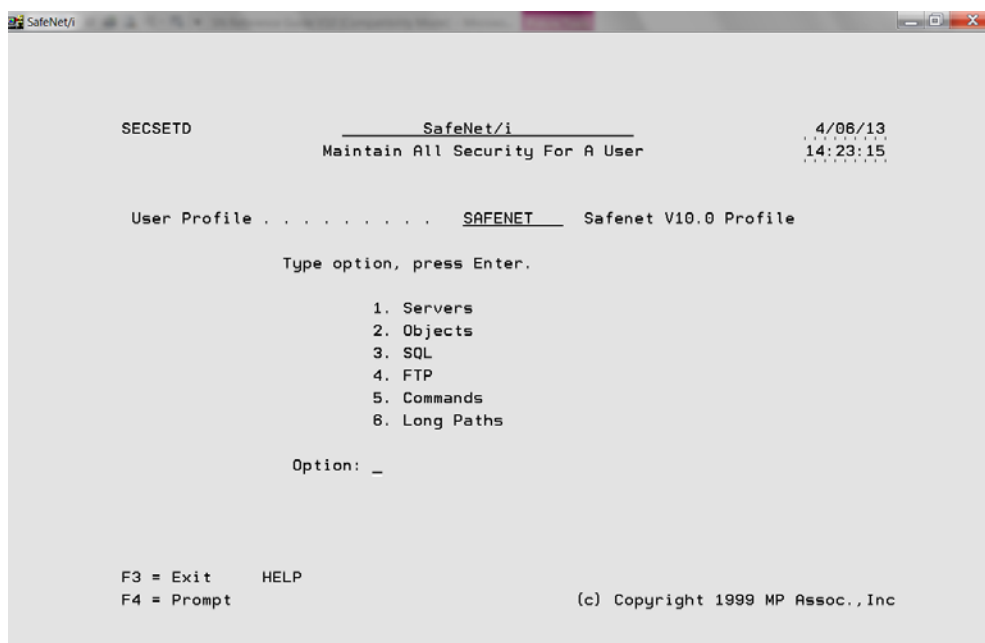
OR

- Use command **RMVSNADM**, which does not appear on any menu.

Maintain all Security for a User

The **WRKUSRSEC** command, which is not found on any of the **SafeNet/i** menus, gives you the ability to perform security maintenance for an individual user without entering several different commands.

When you use the **WRKUSRSEC** command you will be presented with the *Maintain All Security for a User* screen.



From this screen you can select which of the control files you wish to update for this particular user, without entering any additional commands or returning to the SafeNet/i Main Menu.

Within each of the applications, you can use **F9** to advance to the next maintenance screen.

Setting up Time of Day Controls

If you want to exclude users from server functions based on the day of the week or the time of day, use Time of Day controls.

SafeNet/i checks authority in the following sequence:

Is the	authorized to	at this time?
User	Specific Server *ALL Servers	
Group	Specific Server *ALL Servers	
Supplemental Group	Specific Server *ALL Servers	
*PUBLIC	*Specific Server *ALL Servers	

SafeNet/i checks until all the tests are passed or until an exclusion rule is encountered.

Note: In Version 8 and above, Time of Day controls are handled differently than in previous releases of SafeNet/i. With Version 8 and above, TOD controls are activated at the server level. Use the WRKSRV command to turn on Time of Day checking on the appropriate servers.

To set up the Time of Day controls for a specific user, use **Option 1 – Work with User to Server Security** from the SafeNet/i user Settings Menu or the **WRKUSRSRV** command.

Type the user profile, **ENTER** and then press **F10**.

The *User Time-of-Day Maintenance* screen appears.

Opt	Exit Point	Format	S S	a u ---Exclude Times---
			t n	From To From To
-	*ALL	*ALL	--	100 200
-	Distributed Data Management	*DDM	--	
-	DRDA DB2 Database Access Rqst	*DRDA	--	
-	Original Data Queue Server	DTAQ0100	--	
-	Original License Mgmt Server	LICM0100	--	200 300
-	Original Message Server	MESS0100	--	
-	Network Print Server - entry	ENTR0100	--	
-	Network Print Server - spool file	SPLF0100	--	
-	File Server	PWFS0100	--	
-	Original Remote SQL Server	RSQL0100	--	
-	Spooled File Security	SPSY0100	--	
-	Original File Transfer Function	TRAN0100	--	
-	Telnet Device Initialization	INIT0100	--	
-	FTP Client Request Validation	VLRQ0101	--	
-	FTP Server Request Validation	VLRQ0100	--	

F9=Update Holidays
F3=Exit F5=Refresh

To exclude the user from all servers during the same days of the week and time of day, **type 2 – Change** in front of ***ALL**.

To select individual servers, type 2 in front of the servers you want to change

```

UPDATE                               User Time-of-Day Maintenance           KTODM1
User: SAFENET      Safenet V10.0 Profile

Exit Point . . . . . Original License Mgmt Server
Format . . . . . *ALL

Time Of Day Exclude Ranges:
Range 1: From 100 To 200 Access between the given time range will
Range 2: From      To      be denied by SafeNet/i.
Range 3: From      To     

Day Of The Week Exclusions:
Saturday   X   X=Exclusion is set
Sunday     -   Blank=Exclusion is off
Monday     -
Tuesday    -   Access on the indicated days
Wednesday  -   will be denied by SafeNet/i.
Thursday   -
Friday     -
Holidays   -

F5=Refresh      F12=Cancel      F9=Update Holidays

```

You can define up to three time ranges and can select which days to exclude by typing **X** in front of the day.

You can also define holidays that will be used to control Time of Day access.

Press F9 to display the *Time of Day Holiday Maintenance* screen.

Date	Description	Date	Description
01/01/13	New Years		
03/01/13	March first		
04/01/13	April First		
07/04/13	4th of July		

F3=End w/update F12=Cancel

Type the dates and descriptions of your holidays.

Press **ENTER**.

Chapter 2 - SETTING UP SERVERS

The final step in configuring **SafeNet/i** is to enter the Security Level settings for all the server functions.

Important: If you do this step first and restrict access to the server functions prior to setting up user rights, you may disrupt network requests until the users' authority table setup is completed. Setting up the Current Level on the servers should be considered the **LAST STEP** during the setup process.

Typically, use the Future Server Settings for initial setup and testing. When you are ready to activate SafeNet/i settings, you can flip the current and future settings by using **Option 1 - Work with User to Server Security** on the SafeNet/i Main Menu (SN1) then F22.

You can also use the **WRKSRV** command and F22.

SafeNet/i Server Function Security Levels

Level 1:

- IBM default
- Unlimited access, all requests accepted
- Requests can be logged, reporting available
- Performance impact - none

Level 2:

- No access at all, all requests for server are rejected
- Requests can be logged, reporting available
- Performance impact - not a consideration

Level 3:

- Access granted on a user-by-user basis to the server
- Requests can be logged, reporting available
- Performance impact – minimal
- TELNET requires use of the TCP/IP control table

Level 4:

- Access granted on a user to server and object and command basis
- Requests can be logged, reporting available
- Performance impact – higher

Level 4 requires authority to the server function and additionally requires table entries for proper authorization to individual or generic objects and/or folders by user profile. Data rights such as read/write and object management rights can be assigned on an individual basis.

Level 4 on the *DDM*, *FTP* or *Remote Command/Program Call Server* requires setting up authorities to CL commands.

For *DDM*, *FTP* or *Remote Command/Program Call Server*, all commands are restricted.

Level 5:

- This usually denotes a problem with an exit point program registration in IBM i
- This indicates that **SafeNet/i** does not recognize a program assigned to the exit point or has detected a user-defined program assigned. (Use WRKREGINF command to review existing exit point programs.)
- Not supported
- Cannot be changed via **SafeNet/i**, use WRKREGINF command
- See Appendix A, 'Special Technical Considerations'

On the following pages you will find these levels grouped together to make it easier for you to decide the appropriate level of security required for each server function.

Setting the Server Function Logging Levels

The valid logging levels are:

Logging Level A	Log all transactions
Logging Level R	Log only rejected requests
Logging Level N	No logging

As you set up your Server Function logging levels, please remember the following:

- If you set the logging level on the Server Function to *NO LOGGING* or *REJECTIONS*, the Server Function setting will override the individual user logging level.
- If you set the logging level on the Server Function to *ALL*, the individual user logging level will override the Server Function logging level.

To make sure you are logging transactions correctly, we recommend that when you initially set up **SafeNet/i** you set the Server Functions to log *ALL* and set the individual user logging levels to either *ALL* or *REJECTIONS*.

Then, after you have had some experience with checking the logs and interpreting the results, you may want to make changes for specific user and server combinations.

Basic Server Security - Supported by all Servers – Rating LOW

Level 1 - IBM Default

Level 2 - No access to server

Intermediate Server Security - Supported by all Servers - Rating MEDIUM

Level 3 - Users must be authorized to the server

Special
Level 3 - *TELNET - controls signon by IP address

Advanced Server Security - Supported by Specific Servers - Rating HIGH

Level 4 - The user must be authorized to the server, the objects requested, the FTP Op or SQL Op, CL commands or long path to be used.

Supported by the following servers:

- Distributed Data Management Server
- Original Data Queue Server
- Network Printer Server - Spool file requests
- Integrated File Server
- Original Remote SQL Server
- Original File Transfer Function Server
- Original Virtual Print Server
- Database Server - Data base access
- Database Server - SQL access
- Data Queue Server
- Remote Command/Program Call Server
- FTP Server Request Validation
- FTP Client Request Validation
- REXEC Server request Validation
- Showcase™ Server
- Spooled File Security

Recommended Server Settings

<u>Server Description</u>	<u>Recommended Setting</u>
Central Server - client management	Level 1, Log None
Central Server - conversion map	Level 1, Log None
Central Server - license management	Level 1, Log None
Database Server - entry	Level 3, Log All- Limit user access
Database Server - data base access - 100	Level 4, Log All - Limit user and object access
Database Server - data base access - 200	Level 4, Log All - Limit user and object access
Database Server - object information - 100	Level 3, Log All - Limit user access
Database Server - object information - 200	Level 3, Log All - Limit user access
Database Server - SQL access - 100	Level 4, Log All - Limit user, object and SQL statement access
Database Server - SQL access – 200	Level 4, Log All - Limit user, object and SQL statement access
Data Queue Server	Level 1, Log None

<u>Server Description</u>	<u>Recommended Setting</u>
Distributed Data Management	Level 3, Log All - Limit user access or Level 4, Log All - Limit users to specific objects and commands
DHCP	Level 1, Log None
DRDA DB2 Database Access Request	Level 3, Log All - Limit user
File Server	Level 4, Log All - Limit user and object access
FTP Client Server	Level 4, Log All - Limit user access & target connection by IP Address
FTP Logon Server	Level 3, Log All - Limit user access
FTP Server Validation	Level 4, Log All - Limit user, source IP address, object, FTP sub-commands
Network Print Server - entry	Level 1, Log None
Network Print Server - spool file	Level 1, Log None
Original Data Queue Server	Level 1, Log None
Original File Transfer Function	Level 4, Log All - Limit user and object access
Original License Mgmt Server	Level 1, Log None

<u>Server Description</u>	<u>Recommended Setting</u>
Original Message Server	Level 1, Log None
Original Remote SQL Server	Level 4, Log All - Limit user access to objects and SQL statements
Original Virtual Print Server	Level 1, Log None
PWRDWN SYS	Level 1, Log All – Log all requests
Remote Command/Program Call	Level 4, Log All - Limit user and object access and commands
REXEC Logon	Level 3, Log All - Limit user access
REXEC Server Request Validation	Level 4, Log All - Limit user, Source IP address
Spooled File Security	Level 1, Log None - Unless specific requirement for additional spool security
TELNET Logon or TELNET Logoff	Level 1, Log None
TFTP Logon	Level 1, Log None
User Profile Points	Level 1, Log All - Log all requests
TCP Signon Server	Level 1, Log None
Showcase™ Server	Level 4, Log All – Limit User, Object, Log all

Entering Server Function Security Levels

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

The *Maintain Server Security* screen is displayed.

```

SafeNet/i
-----
WRKREG2R                      SafeNet/i  V10                      4/06/13
MPA1                          Maintain Server Security          14:31:11

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:
A=Log All  N=No Logging  R=Log Rejected

TOD=Time of Day Checking:
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. Enter the level of security and the logging level that is required for each server description in the *Current* columns.

The *Future* column lets you enter a setting for each server based on what you think the setting will be in the future. This makes it possible to use your historical transactions against both current and future server levels for testing purposes.

When you change the TOD value it becomes effective immediately. Make sure you have used the *Time of Day* setup function, accessed via F10 within the **WRKUSRSRV** command, before you change this value on the server function.

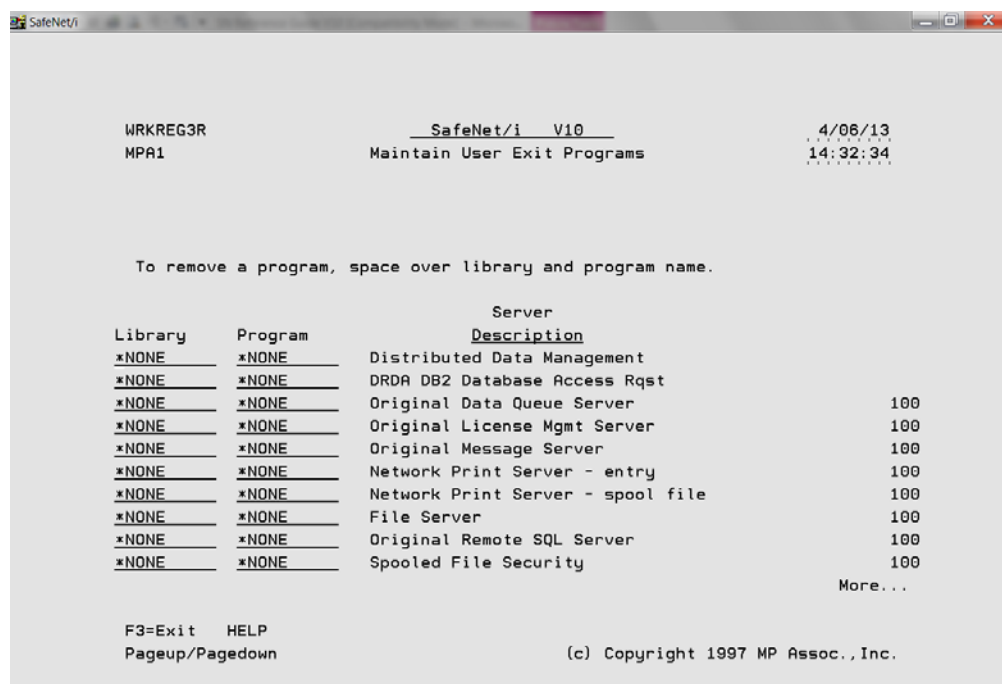
Note: The server functions are listed on multiple screens. **PageDown** to ensure you enter a level for all the servers.

3. When you have finished entering information for all the servers, **press ENTER**.

The screen is refreshed and any changes you made are reflected in the *Current* columns.

Customer Exit Programs

If you would like to use your own programs over these server exit points, **F18** on the *Maintain Server Security* screen gives you the ability to do so.



SafeNet/i will look to see if there is a customer-written program to call. If there is, it calls the program, passing two parameters, a one-byte status code, plus the rest of the data string from the client. The customer exit program is always processed **BEFORE** the **SafeNet/i** checks are done.

Your custom exit program can do whatever you want. When it returns to **SafeNet/i**, if the status code has been changed to indicate any type of rejection, **SafeNet/i** stops and logs the request, and returns a rejection to the client.

If the exit program does not change the status code, the request will go through the normal **SafeNet/i** checking process.

The string that is passed is limited to 4,000 characters, as defined by IBM. Examples of these strings can be found in the TRAPOD file and the appropriate IBM manuals.

Chapter 3 - TELNET, TCP/IP ADDRESS CONTROLS

Setting up TELNET

TELNET control features are supported only when the server is set to Level 3. You may use some or all of the features available with the TELNET server point:

- Control access by IP address
- Allow auto sign-on (bypass sign-on)
- Restrict IP address to use specific device names (enhanced TELNET clients only)
- Restrict access based on the password type sent (none, clear or encrypted)

Controlling TELNET Access by IP Address or Restricting Device Naming in TELNET

1. Set the TELNET server to Level 3 using the **WRKSRV** command.
2. From the SafeNet/i Main Menu (SN1), select **Option 5 – Work with TCP/IP Address Security** or use the **WRKTCPIPA** command and enter ***TELNET** as the server to control
3. **Enter the IP address** in dotted decimal format (i.e., 10.2.2.2)

Use wild card options if desired (10.2.2.x)
4. **Enter A or R** to accept or reject the request
5. To restrict access to specific device names **enter the device name** in the *Device Name* field with its corresponding IP address.

You may also use a generic device name by putting an * at the end of the name. If you use a generic name, up to 99 will be used.

For example:

An entry of AP* would allow devices to be used as AP01 through AP99. The login process through TELNET will select the next available device name.

Setting the Required Password Type

This field must be set if the *TELNET Server* is set to Level 3. You must enter the appropriate setting for ALL TELNET IP address controls. As of OS/400 V4R2, only a setting of 0 or 1 is available. A setting of 2, although allowed here for encrypted passwords, is only available in V5R1 of OS/400.

Valid settings are:

- 0** – No password was received or validated
 - 1** – A clear text password was received and validated
 - 2** – An encrypted password was received (SSL TELNET only in V5R1)
-
- For normal TN5250 (TELNET support is VT100) you must set this to 0, since non-enhanced TELNET clients do not support this feature.
 - For IBM i Access for Windows TELNET, you can use a setting of 1. However, certain IBM i Access for Windows clients do not support this, so you **MUST** test this at your location.
 - A setting of 0 will always allow the client to connect.

Kerberos

For use with additional external Kerberos authentication you must also use the CHGTELNET command to modify the parameter value *KERBEROS* (**YES*) or (**NO*).

The CHGTELNET command is not found on any SafeNet/i menu; you must execute it from the command line.

1. Type **CHGTELNET** and prompt with **F4**
2. Change *KERBEROS* to **YES* or **NO*

Single Sign-on

This feature will let you implement Kerberos single sign-on through SafeNet/i without having to use the SafeNet/i automatic sign-on feature. This can be helpful if you do not have static IP addresses assigned to local workstations and are implementing Kerberos.

If your Telnet exit point in SafeNet/i is set to level 1, then Kerberos single sign-on will work as is and you can stop here.

To enable the function:

1. Disable the SafeNet/i automatic sign-on option.

If you have not enabled it yet, you can bypass this step.

2. To enable the Kerberos feature, run this command from the command line:

CHGTELNET and prompt with **F4**

Change *KERBEROS* to **YES*

At this point, the SafeNet/i automatic sign-on feature will not work and the data stream necessary for Kerberos single sign-on will work correctly.

If you want to revert back to the way this was set prior to the change, run this command:

CHGTELNET and prompt with **F4**

Change *KERBEROS* to **NO*

Allow Auto Sign-on

1. Use the **WRKSRV** command to set the TELNET server to Level 3
2. Use the **WRKTCPIPA *TELNET** command **to enter the IP address** allowed for auto sign-on
3. **Enter the password type** (0 or 1 is required)
4. **Enter a Y** to allow auto sign-on
5. Use the **WRKSIGNON** command to **enter the IP address, the user profile, library, program or menu** that the client will automatically be signed on to.

For IBM i Access for Windows, you must set the TN5250 session parameters on the client setup to bypass sign-on (see the IBM i Access documentation). This is required if you set the password type to 1 in the WRKTCPIPA setting.

For non-IBM i Access clients (named TELNET VT100 clients) you cannot use a password type of 1, only 0 is supported.

Important: If you intend to allow auto sign-on, please test this thoroughly, since it could present a security exposure.

Logging of TELNET Sessions

Under normal sign-on conditions (no auto sign-on allowed), each request for a TELNET session is logged into the transaction history file (TRAPOD) by IP address, and a user name of QSYS. QSYS is used because no user profile is associated with the actual TELNET session start request. Each logoff is also recorded by IP address with a user of QSYS.

If you use the auto sign-on feature, the request will be logged with the associated user set up in the Auto Sign-on Control file. Each logoff of a TELNET will also record the transaction with the user profile that was automatically signed on.

Setting up TCP/IP Address Controls

SafeNet/i allows you to specify which client IP addresses are either accepted or rejected by the *Telnet* and the *FTP Servers*.

Turning on TCP/IP Address Checking

To set-up and turn on TCP/IP address checking for the **FTP Server** and **Rexec Server**

1. Type **WRKTCPIPA *FTPSEVER** then **ENTER** (Menu SN1, *Option 5*)
2. Add the IP addresses to the Control Table
3. Type **CHGFTPSET** then press **F4**
4. Change *Server Source limit by IP Address?* to **YES* then **ENTER**
5. Use **WRKSRV** command and set the **FTPSEVER* and/or **REXEC* Server exit point to level 3 or 4.

To set-up and turn on TCP/IP address checking for the **FTP Client**:

1. Type **WRKTCPIPA *FTPCLIENT** then **ENTER** (Menu SN1, *Option 5*)
2. Add the IP addresses to the Control Table
3. Type **CHGFTPSET** then press **F4**
4. Change *Client Target limit by IP Address?* to **YES* then **ENTER**
5. Use **WRKSRV** command and set the **FTPCLIENT* exit point to level 3 or 4.

To set-up and turn on TCP/IP address checking for **TELNET**:

1. Type **WRKTCPIPA *TELNET** then **ENTER** (Menu SN1, *Option 5*)
2. Add the IP addresses to the Control Table
3. Type **WRKSRV**
4. Change the **TELNETON* point to Level 3

Setting up TCP/IP Address Control Table

1. Use SafeNet/i Main Menu (SN1), **Option 5 – TCP/IP Address Control Settings** or the **WRKTCPIPA** command
2. In *IP Addresses for Server* enter ***FTPSERVER**, ***FTPCLIENT** or ***TELNET** for the proper control table.
3. **Type the addresses to accept or reject.** **A** indicates Accept; **R** indicates Reject.

Example 1:

Address	Accept/ Reject
10.2.2.X	A
10.2.2.5	R

In this example any address from 10.2.2.1 through 10.2.2.255 will be accepted, with the exception of 10.2.2.5, which will be rejected.

Example 2:

Address	Accept/ Reject
10.2.2.1XX	A
10.2.2.14X	R

In this example all clients with addresses from 10.2.2.100 through 199 will be accepted, with the exception of clients addressed 10.2.2.140 through 10.2.2.149, which will be rejected.

To print the control table, select **Option 10 - Print TCP/IP Address Control Listing** on the SafeNet/i Reports Menu, (SN3).

Chapter 4 - SETTING UP FTP

Setting up for Normal User IDs and FTP Servers

Example

1. From the SafeNet/i Main Menu (SN1), select **Option 4 – Additional FTP Settings** or use **CHGFTPSET** command
2. On the Change SafeNet FTP Settings screen, set *Allow normal user IDs to log on the FTP* to ***YES** or use **RLOGON (*YES)** parameter
3. Return to the SafeNet/i Main Menu (SN1) and Select **Option 1 - Server Security Settings** or use **WRKSRV** command

Locate the *FTP Logon*, *FTP Client* and/or *FTP Server* points. These must be set to Level 1, 3, or 4. (If you set these to Level 1, you can skip the rest of these steps.)

4. From the User Settings Menu (SN7), select the following options:
 - a. **Option 1 - Work with User to Server Security** or use **WRKUSRSRV** command

The user ID must be authorized to the *FTP Logon server* and one of the following:

*FTP Client – if an IBM i user will be FTP-ing OUT from your IBM i

*FTP Server – if an IBM i user will be FTP-ing INTO your IBM i

- b. **Option 2 - Work with User to Object Level Security** or use **WRKUSROBJ** command

Authorize the user ID to their own current library as specified in the i OS user profile. Enter this library in *User to Object Security*

Authorize the user ID to any other library or object. Enter these in *User to Object Security*

- c. **Option 4 - Work with User to FTP Statement Security** or use **WRKUSRFTP** command

Authorize the user ID to the FTP statements they will use. Use **F4** for additional user settings if required.

- d. **Option 5 - Work with User to CL Command Security**

Authorize the user to the CL commands they will issue through the *FTP Server*

Set the parameters for **CHGFTPSET** command as follows. The default value is highlighted in **bold**.

Parameter	Screen Selections	Value	Description
RLOGON	Allow Normal USERID FTP Logon	*YES *NO	<p>This parameter is used to determine whether or not you want regular IBM i user IDs to be able to sign on through the FTP server. If you want only anonymous logons, set this to *NO and FTP for anonymous logons to *YES.</p> <p>If you say *NO to this option (allow normal IBM i user profiles to log on) then only anonymous logons will be allowed/disallowed based on the other parameters. Regular IBM i user IDs will not be accepted for FTP logons.</p>
IPCTL	Server Source limit by IP Add?	*YES *NO	<p>To validate source IP addresses against a SafeNet/i control table. Use WRKTCPIPA *FTPSERVER</p>
IPCTL	Client Target limit by IP Add?	*YES *NO	<p>To validate Target IP addresses against a SafeNet/i control table. Use WRKTCPIPA *FTPCLIENT</p>
ALOGON	Allow Anonymous FTP Logon	*YES *NO	<p>If you want users to be able to login with the user ID of Anonymous, enter *YES. If you don't want a user to use the FTP Logon User as Anonymous, leave this field *NO.</p>
ALIBR	Anonymous User Library	<i>Libname</i>	<p>When you allow anonymous logons, you must restrict those FTP users to a specific library. For security purposes, enter it here <u>AND</u> grant the user profile for anonymous logons object rights to this library or group of objects within this library from the <u>SafeNet/i Main Menu, Option 3</u>. For the ANONYMOUS user profile under IBM i, make the 'Current Library' this library name.</p> <p>Also grant the anonymous user ID authority to the FTP server on the <u>Main Menu, Option 2</u>. Add the user to the valid FTP statements from the <u>Main Menu, Option 5</u>.</p>

GUEST	Allow Anonymous GUEST Password	*YES *NO	<p>To allow Anonymous user logins with the password of GUEST, enter *YES here. You can choose GUEST or use an e-mail address.</p> <p><i>Note:</i> If you select GUEST, the IBM i still prompts an anonymous user for their e-mail address. SafeNet/i, however, will only allow GUEST as the password.</p>
EMAIL	Allow E-mail Address for Password	*YES *NO	<p>If you allow an anonymous user to accept an e-mail address, SafeNet/i will scan the address entered for an embedded “@” (at sign) for validation, and record the address in the log request file for reporting</p>
AUSRPRF	Profile for Anonymous Logons	<i>profilename</i>	<p>If you allow anonymous logons, you must specify a <u>valid, pre-existing</u> user profile to run anonymous user logons in IBM i when the anonymous user logs on under FTP. In other words, a user would FTP to an IBM i FTP site running SafeNet/i, and that FTP site would prompt for a user name. The user keys ‘ANONYMOUS’ and the IBM i prompts for a password. The user then keys in a valid e-mail address and the IBM i starts a job assigned to the user ID you have specified here. The IBM i job is initiated using this profile and all its associated authorities.</p> <p>Enter the ANONYMOUS profile here, and if you want to assign a password to the profile enter that here also. It is highly recommended that you leave this as *NONE, *NONE. If you enter a password here, or use a profile other than ANONYMOUS, you leave a potential security exposure.</p> <p>Important: When using SafeNet/i and allowing for Anonymous, it is strongly recommended that you create an IBM i user profile called ‘ANONYMOUS’ with a password of *NONE and *USER for the profile type. If you do this, no one can use</p>

			this profile to sign on since the password is set to *NONE.
APWD	Password for Above Profile	<i>pwd</i>	Enter the password to be used with the profile in parameter AUSRPRF for Anonymous FTP.

Anonymous FTP Logon

To set up for Anonymous Logon, you must fill in the special FTP settings, and set the *FTP Logon Server* to Level 3 and the *FTP Server Validation* to Level 4.

Follow these steps for FTP:

1. From the SafeNet/i Main Menu (SN1) select **Option 4 – Additional FTP Settings** or use **CHGFTPSET** command along with **F4**

The *Change SafeNet FTP Settings* screen is displayed.

Press F9 to see all parameters.

Change SafeNet FTP Settings (CHGFTPSET)

Type choices, press Enter.

Allow Normal USERID FTP Logon.	<u>*YES</u>	*YES, *NO
Server Source limit by IP Add?	<u>*NO</u>	*YES, *NO
Client Target limit by IP Add?	<u>*NO</u>	*YES, *NO
Allow ANONYMOUS FTP Logon. . .	<u>*NO</u>	*YES, *NO
ANONYMOUS User Library	<u>ANONFTP</u>	Name
Allow Anonymous GUEST Pswd . .	<u>*YES</u>	*YES, *NO
Allow E-Mail Address for Pswd.	<u>*YES</u>	*YES, *NO
Profile For ANONYMOUS Logons .	<u>ANONYMOUS</u>	Name
Password for Above Profile . .	<u>*SAME</u>	Name, *SAME

Bottom

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

Here you will find the special parameters to control login access to the *FTP Servers* from both Anonymous and regular user IDs.

Setting up for ANONYMOUS FTP

Example

1. Create a user profile on the IBM i called ANONYMOUS, with password *NONE and user class *USER, and set the Current Library.
2. From the SafeNet/i Main Menu (SN1), select **Option 4 – Additional FTP Settings** or use **CHGFTPSET** command along with **F4**
3. Set the parameters as follows:
 - If you want to allow IBM i users other than ANONYMOUS to log in through FTP server set parameter **RLOGON** to ***YES**
 - Enter **ALOGON(*YES)** to allow ANONYMOUS
 - Enter **the library name** to which the user is restricted in parameter **ALIBR**
 - Enter **the type of password** you want the user to enter - e-mail or Guest, or both
 - Enter **the IBM i user profile** in parameter **AUSRPRF** that was created in Step 1 above (ANONYMOUS)
 - Enter password for the ANONYMOUS user profile in **APWD** parameter
4. Press **ENTER**
5. Return to the SafeNet/i Main Menu
6. Select **Option 1 - Server Security Settings** or use **WRKSRV** command
7. Locate the *FTP Logon Server* point
8. Change the *FTP Logon Server* to Level 3
9. Change the *FTP Server Validation* point to Level 4. If you want to allow for anonymous logons, you **MUST** set this to Level 4
10. From the SafeNet/i User Settings Menu (SN7), select **Option 1 -Work with User to Server Security** or use **WRKUSRSRV** command
11. Grant the ANONYMOUS user profile authority to the *FTP Logon* and *FTP Server Request Validation* server points.
12. From the SafeNet/i User Settings Menu (SN7), select **Option 2 - Work with User to Object Level Security** or use **WRKUSROBJ** command
13. Grant the ANONYMOUS user authority to the library entered in step 3 above (Current Library), and specifically to any objects within the library. Or, enter *ALL for all object and then assign the required data rights.

If using long path support, use the **WRKUSRPTH** command to enter the correct path or paths for ANONYMOUS.

14. From the User Settings Menu (SN7), select **Option 4 - Work with User to FTP Statement Security** or use the **WRKUSRFTP** command to grant the ANONYMOUS user ID authority to specific FTP commands. Use the additional FTP settings if required or if you want the ANONYMOUS profile initial path to be an IFS directory.

Object Level Security for FTP Client Sessions

To implement this function, set the *FTP Client Request Validation Server Function* to Level 4 in SafeNet/i.

When setting up object level security for the *FTP Client Request Validation Server*, remember that the data roles are reversed from *FTP Server Request Validation Function*.

For example, a PUT from the FTP Client requires READ authority to the object; a GET requires both WRITE and OBJ MGMT authority to the object.

IP Address Checking for FTP Client Sessions

When the *FTP Client Request Validation Server Function* is set to Level 3 or Level 4, you can control which IP addresses the FTP Client users are permitted to connect to.

Chapter 5 - REPORTS

SafeNet/i reports are grouped into the following categories:

- **Setup Reports** provide information on server settings, user authorities to servers and to data, etc.
- **Analysis Reports** provide data on **SafeNet/i** usage – the who, what, where and when information you need to manage your system.

Analysis reports have been enhanced to include the ability to select specific dates and/or users, including summaries by group profile. You can choose to print the reports or create an OUTFILE of the selected records in a readable format to use for your own ad-hoc reporting.

You can also use the analysis reports to take advantage of the Auto-enrollment feature of **SafeNet/i**. See the [SafeNet/i Implementation Guide](#) for more information.

- **Journal Reports** provide additional auditing and controls if you have enabled the Journaling feature in **SafeNet/i**. See Chapter 8 in this guide for details on journaling.

Setup Reports

These reports are accessed through the SafeNet/i Reports Menu (SN3).

Each of these reports can be generated for a selected user or for *ALL users.

- | | |
|--|-------------------|
| 1. Server Status | PRTSRVSTS |
| Prints each Server Function and its security level setting | |
| 2. User to Server Security Listing | PRTUSRSRV |
| Lists users and the Server Functions they are authorized to | |
| 3. User to Object Security Listing | PRTUSROBJS |
| Lists users, the libraries and objects they have authority to and the rights the users have to the objects | |
| 4. User to SQL Statement Listing | PRTUSRSQL |
| Lists all users and the SQL statements they are authorized to use | |
| 5. User to FTP Statement Listing | PRTUSRFTP |
| Lists all users and the FTP statements they are authorized to use | |
| 6. User to CL Command Listing | PRTUSRCMD |
| Lists users and the CL commands they are authorized to use | |
| 7. User to Long Path Security Listing | PRTUSRPTH |
| Lists users and long path names they are authorized to use | |
| 8. Print all the User Setup Reports | PRTUSRALL |
| Prints ALL the setup reports for a user | |
| 9. Print Swap Profiles | PRTSWPPRF |
| Prints a list of all swapped profiles | |

- | | | |
|------------|---|------------------|
| 10. | TCP/IP Address Control Listing | PRTTCPIPA |
| | Lists the TCP/IP address controls for FTP servers –
*FTPSERVER, *FTPCLIENT and *TELNET | |
| 11. | Print Admins | PRTSNADM |
| | Lists all of the SafeNet/i administrators | |
| 12. | Print Super Users | PRTSNSUSR |
| | Lists all of the SafeNet/i super users | |

Usage Reports

These reports are accessed through the Network Transaction Analysis Reports Menu (SN4).

Options 2 through 7 on this menu also give you the ability to run auto-enrollment reports and perform the auto-enrollment process.

- | | | |
|-----------|---|------------------|
| 1. | Security Report by User
(Also Batch Transaction Test Report) | PRTSECRT |
| | <p>Lists each request by user, the Server Functions they are requesting, the server's security level setting, and whether the request was accepted or rejected.</p> <p>Can also be used as a test report to recheck all historical transactions against current and future SafeNet/i settings.</p> <p>Allows "what if" testing of all historical transactions against current and future control file settings to see if further set up is required.</p> | |
| 2. | User to Server Usage Report | PRTSRVUSG |
| | <p>Using historical transactions, lists each server a user has accessed</p> | |
| 3. | User to Object Usage Report | PRTOBJUSG |
| | <p>Using historical transactions, lists each LIB/OBJ a user has accessed and the type of access, i.e., READ, WRITE, DELETE.</p> | |
| 4. | User to SQL Usage Report | PRTSQLUSG |
| | <p>From historical transactions, lists each SQL operation performed by each user.</p> | |
| 5. | User to FTP Usage Report | PRTFTPUSG |
| | <p>From historical transactions, lists each FTP operation performed by each user.</p> | |
| 6. | User to CL Command Usage Report | PRTCLUSG |
| | <p>Using historical transactions, lists each CL command issued by each user.</p> | |

7. User to IFS Path Usage Report

PRTPTHUSG

Using historical transactions, lists each path accessed by each user.

10. Print Executive Summary

SNEXESUM

Provides a report, either detailed or summary, containing the current status and statistics of SafeNet/i on your system.

Run Security Report by User from Archive

You can run this report using data that has been purged from the transaction history file and has been archived to a member of file TRAPARCW in library PCSCDTA or from a converted transaction journal receiver placed into the TRAPARW file. .

TRAPARCW is a multiple member file where member names are based on the date when the purge was run and records were written to the archive. In order to run the report from the archived data, you will need to know which member name to use.

For example, a member named 'A20090117' contains archive records from the purge that was run on January 17, 2009.

Run the *Print Security Report by User* from the Network Transaction Analysis Reports Menu (SN4), **Option 1** or use the **PRTSECRTP** command.

Page down to the second screen to locate the *Print from Archive Member* parameter.

Print Security Report (PRTSECRPT)

Type choices, press Enter.

Outfile Name for Report *NONE Name, *NONE
Library. Name,
Print Empty/Blank Reports? . . . *YES *YES, *NO

Additional Parameters

Print from Archive Member? . . . *NO *NO OR Member Name

Bottom

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

Enter the **member name** containing the archive data you want to include in the report.

On the first screen of the PRTSECRPT command, you can enter the *Selection from Date* and/or the *Selection to Date*. If you use an archive member, you can leave the default date range selection as *BEGIN *END and specify the archive member. That will print everything in the member.

To report on a sub-set of what's in the member, you can specify a *FROM* date and a *TO* date in addition to the member name. If you do this, make sure your date selection range includes the dates in the member, or you will not get any results.

Note: You can also use this option to print a report from Converted Transaction Journal entries. You must first use the CVTTRNJRN command and copy the result data set from the command run to a new archive member. See CVTTRNJRN command in *Chapter 7* of this guide.

Chapter 6 - TESTING YOUR SECURITY SETTINGS

Once you have planned your server function Security Level settings, **SafeNet/i** gives you a method to test the settings to make sure they will provide the level of security you anticipate. It acts as a “what-if” tool to verify the effect your settings will have before you actually turn on access control.

If you have been logging network requests with **SafeNet/i** you can, at any time, run each historical record through the security checking routines and receive a result of ‘ACCEPTED’ or ‘REJECTED’ based on current or future **SafeNet/i** settings.

This allows you to make changes to the server function Security Level, the user-to-server settings, or data rights authorities, and using previously logged requests, tell immediately if your settings will give the desired response to the clients.

To test your collected transactions use one or both of the following, found on Special Jobs Menu (SN2):

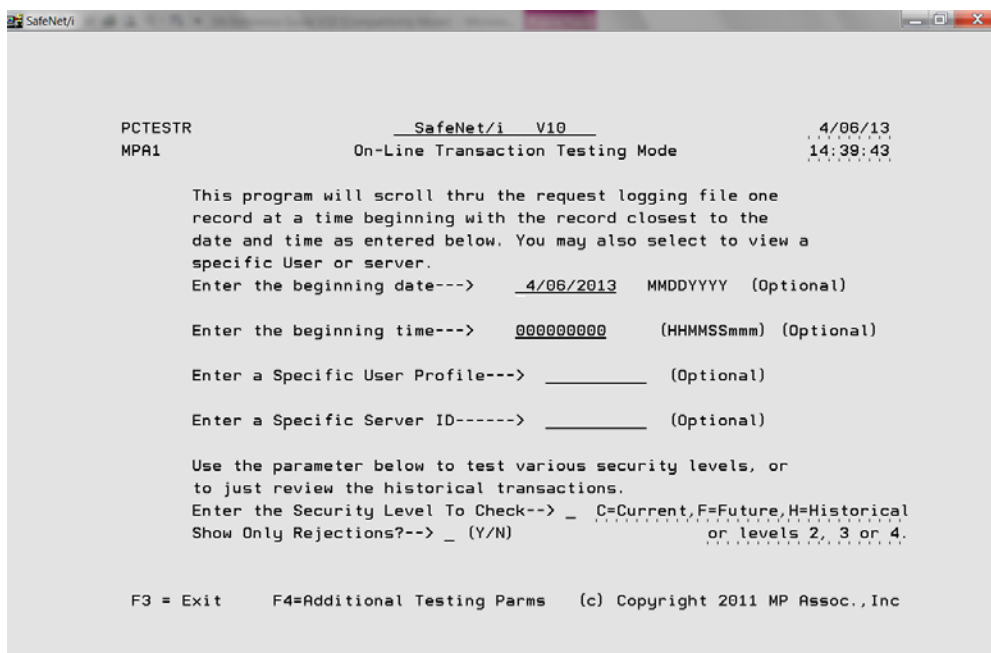
- **Option 4** - *On-line Transaction Testing* (PCTESTR) – the preferred method
- **Option 2** – *Print Transaction Security Report* in test mode

Testing SafeNet/i settings based on your historical data with the on-line transaction tester

This is the preferred method if you would like immediate feedback.

1. From the SafeNet/i Main Menu (SN1) select **Option 22 - Special Jobs Menu** (SN2)
2. Select **Option 4 - On-Line Transaction Testing** or use **PCTESTR** command

The *On-Line Transaction Testing* screen will appear.



The screenshot shows a terminal window titled "SafeNet/i". The screen displays the following text:

```
PCTESTR                               SafeNet/i  V10                               4/06/13
MPA1                                  On-Line Transaction Testing Mode          14:39:43

This program will scroll thru the request logging file one
record at a time beginning with the record closest to the
date and time as entered below. You may also select to view a
specific User or server.
Enter the beginning date--->  4/06/2013  MMDDYYYY  (Optional)

Enter the beginning time--->  0000000000  (HHMMSSmm) (Optional)

Enter a Specific User Profile--->          (Optional)

Enter a Specific Server ID----->         (Optional)

Use the parameter below to test various security levels, or
to just review the historical transactions.
Enter the Security Level To Check--> _  C=Current,F=Future,H=Historical
Show Only Rejections?--> _  (Y/N)                               or levels 2, 3 or 4.

F3 = Exit      F4=Additional Testing Parms  (c) Copyright 2011 MP Assoc., Inc
```

If you want, you may enter a beginning date and time, or the user or server ID, then enter the desired security level to test against your logged transactions.

If you do not enter a date and time, you will be shown requests beginning with the first available record in the file.

3. In the *Security Levels to Check* field:

Type C (Current) to test transactions with your **present SafeNet/i** Server Security Levels

Type H (Historical) to review the actual status received when the transaction was logged; no new 're-testing' is performed.

Type F (Future) to test transactions with your **future** Server Security Levels. This will test each selected transaction against the future security setting to determine if your security control files are set up correctly.

Type 2, 3 or 4 for other levels

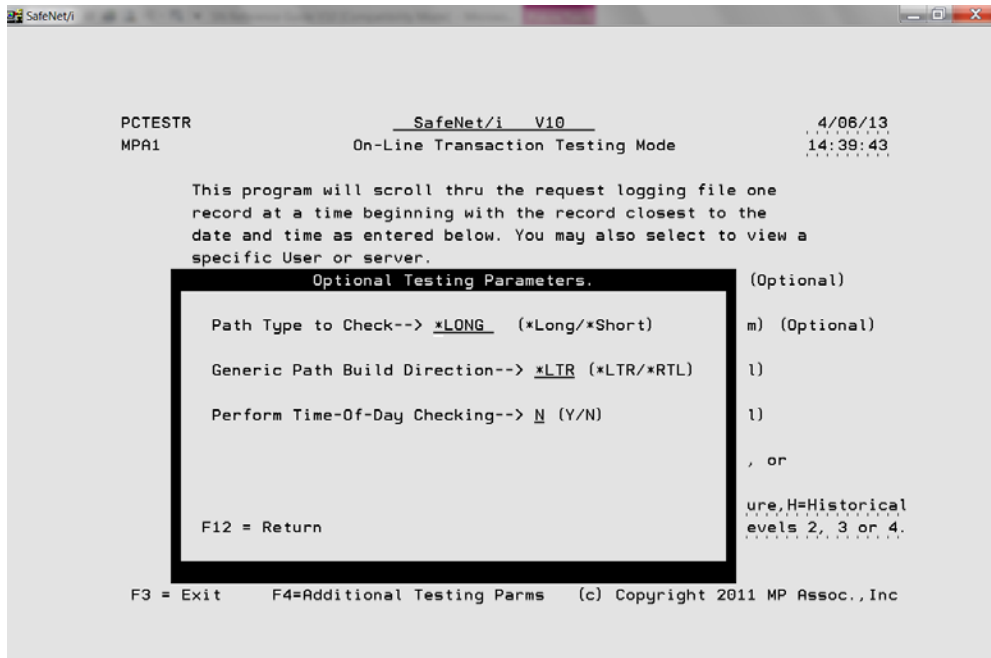
If you want to test your Time-of-Day controls, **type Y** in Time of Day Check.

If you want to see only rejected requests, **type Y** in *Show only Rejections*.

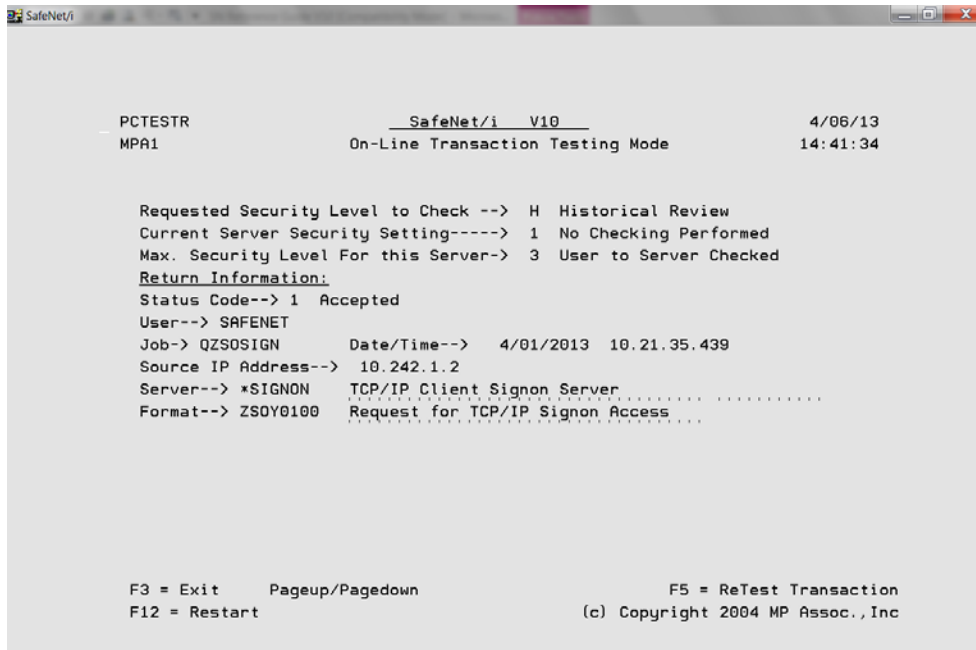
Important: If you elect to display only rejections, be advised that this may seriously impact interactive performance. Consider using the *Batch Transaction Test Report* as an alternative.

Use the F4 key to set additional testing options as you require.

- Path Type lookups
- Generic Path build direction
- Perform time-of-day checking



4. When you press **ENTER** and a transaction that meets your selection criteria is found, the *On-Line Transaction Testing Mode* screen is displayed.



```
PCTESTR                               SafeNet/i  V10                               4/06/13
MPA1                                   On-Line Transaction Testing Mode          14:41:34

Requested Security Level to Check -->  H  Historical Review
Current Server Security Setting----->  1  No Checking Performed
Max. Security Level For this Server->  3  User to Server Checked
Return Information:
Status Code--> 1  Accepted
User--> SAFENET
Job-> QZSOSIGN      Date/Time-->  4/01/2013  10.21.35.439
Source IP Address-->  10.242.1.2
Server--> *SIGNON   TCP/IP Client Signon Server
Format--> ZSOY0100  Request for TCP/IP Signon Access

F3 = Exit      Pageup/Pagedown          F5 = ReTest Transaction
F12 = Restart                                     (c) Copyright 2004 MP Assoc., Inc
```

This describes:

- The Requested Security Level setting to check
- The current Security Level for the server
- The maximum security level setting for this server
- The user making the request
- The group profile related to the user
- The date and time of the request
- The IBM i server job name the request came from
- The format
- The server function receiving the request
- Data used, if any
- Whether the request was accepted or rejected, and the reason for the rejection
- If it is displayed as a valid function key, you can **press F10** to view even more detail.

- Additional command keys are shown when rejections are displayed. These additional command keys will allow you to work directly with the appropriate user setting based on the rejection code.
5. You can roll up or down to scroll backward and forward, or you can press **ENTER** to scroll forward to the next record in the logging file.

At any time you can press **F12** to return and enter a new starting date and time, server or user, or change the Security Level to check.

Note: Use this tool to develop and test your initial security settings prior to putting them into production. You can go back and change the different **SafeNet/i** parameters to see how they affect each transaction.

Use the additional command keys shown in rejections to immediately make changes to user settings.

Batch Transaction Test Review/Report – Security Report by User

You can use this batch report to test all the historical transactions through current and future control file settings.

With this report you can make changes to control files, then re-run all the historical transactions back through a security check process to determine if further security set up is required.

If you want to see the same servers each time you run this security report, you can customize it by using Special Jobs Menu (SN2), **Option 1 - Select Default Servers for Security Report**. This option lets you select the specific servers you are interested in, then makes them the default each time you run the report.

This report is available from the Network Transaction Analysis Reports Menu (SN4), **Option 1 - Print Security Report by User** or the Special Jobs Menu (SN2), **Option 2 – Print Transaction Security Report**. You can also use the **PRTSECRPT** command.

Use F9 to display all parameters

Print Security Report (PRTSECRPT)

Type choices, press Enter.

Only print rejections	<u>Y</u>	Y, N
Select Servers	<u>*ALL</u>	*ALL, *DEFAULT, *SELECT
Sort Type	<u>*USRDAT</u>	*USRDAT, *USRSRV, *SRVUSR
Security Level Check	<u>H</u>	H, C, F
Test Time of Day	<u>N</u>	Y, N
Selection From Date	<u>*BEGIN</u>	Date, *BEGIN,
From Time	<u>*BEGIN</u>	Time, *BEGIN,
Selection To Date	<u>*END</u>	Date, *END,
To Time	<u>*END</u>	Time, *END,
User Profile(s) to Select	<u>*ALL</u>	Name, Generic*
+ for more values		
User Profile(s) To OMIT	<u>*NONE</u>	User Name
+ for more values		
Job queue	<u>*JOBQ</u>	Name, *JOBQ
Library		Name,

More...

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

MR A 05/037

On the *Print Security Report* screen fill in the following:

1. Decide if you wish to print all transactions or only those that were rejected.

Enter Y for only rejections (the default) or **N** to print all transactions

Printing only rejections will reduce the size of the output report

2. Select the servers to include in the report

- ***ALL** - all servers
- ***DEFAULT** - based on servers that were selected on the Special Jobs Menu (SN2), **Option 1 - Select Default Servers for Security Report**
- ***SELECT** - displays a list of servers to choose from

3. Select your preferred *Sort Type*

- ***USRDAT** - by user, then by date within user
- ***USRSRV** - by user, then by server within user
- ***SRVUSR** - by server, then by user within server

4. Select the correct *Security Level Check* value

- **H** = Historical Review only
Show status at actual time of client request
- **C** = Check all transactions against current server settings
- **F** = Check all transactions against the *Future* server settings

5. Decide if you want to test the time of day controls

Enter **Y** or **N** for the *Test Time of Day* parameter

6. Select these optional parameters

- Enter a start date and time or accept the default value
- Enter an ending date and time or accept the default value
- Enter a specific user ID or ***ALL**

Page Down if you would like to print the report to an output file.

When you have finished making your selections, **ENTER** to submit the report to batch.

Recommended approach to testing

A recommended approach to using the *On-Line Transaction Testing* program is:

1. Set all of the important server functions to Security Level 1, Log All. This will log all requests without affecting any users. Set your *Future Server* settings or use the pre-loaded recommended values.

Turn off logging on the non-critical servers to limit logging.
2. Collect your requests and print out the *Security Report by User* from the Network Transaction Analysis Reports Menu (SN4). Select *Historical Review*.
3. Set up your *User to Server* and *User to Object, SQL, FTP, CL*, etc. tables if you wish to go to Security Level 4.
4. You can use several tools provided with **SafeNet/i** to test your security settings. Use the *Security Report by User* or the on-line version, *PCTESTR*. These can be run to test the collected transactions against the current or future server settings. (Use Future Setting)
5. Use *Show only Rejections* on PCTESTR and *Print only Rejections* on the batch report. If your settings are correct for the Security Levels being tested, you should receive messages only for transactions that would be rejected.

If any of the requests are rejected, check the message description and make the appropriate corrections to the **SafeNet/i** settings. Try the transaction again.

Note: If you request Level 4, you may only get a security check to Level 3 since some servers support only up to Level 3. This is noted on each record in the *On-Line Transaction Testing* as “Level Requested”, “Level Checked” and “Max Level”.

PCREVIEW

Use the **PCREVIEW** command or **Option 3 - On-Line Transaction Review** from the SafeNet/i Special Jobs Menu (SN2) to review each transaction logged by **SafeNet/i**.

This displays the historical transactions only. No testing can be performed using this tool.

1. Type **PCREVIEW** and press **ENTER**.

The *Network On-Line Transaction Review* screen is displayed and the **HELP** key is active.

2. Using the fields at the top of the screen, you can select only the records you wish displayed. You can select by user, server, status, from and to date.

For example, to review only rejections for today:

- **Type R** in the Status field
- By default, today's date is entered for you

3. To obtain additional information about a particular record, **type a 1** next to the record and press **ENTER**.

The *On-Line Transaction Review Mode* screen is displayed, supplying more detailed information about the specific transaction.

```
SafeNet/i
-----
PCTESTR                               SafeNet/i  V10                               4/06/13
MPA1                                  On-Line Transaction Review Mode          14:46:24
                                      Actual Status At Time Of Request

Requested Security Level to Check --> H  Historical Review
Current Server Security Setting-----> 1  No Checking Performed
Max. Security Level For this Server-> 4  Object Level Checking
Return Information:
Status Code--> 1  Accepted
User--> SAFENET
Job-> QZRCRVS      Date/Time--> 4/01/2013 10.22.12.745
Source IP Address--> 10.242.1.2
Server--> *RMTSRV  Remote Command/Distributed Pgm Srvr
Format--> CZRC0100 Remote Command or Program Call
Details----: QSYS/QWCRTVCA

F3 = Exit      Pageup/Pagedown
F12 = Restart                                     (c) Copyright 2004 MP Assoc., Inc
```

You can use the **ROLL UP/ROLL DOWN** keys to scroll through the sequential transactions or **press ENTER** to return to the PCREVIEW sub-file screen.

If you selected only a specific user or server to be displayed in PCREVIEW, you will find that only those records meeting the selection criteria will be displayed as you scroll through the file with the on-line transaction test program.

Chapter 7 - BACKUPS AND PURGES

Log file Purge

When **SafeNet/i** is logging client requests, the information is kept in the TRAPOD file in library PCSECDTA. At times this file may grow to a considerable size. This function deletes the records in the TRAPOD file.

There are two ways to purge the TRAPOD file:

1. Standard purge using retention days or purge-through date
2. Archive TRAPOD records and generate a report

This allows you to specify the number of days to retain records or a purge-through date, and provides the capability to archive the records to an alternate file and member. You can also print a report listing either all of the purged records or only those records that were rejections.

When using **SafeNet/i** with Transaction Journaling active you can also purge old journal receivers at the same time. See additional information on journaling in Chapter 8 of this guide.

Review the STRPRGARC command, parameters *RMVRCUS* and *RRMVSTAT*. Use **F9** to display all parameters.

To perform a standard purge

1. Backup the TRAPOD file to tape, if desired.

If you do not use save-while-active, you will need to issue the **ENDTRP** command **BEFORE** beginning the backup and the **STRTRP** command **AFTER** the backup.

2. Select **Option 6** from the Special Jobs Menu (SN2) or use the **STRPRGARC** command.
3. Enter **the number of days** to retain information in the TRAPOD file or **enter the date** to purge through. The default is to retain the information for thirty days.
4. You can direct the processing of the purge to a specific job queue.

If you leave the default value of *JOBID, then the default job queue for your job will be used.

If you choose to use a different job queue, you can enter the name here. You must have the job queue's library name in your job's library list when you use this option.

5. If you ended logging prior to performing a backup, issue the **STRTRP** command to restart logging.

You can use the following command instead of the menu option:

STRPRGARC DAYS(060) ARC(*NO)

This will purge the TRAPOD file and retain 60 days of data. The number of days must be entered as three characters, i.e., 020 for 20 days.

There will be no archiving of purged records with the *ARC(*NO)* parameter.

To purge the log and archive the records

1. Select **Option 6** from the Special Jobs Menu (SN2) or use the **STRPRGARC** command.
2. Enter **the number of days** to retain information in the TRAPOD file or **enter the date** to purge through. The default is to retain the information for thirty days.
3. Make sure *Archive purged records* is set to ***YES**
4. Set *Print purged records* and *Only print rejections* to whichever option you wish
5. Use **F10** to display *Additional Parameters*
6. Select ***YES** or ***NO** for *Remove deleted records*

***YES** requires that transaction logging be turned off

You can use the following command instead of the menu option:

STRPRGARC DAYS(060) ARC(*YES) PRT(*YES) PRTR(*NO) RMVDEL(*NO)

This will purge the TRAPOD file and retain 60 days of data; archive the records; print a report listing all records, not just rejections.

All archived records are transferred to a file named TRAPARCW in PCSECDTA. Each time the archive command is run, a new file member is added to this file. It is recommended that for auditing purposes you save the archive file to tape, then remove the members.

Journaling Purge Consideration

If you are also journaling network requests and wish to purge the associated journal receivers, use parameters *RMVRCVS* and *RRMVSTAT* on the STRPRGARC command.

Press **F9** to display these additional parameters.

Automating the log file purge

To automatically purge the log file, archive the purged records and generate the transaction report, use the following command or add it to the system job scheduler:

SBMJOB CMD(PCSECLIB/STRPRGARC DAYS(XXX) JOB(SECPRG)

XXX is the number of days to retain records (060 = 60 days retention)

Automating the One Step Security Report

To automatically run the security report without purging or archiving any records, use the following command:

PRTSECRPT

There are no parameters required for this command.

If you run this command without parameters, it will generate the report using the full log file content.

To submit this command to batch type:

SBMJOB CMD(PCSECLIB/PRTSECRPT)

For additional selection criteria for this report, use the Network Transaction Analysis Reports Menu, (SN4) **Option 1 - Print Security Report by User**.

Automating and Running the Security Report and the Log File Purge Together

Use this method to automate both the **SafeNet/i Security Report** and the *Log File Purge*.

For this example, the purge is being done on Mondays and Thursdays. You may use any schedule you wish; however, make sure your purge is retaining enough days for reporting purposes.

Each of these commands provides parameters to print either only rejections or all transactions. Review these parameters and change as required.

Monday

1. Run purge and retain 5 days, print report of all rejected, purged records

STRPRGARC DAYS(005)

2. Run security report - it will print rejections for the last 5 days (Thursday through Monday)

PRTSECRPT

Thursday

1. Run purge and retain 4 days, print purged rejected records

STRPRGARC DAYS(004)

2. Run security report - it will print rejections for the last 4 days (Monday through Thursday)

PRTSECRPT

This example runs the Log File Purge and retains only 1 day of data in the file.

Saturday

1. Run security report and see entire contents of log

PRTSECRPT

2. Run purge and retain 1 day

STRPRGARC DAYS(001)

Note: It is a good idea to run these commands back-to-back and at off-peak hours to minimize performance impact.

Daily Backup Procedure

Modify your daily backup procedure to follow these guidelines.

Note: If you utilize the *Save-while-active* function for your backups, you may skip all of these steps and continue with your backups.

1. Enter command **CHGSPCSET LOGALL(*NO)**

This prevents **SafeNet/i** from attempting to log requests

2. Issue the **ENDTRP** command within **SafeNet/i**

This will end the transaction logging program and subsystem

3. Perform your normal backup steps

If you skipped Step 1, skip Step 4 also.

4. **CHGSPCSET LOGALL(*YES)** to begin logging

5. Issue the **STRTRP** command to re-start the transaction logging subsystem and program

Remember to include the **SafeNet/i** data library, PCSECDTA in your daily backup procedure. If you have SafeNet/i journaling active also include the PCSECJRN library.

Chapter 8 - JOURNALING SAFENET/i ACTIVITY

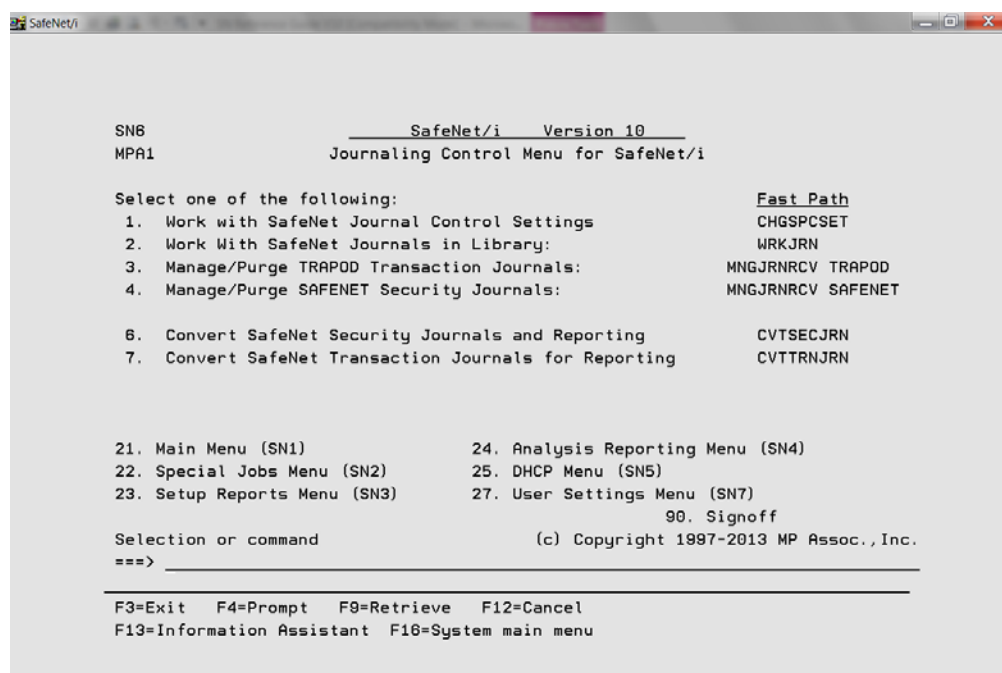
Journaling Security Files and Network Transactions

A new feature of SafeNet/i, beginning with Version 9, provides additional security and reporting capabilities through the use of IBM i Journals.

There are now two types of journal functions available for SafeNet/i:

1. Journal all the SafeNet/i security control files and data areas
2. Journal all network transactions. You may choose to log all the network transactions to the standard TRAPOD file, to a journal receiver or both the journal and the physical file

All Journal Management processes can be accessed via the Journaling Control Menu (SN6)



To start the journal processes select **Option 1 – Work with SafeNet Journal Control Settings** or use command CHGSPCSET

1. For network transaction journaling, set *Record All Transactions* (*LOGALL* parameter) to one of the following:

- *FILE
- *JOURNAL
- *BOTH
- *NONE

Note: If you select option *JOURNAL, there will be NO entries recorded into the standard TRAPOD file. If you wish to re-build the standard transactions from the journal receivers into the TRAPOD file format for reporting, you must use menu *Option 7 – Convert SafeNet Transaction Journals*.

2. For SafeNet/i security and control file journaling, set *Journal SafeNet Sec Changes* (*JRNSEC* parameter) to either *YES or *NO

Library PCSECJRN

When you activate either of the journaling types, a new library called PCSECJRN will be created on your system. This library will contain all the journals and journal receivers required for SafeNet/i.

- To **view** the Journals and Receivers in library PCSECJRN, use **Option 2 - Work with SafeNet Journals in Library** on the Journaling Control Menu (SN6)

This option utilizes the standard IBM i commands for working with journals and receivers.

- To **manage** the Journal Receivers in library PCSECJRN, use **Option 3 – Manage/Purge TRAPOD Transaction Journals** and **Option 4 – Manage/Purge SafeNet Security Journals** on the Journaling Control Menu (SN6)

Verify or Delete Journal Receivers – STRPRGARC command

- For the Network Transaction Journal, we have included an automated process to purge old journal receivers via the STRPRGARC command, found on the Special Jobs Menu (SN2), **Option 6 - Purge/Archive Log File - TRAPOD**.

Using the STRPRGARC command you can have the receiver entries purged just as you would normally purge the TRAPOD file or you can just leave the receivers on your system for future use.

- For the SafeNet/i Security Journals, you will have to remove any unwanted journal receivers using **Option 4 – Manage/Purge SafeNet Security Journals** on the Journaling Control Menu (SN6) or use the MNGJRNRCV command. Specify a purge-thru date or number of days to retain.

There is no automated management tool provided for the SafeNet/i Security journal receivers.

```
SafeNet/i

Manage SN Journal Receivers (MNGJRNRCV)

Type choices, press Enter.

Journal . . . . . > SAFENET      Name
Library . . . . . > PCSECJRN     Name, *LIBL, *CURLIB
Journal receiver saved before:
Save date . . . . . *NOCHK       Date, *NOCHK, *CURRENT
Save time . . . . .          Time, *BEGIN, *CURRENT
Journal receiver retain days . . *NONE      1-999, *NONE
Journal receivers to retain . . *NONE      1-999, *NONE
Journal receiver status . . . . *SAVED     *SAVED, *ONLINE, *PARTIAL...
Journal receiver option . . . . *VERIFY    *VERIFY, *DELETE

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

Convert and Print SafeNet/i Security Journals – CVTSECJRN command

Use this command to convert SafeNet/i Security Journal Receiver entries to a usable format and request optional reports.

The Convert Security Journal Command (CVTSECJRN) allows you to extract all the SafeNet/i Security File Journals into regular database output files for reporting and/or to track changes made to SafeNet security files for a given time frame. Any output files will be placed in the OUTFILE library specified. All the output files will have the letter "J" prefixed to the original file name.

From the Journaling Control Menu (SN6), use **Option 6 – Convert SafeNet Security Journals and Reporting** or use the **CVTSECJRN** command

```
SafeNet/i

Convert SafeNet Sec Journals (CVTSECJRN)

Type choices, press Enter.

Convert From Date . . . . . _____ Date
Convert To Date . . . . . _____ Date
Run Journal Entry Reports? . . . *YES *YES, *NO
Original File Name . . . . . *ALL *All or Specific File Name.
Job queue . . . . . *JOB *Name, *JOB
Library. . . . . _____ Name,
Report Sequence . . . . . *BYADMIN *BYUSER, *BYADMIN, *BYDATE
Admin Profile to Select. . . . *ALL Name, *ALL
User Profile to Select. . . . *ALL Name, *ALL
Report Output Queue . . . . . *JOB Name, *JOB
Library. . . . . _____ Name,
Delete Outfile after Reports? . *YES *YES, *NO
Outfile Library . . . . . QTEMP Library Name
Email Results to Address . . . *NONE

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

MP A 05/037
```

Additionally you can generate reports of any changes made by using the CVTSECJRN Reports option. Selection options allow you to specify a specific file, administrator or user to generate reports for. In addition, you can email the result reports to any valid email address.

Using this command in conjunction with SafeNet/i security journaling, it is possible to automatically generate a daily report of any SafeNet/i security setting changes made and have it automatically email you the results.

We have provided you with a sample CL program to demonstrate how you can generate a daily report.

See source file QSAFESRC in library PCSECLIB member RUNDLYJRN. Modify as required.

Sample Security Audit Report

REPORT - Notepad

File Edit Format View Help

Convert Network Transactions Journal Receivers – CVTTRNJRN command

Use this option to convert the network transactions journal receiver entries to a usable format.

From the Journaling Control Menu (SN6), use **Option 7 – Convert SafeNet Transaction Journals for Reporting** or use the **CVTTRNJRN** command

```
SafeNet/i

Convert SN Transaction Journal (CVTTRNJRN)

Type choices, press Enter.

Convert From Date . . . . . _____ Date
Convert To Date . . . . . _____ Date
Outfile Library . . . . . _____ Character value
Job queue . . . . . *JOBID Name, *JOBID
Library. . . . . _____ Name,

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

Bottom
```

You must specify a date range to select and a library name to contain the converted file. The file will be called JTRAPOD. It is in the same format as the original TRAPOD file normally used for transaction logging.

If you wish to use the converted file for additional reporting, you must first either copy it to a new archive member (file TRAPARCW) or copy the records back into the TRAPOD file.

Important: If you copy the records directly back into the TRAPOD file, you must make sure you are not duplicating or replacing the existing records in the TRAPOD file. Confirm that the date range you select will not include records that are currently in your TRAPOD file or you may duplicate existing transaction records.

If you use the TRAPARCW archive file:

1. Add a new member to the file.

2. Copy the records from the converted JTRAPOD file to the new member in TRAPARCW file.
3. You can use the PRTSECRPT command to print a normal SafeNet/i security report from the converted transaction journals by simply specifying the archive member name in parameter ARCMBR.

Chapter 9 - SPECIAL SAFENET CONSIDERATIONS

This section contains information on procedures that will help you manage and automate certain **SafeNet/i** functions.

Excluding an Exit Point from SafeNet/i Checking

You can 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 before consulting with SafeNet/i support staff. However, you may find that your system requires that a specific exit program be excluded.

To exclude an exit point from SafeNet/i checking, follow these steps EXACTLY:

1. At the command line, run the following commands

ADDLIB PCSECLIB
ADDLIB PCSECDTA

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

CALL ACTEPXCL

3. Find the exit point on the list that place a **2** next to it. On the detail screen that follows, code the exclusion code with the letter X and press **ENTER**.
4. Bring your system to a 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.

Restoring an Exit Point to SafeNet/i Checking

If it becomes necessary to once again have SafeNet/i linked to the exit point that has been excluded, you can do so by following the exact same procedure as excluding the point, outlined on the previous page, EXCEPT that at step #3, remove the letter X and leave the exclusion code blank.

When you start your controlling subsystem, SafeNet/i will be re-connected to the exit point.

When you restore an exit point, SafeNet/i will re-set the server security level to 1. Use **Option 1** on the SafeNet/i Main Menu (SN1) or the **WRKSVR** command to check the security level of the server and change it to the level you require.

Resetting Level 5 within SafeNet/i

When an installation has a user exit program in place that **SafeNet/i** does not recognize, the exit point will automatically be set to Level 5 (unsupported). To allow **SafeNet/i** to support this server you must do the following:

1. Remove your user exit program from the registration facility in i OS.

Type **WRKREGINF** and press **ENTER**

Locate the exit point and remove your exit program.

Important: Do not remove any program called from PCSECLIB.

You may have several servers set to Level 5. You must remove each one. Then, using the DSPNETA or CHGNETA command, verify that your IBM i network attributes DDMACC and PCSACC are both set to *OBJAUT.

If these attributes are not initially set to *OBJAUT, **SafeNet/i** will flag several exit points to Level 5.

2. Type the following:

CALL PCSECLIB/DELST5CL and press **ENTER**

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

Press F3 to exit **without making any changes**

4. Using the IBM i console, you must place the system in a restricted state with the **ENDSBS *ALL *IMMED** command, or any other site-specific shutdown process.

5. De-activate **SafeNet/i**

From the Install Menu select **Option 50 - Activate/De-Activate SafeNet/i**

Follow the instructions to de-activate the program found in Chapter 13 in this guide, 'De-activating and Removing SafeNet/i'.

6. Re-activate **SafeNet/i**

Select **Option 50 - Activate/De-Activate SafeNet/i**

7. Restart your system

Pre-Power Down Program Point

You can create a power down CL program to be called whenever the PWRDWN SYS command is issued. **SafeNet/i** will call this program and log the request whenever the command is processed.

To use this feature, create a CL program called PWRDWNCL and place it in library QGPL.

Profile Swapping

Profile Swapping allows you to assign an alternate or a "swapped" user profile to be interrogated by **SafeNet/i** and passed to i OS for security lookups.

When profile swapping is in use, any incoming network transactions or jobs are assigned the alternate profile (the 'Swap to' profile) and passed as this alternate profile to i OS. The operating system then performs all security related checking as if the request came from the 'Swap to' profile and not the original profile. The job in i OS retains its original user name.

All authority checking by **SafeNet/i** is performed using the original profile name.

Alternate Profile Swapping is controlled using the **CHGSPCSET** command or from SafeNet/i Main Menu, (SN1) *Option 2*. Set the *SWAPU* parameter to one of these values:

- ***NO**

Do not swap profiles within **SafeNet/i**

- ***OPT**

SafeNet/i will swap profiles if the original user has an alternate swap profile set up in **SafeNet/i**

- ***RQD**

Requires that a swap profile must be set up for the original profile in **SafeNet/i**, or all requests are rejected.

Setting up a Swap Profile

Make sure that you have set the *SWAPU* parameter on the **CHGSPCSET** command to allow profile swapping. Then follow these steps to set up your alternate profiles.

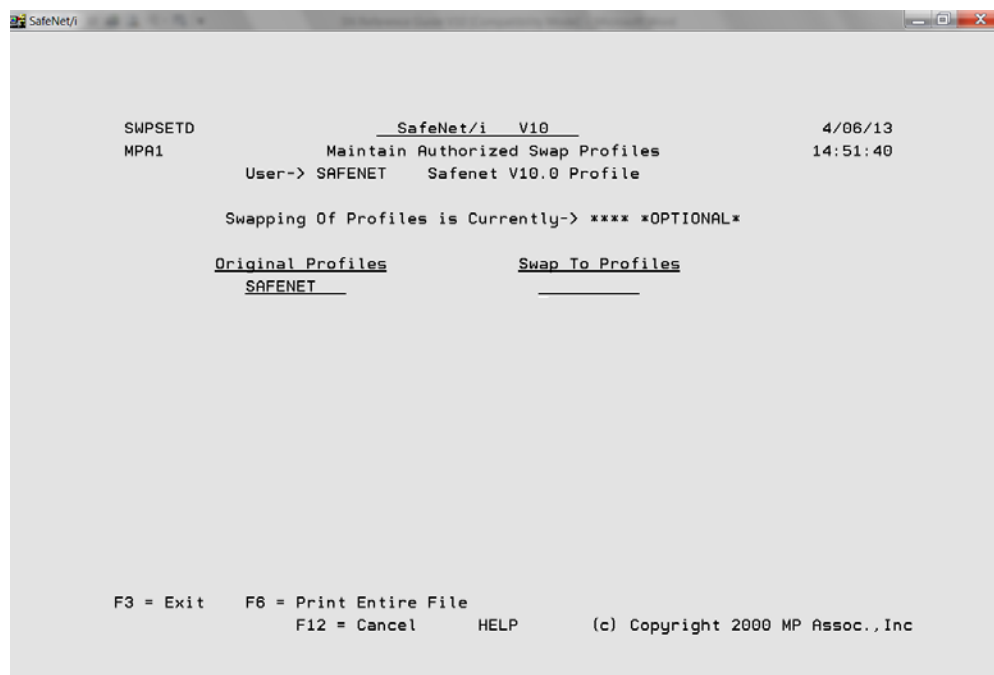
1. From the User Settings Menu, (SN7) select **Option 9 – Work with Swap Profile Maintenance** or use the **WRKSWPPRF** command

2. Enter the **user profile** to work with.

You can type the user profile, use F4 for a list, or type *ALL for a complete list of swap profiles.

Press **ENTER**

The *Maintain Authorized Swap Profiles* screen appears



3. On the Maintain Authorized Swap Profiles screen, **type the Swap To Profile** then press **ENTER**

Now, whenever a user connects to the IBM i through a client/server connection after **SafeNet/i** checks the original profile, i OS will do all security checking on the 'Swap to' profile.

Files Contained in SafeNet/i

These files are available for you to use for any additional reporting requirements you may have. All are located in library PCSECDTA.

DHCPBLOG

Contains DHCP Bindings log reports

DHCPRLLOG

Contains DHCP Release log reports

ERRORD File

Contains all error codes (accepted/rejected) associated with **SafeNet/i**.

FIXEDIPS

Contains fixed IP client addresses (static addresses)

IBMFLR File and IBMFLRL (Long paths to IBM folders)

Contains all IBM supplied folder names. You may add additional folder names to this file for automatic READ and/or WRITE authority as required.

JRNFILES

Contains the names of files in SafeNet/i that are journaled when using the journaling feature within SafeNet/i

MACNAMES

Contains MAC addresses with names of associated DHCP clients

TRAPARCW File

Contains all the purged transactions if the STRPRGARC command was utilized

TRAPOD File

All logged network requests are placed in this file. This file will grow significantly over time, depending on network traffic. Be sure to pay close attention to its size and establish a schedule to purge records.

This file can also be used for additional user-developed reporting. See IBM OS/400 Servers and Administration for additional information and record layouts.

Extra Security for TRAPOD

SafeNet/i provides an option for imposing extra security on the TRAPOD file to prevent anyone from altering the file.

By default the TRAPOD file is secured by the SAFENET authorization list. As such, the only users who have full access to the file are SafeNet/i administrators plus any other users with *ALLOBJ authority.

Normally, this should be sufficient security since all of these users fall into the category of security officers.

However, if you need an extra level of security for this file in order to satisfy audit requirements, you can use the SETTRAP command to activate additional security for the TRAPOD file.

The SETTRAP command will toggle this extra security on or off. To activate the additional security us this command:

SETTRAP SECSTS(*ON)

When the extra security is turned on, SafeNet/i administrators will no longer have direct access to the TRAPOD file. They will be limited to using SafeNet/i tools which do not permit data manipulation, only purging.

Users with all object authority will still have access, but this should limit the pool of users to very few for your installation.

To deactivate this extra security, use the following command:

SETTRAP SECSTS(*OFF)

This will re-establish security based on the SAFENET authorization list.

SafeNet/i Commands

Commands	Description
ADDSNADM	Maintain SafeNet Administrators
ADDSNUSR	Allows batch maintenance of SafeNet/i users
ADDUSRCMD	Allows batch maintenance of users to commands
ADDUSRFTP	Allows batch maintenance of users to FTP
ADDUSROBJ	Allows batch maintenance of users to objects
ADDUSRSQL	Allows batch maintenance of users to SQL
ADDUSRSVR	Allows batch maintenance of users to servers
CHGFTPSET	Change FTP special settings
CHGNOTIFY	Changes status of Alert Notification
CHGSPCSET	Change SafeNet/i special settings
CHGTELNET	For Kerberos and Telnet security setting override
CPYSNUSR	Copy settings from one SafeNet/i user to another
CVTTRNJRN	Extract all the SafeNet/i Network Transactions journals into regular DB files for reporting
CVTSECJRN	Extract all the SafeNet/i Security File journals into regular DB files for reporting
ENDTRP	Ends the transaction logging program
MNGJRNRCV	TRAPOD
MNGJRNRCV	SAFENET
IPPING	Performs IP Address ping check
PCREVIEW	Starts the on-line transaction review process
PCTESTR	Starts the on-line transaction testing program
RMVSNUSR	Removes a user from all SafeNet/i enrollments
RMVSNUSR1	Removes all profiles not defined to OS400. Excludes profiles beginning with '*' (*Public)
RMVUSRCMD	Removes user's authorities to CL commands
RMVUSRFTP	Removes user's authorities to FTP
RMVUSROBJ	Removes user's authorities to objects

Commands	Description
RMVUSRSQL	Removes user's authorities to SQL
RMVUSRSRV	Removes user's authorities to server functions
SETSAFENET	OPTION(A) – Activates SafeNet/i
SETSAFENET	OPTION(B) – Deactivates SafeNet/i
SETVER	Used to change the license code level of SafeNet/i
SNDHCPPRG	Purge expired DHCP lease information
SNEXESUM	Generate Executive Summary report
STRALRT	Starts Alert Notification monitoring
STRPRGARC	Starts archive purge/security report of log file
STRTRP	Starts the transaction logging program and SBS
WRKDFTSRV	Select servers to include in Security Report
WRKSIGNON	Work with TELNET sign-on parameters
WRKSNADM	Maintain SafeNet/i Administrators
WRKSNSUSR	Work with SafeNet/i Super Users
WRKSNDHCP	Work with current DHCP activity
WRKSRV	Work with server security settings
WRKSWPPRF	Work with Swap Profiles
WRKTCPIPA	Work with TCP/IP address control
WRKUSRCMD	Work with user to CL commands
WRKUSRFTP	Work with user to object FTP statement security
WRKUSROBJ	Work with user to object security
WRKUSRPTH	Work with User to IFS path security
WRKUSRSEC	Work with user security. Permits access to all security screens for an individual user without entering several different commands
WRKUSRSQL	Work with user to object SQL statement security
WRKUSRSRV	Work with user to server security

Print Commands

Commands	Description
PRTCLUSG	Reports command usage and auto-enrollment
PRTFTPUSG	Starts the FTP transaction and testing program
PRTMACINF	Print MAC Address and Static IP Address
PRTOBJUSG	Starts the object transaction and testing program
PRTPTHUSG	Starts the IFS path transaction and testing program
PRTSECRPT	Print security report
PRTSNADM	Print the list of SafeNet/i Administrators
PRTSNSUSR	Print the list of SafeNet/i Super Users
PRTSQLUSG	Reports SQL statement usage and auto-enrollment
PRTSRVSTS	Print Server Status listing
PRTSRVUSG	Reports server usage and auto-enrollment
PRTTCPIPA	Print the TCP/IP address controls listing
PRTUSRALL	Prints all the setup reports for a user
PRTUSRSRV	Prints the User to Server Authorization report
PRTUSROBJS	Prints the User to Object Authorization report
PRTUSRSQL	Prints the User to Authorized SQL Statement report
PRTUSRFTP	Prints the User to Authorized FTP Statement report
PRTUSRCMD	Prints the User to Authorized Command report
PRTUSRPTH	Prints the User to Long Paths report
PRTUSRSWP	Prints the Swap Profile listing

Menu Fast Path Commands

Commands	Description
SN1	SafeNet/i Main Menu
SN2	Special Jobs Menu
SN3	Reports Menu
SN4	Network Transaction Analysis Reports
SN5	DHCP Control and Reports Menu
SN6	Journaling Control Menu
SN7	User Settings Menu
SNX	Fast Path Expert Menu

Chapter 10 - Using Automatic Alert Notification

Alert notification continually monitors network activity and can issue warning messages to up to five different message queues whenever an attempt is made to access an unauthorized server or object.

You can also choose to have alerts sent via e-mail directly or using the **SNDDST** command. If you use a distribution list for alert notification instead of a regular e-mail address, the Distribution List ID Qualifier **MUST** be your IBM i system name.

In addition, you must have set up SMTP mail options on the IBM i.

There are two types of alert notification available. We recommend using summarized alerts after the initial installation and setup. Using summarized alerts, you can prevent a flood of e-mails in the event of a large number of rejected transactions being processed by SafeNet/i.

1. Summarized alerts - you can receive a message that gives summarized information regarding **SafeNet/i** rejections. For example, "There have been six (6) rejections by **SafeNet/i** since 01/01/99 at 12:00:00".

This process starts the SAFELOGING subsystem, which contains a pre-start job called ALERTWATCH. SAFELOGING runs from the *BASE memory pool and uses very little system resources. You can set the time interval between alerts; by default 30 minutes is used.

When you specify summary alerts via e-mail, **SafeNet/i** will include a list of the summarized alerts in the form of an e-mail attachment text file.

This attachment provides information regarding the nature of the alerts being reported and eliminates the need to access the system for details.

2. Detailed alerts - you can specify that **SafeNet/i** send detailed alert messages. Every **SafeNet/i** rejection will generate a message that describes the user, server and date/time that a request was rejected.

This option does not start the ALERTWATCH program, since it is not required when detailed messages are specified.

Activating SafeNet/i Alert Notification

1. From the SafeNet/i Main Menu (SN1) select **Option 3 - Alert Notification Settings** or use the **CHGNOTIFY** command and **press F4**.
2. **Type *ON** for parameter *ALERT* to activate alert notification, then **ENTER**.
3. Enter ***YES** to receive summarized alerts or ***NO** for detailed alerts.
4. Enter ***YES** to receive alerts as e-mail or ***NO** to receive alerts as workstation messages only.

Your system must be configured for SMTP before e-mails can be used.

5. **Enter the message queue(s) and/or e-mail distribution list(s)** that should receive these alerts. You can send alerts to both message queues and distribution lists, or directly to a specific Internet email address.

The alerts are not sent to message queues in **BREAK* mode. To receive these alerts immediately, make sure the user message queue is in **BREAK* mode. (See **CHGMSGQ** command in the IBM CL Manual)

6. You can enter **individual e-mail addresses** to receive alerts in addition to, or instead of, message queues and distribution lists.

Use the '+' sign to enter additional values.

7. et the **Summarized Alert Interval**

If the *Summarized Alerts* parameter is set to ***YES**, you can specify the number of minutes between alerts. You will receive notification when each interval expires, indicating the number of rejections since the last notification.

Creating a Distribution List

Use the **CRTDSTL** command to create a distribution lists for SafeNet/i alerts if required.

Chapter 11 - DHCP CONTROLS AND REPORTING

Dynamic Host Configuration Protocol

DHCP allows clients to obtain IP network configuration, including an IP address, from a central DHCP server. DHCP servers control whether the addresses they provide to clients are allocated permanently or leased for a specific period of time. When the server allocates a leased license, the client must periodically check with the server to re-validate the address and renew the lease.

The DHCP client and server programs handle address allocation, leasing and lease renewal.

If you are using DHCP on your IBM i this gives you a way to control it. If you are not using DHCP, you can still use these options to review other activity.

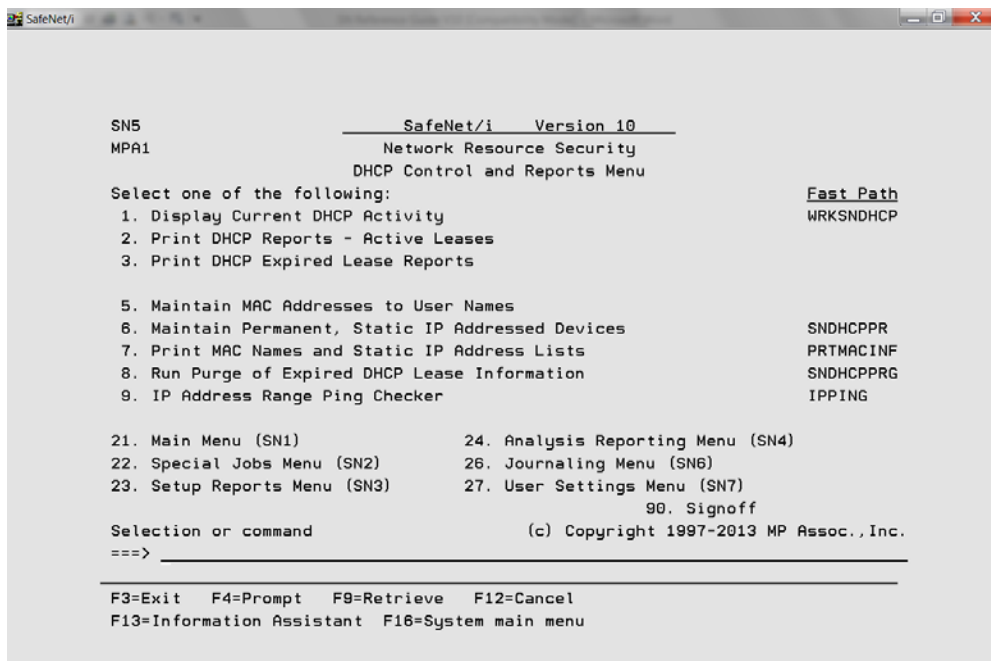
To use the IBM i as a DHCP server, refer to the relevant i OS manual and/or System i Navigator.

Working with DHCP

DHCP functions are performed from the DHCP Control and Reports Menu (SN5).

From the SafeNet/i Main Menu (SN1) select **Option 25 – Go To DHCP Menu**

The *DHCP Control and Reports Menu* appears.



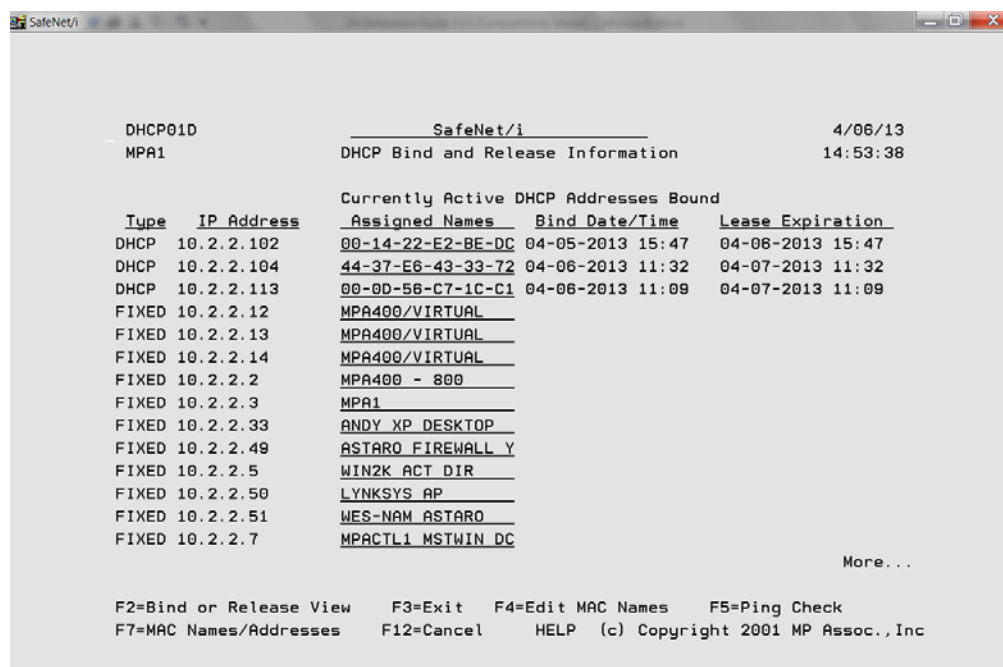
The DHCP functions provide the ability to maintain MAC addresses and device names, set IP addresses and ping IP addresses.

From the DHCP Control and Reports Menu (SN5) you can also run reports for active and expired leases, MAC names and IP address lists.

Current DHCP Activity

To see current status, from the DHCP Control and Reports Menu (SN5) select **Option 1 – Display Current DHCP Activity**

This screen displays bind and release information



DHCP01D		SafeNet/i		4/06/13	
MPA1		DHCP Bind and Release Information		14:53:38	
Currently Active DHCP Addresses Bound					
Type	IP Address	Assigned Names	Bind Date/Time	Lease Expiration	
DHCP	10.2.2.102	00-14-22-E2-BE-DC	04-05-2013 15:47	04-06-2013 15:47	
DHCP	10.2.2.104	44-37-E6-43-33-72	04-06-2013 11:32	04-07-2013 11:32	
DHCP	10.2.2.113	00-0D-56-C7-1C-C1	04-06-2013 11:09	04-07-2013 11:09	
FIXED	10.2.2.12	MPA400/VIRTUAL			
FIXED	10.2.2.13	MPA400/VIRTUAL			
FIXED	10.2.2.14	MPA400/VIRTUAL			
FIXED	10.2.2.2	MPA400 - 800			
FIXED	10.2.2.3	MPA1			
FIXED	10.2.2.33	ANDY_XP_DESKTOP			
FIXED	10.2.2.49	ASTARO_FIREWALL_Y			
FIXED	10.2.2.5	WIN2K_ACT_DIR			
FIXED	10.2.2.50	LYNKSYS_AP			
FIXED	10.2.2.51	WES-NAM_ASTARO			
FIXED	10.2.2.7	MPACTL1_MSTWIN_DC			

More...

F2=Bind or Release View F3=Exit F4=Edit MAC Names F5=Ping Check
F7=MAC Names/Addresses F12=Cancel HELP (c) Copyright 2001 MP Assoc., Inc

Use function keys to switch views:

- F2 switches between the *Currently Active DHCP Addresses Bound* and *Expired or Released DHCP Addresses* screen

The *Expired or Released* addresses list contains information gathered since the last time the list was purged.

- F7 switches between *MAC addresses* and the assigned names

You will notice that the devices with fixed IP addresses do not change as you toggle between the two displays.

- F4 puts you in edit mode and allows you to revise the assigned names

Move your cursor to the name you want to change in the *Editable Names* column. Press **ENTER** to record the change.

To use this function make sure you are looking at the *Currently Active DHCP Addresses Bound* screen. Use F2 if necessary to switch.

- F5 pings the addresses

This will ping all the IP addresses that are displayed. The responses will flash at the bottom of the screen. When the process has completed, you will see a *Ping Status* column indicating the results of the pings.

If you are looking at the active addresses, you will ping those. If you are looking at expired or released addresses, all of those will be pinged.

Be aware that pinging the expired or released addresses can take a very long time depending on the last time the list was purged.


The number of packets and time-to-wait are controlled by two data areas: PINGPKTS and PINGTIME in PCSECDTA.

The default is one packet and one second wait. You can change these data areas manually if required.

Maintaining MAC Addresses

From the DHCP Control and Reports Menu (SN5) select **Option 5 – Maintain MAC Addresses to User Names**

This operates as a standard IBM i DFU program.



The screenshot shows a terminal window titled 'SafeNet/i' containing the MACDFU program interface. The interface is a text-based menu with the following fields and options:

```
MACDFU                                     Mode . . . . : INSERT
Format . . . . : RMAC                     File . . . . : MACNAMES

MAC Address: 00-02-E3-0C-1E-FA
Assigned Name: CD

F3=Exit      F5=Refresh      F8=Select format
F9=Insert    F10=Entry       F11=Change
```

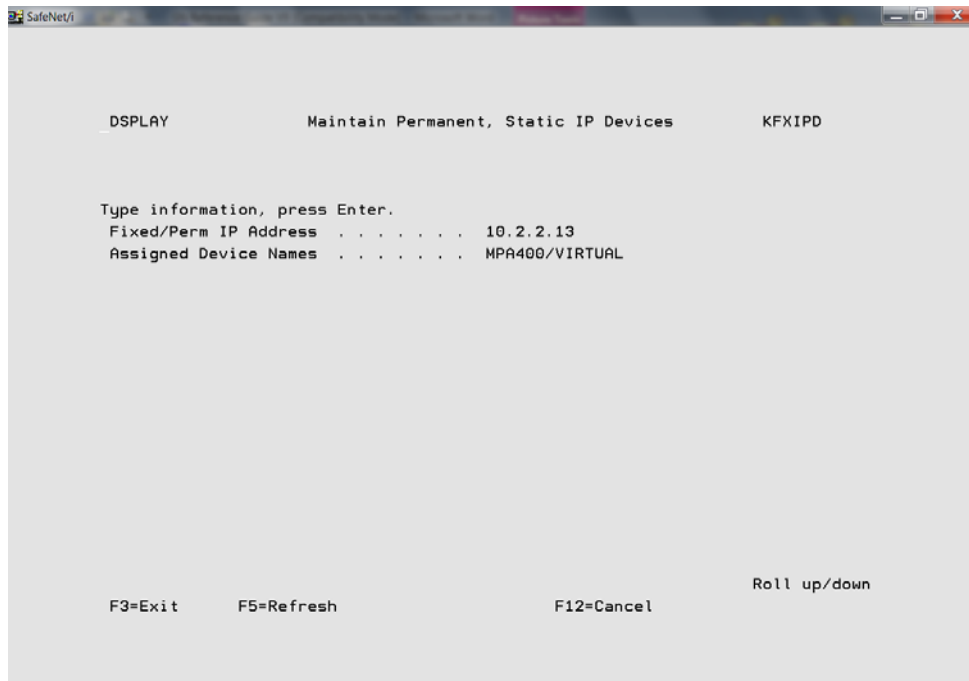
Press **F9** to use insert mode when editing

Press **F23** to delete the MAC address and name

Fixed IP Addresses

To assign IP addresses to devices, from the **DHCP Control and Reports Menu (SN5)** select **Option 6 – Maintain Permanent, Static IP Addressed Devices** or use the **SNDHCPPR** command

Even if you are not using DHCP on your IBM i, you can use this option to do PING checks for network troubleshooting.

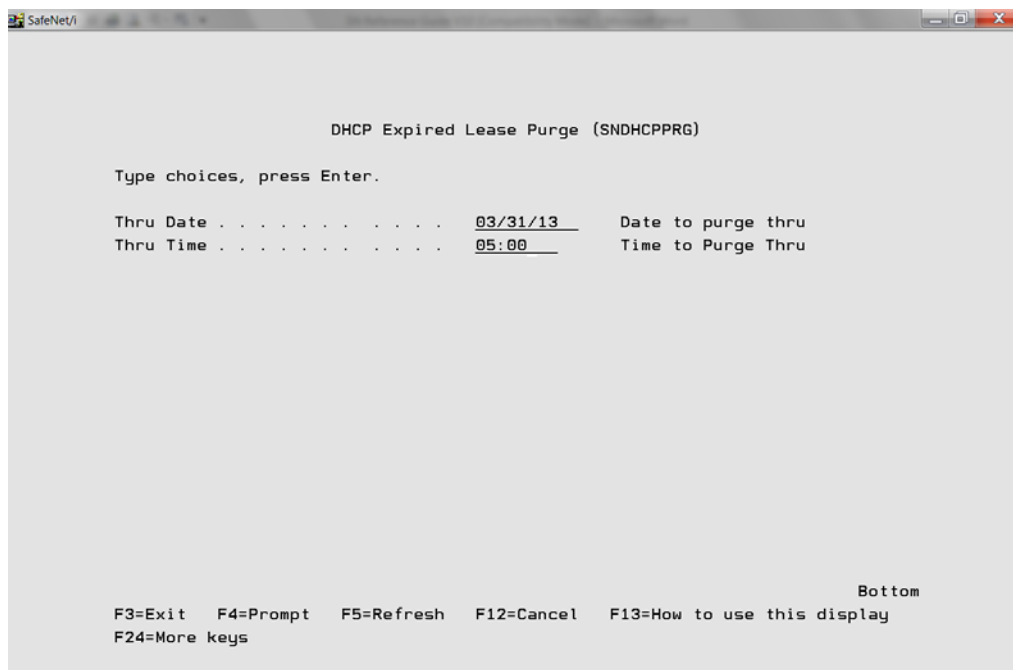


If you enter a DHCP IP address you will receive an error message. This is for fixed IP addresses only.

Purging Expired DHCP Lease Information

The *Expired or Released DHCP* address information is cumulative and will remain in the system until you purge it.

From the DHCP Control and Reports Menu (SN5) select **Option 8 – Run Purge of Expired DHCP Lease Information**



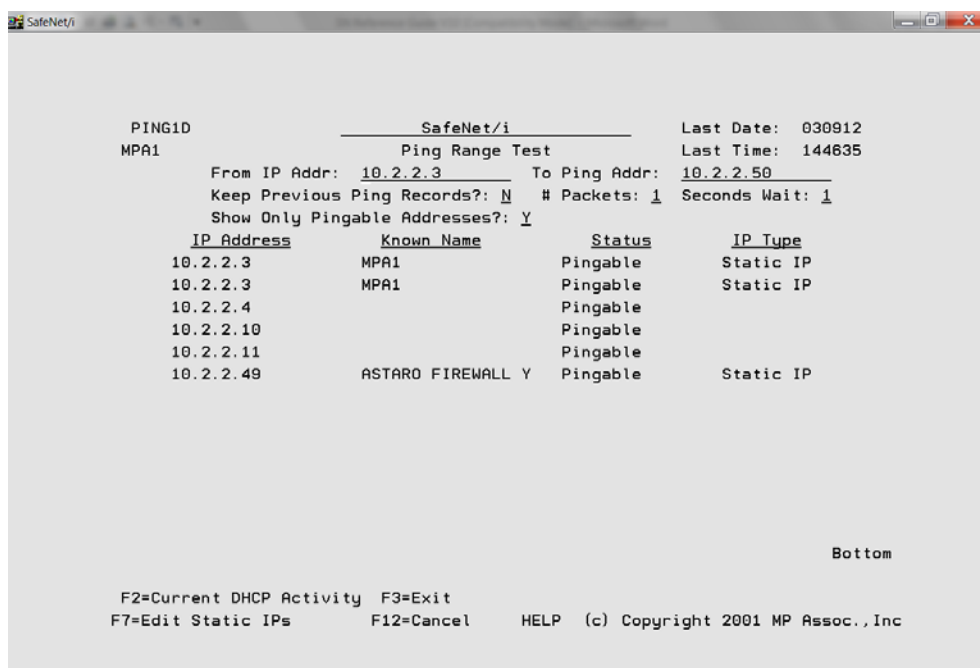
The screenshot shows a window titled "SafeNet/i" with a standard Windows title bar. The main content area is titled "DHCP Expired Lease Purge (SNDHCPPRG)". Below the title, it says "Type choices, press Enter." There are two input fields: "Thru Date 03/31/13" and "Thru Time 05:00". To the right of these fields are the labels "Date to purge thru" and "Time to Purge Thru". At the bottom of the window, there is a section labeled "Bottom" containing a list of function key shortcuts: "F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display F24=More keys".

Enter the date and time to purge through. When you **ENTER** the log of expired DHCP leases will be cleared.

Ping Checker

You can use this option to ping a single IP address or a range of addresses.

From the DHCP Control and Reports Menu (SN5) select **Option 9 – IP Address Range Ping Checker**



```
SafeNet/i
PING1D
MPA1
      SafeNet/i
      Ping Range Test
      From IP Addr: 10.2.2.3 To Ping Addr: 10.2.2.50
      Keep Previous Ping Records?: N # Packets: 1 Seconds Wait: 1
      Show Only Pingable Addresses?: Y
      IP Address      Known Name      Status      IP Type
      10.2.2.3        MPA1          Pingable    Static IP
      10.2.2.3        MPA1          Pingable    Static IP
      10.2.2.4          Pingable
      10.2.2.10         Pingable
      10.2.2.11         Pingable
      10.2.2.49        ASTARD FIREWALL Y Pingable    Static IP

Bottom

F2=Current DHCP Activity F3=Exit
F7=Edit Static IPs      F12=Cancel  HELP (c) Copyright 2001 MP Assoc., Inc
```

Enter the range of IP addresses that you want to ping.

You must re-type at least one of the IP addresses to refresh the data entry fields.

Press **ENTER** and you will begin to see replies flash on the bottom of the screen.

When all the IP addresses have been pinged the *Status* column will display the results of the pings.

Chapter 12 - PROBLEM DETERMINATION

If **SafeNet/i** is not working properly, there are a few general things to check.

Error Message Received on the IBM i

1. Did you perform an IPL after the initial **SafeNet/i** installation?

It is necessary to IPL your IBM i after completing the installation steps. If you do not IPL your system, you will experience unpredictable results.

Recovery: IPL your system then try **SafeNet/i** again.

2. Is the PTF level on your IBM i current?

Compare your PTF level with **SafeNet/i** required levels.

Recovery: Install the latest cumulative PTF package if necessary.

3. Is your client application current on service packs or fixes?

Check to make sure you have the most recent level of fixes for your client.

Recovery: Apply latest service pack or fix package

4. Is this the first time you are using this client application?

If this is the first time you are using this particular application, it may be that your server functions are not set up properly.

Recovery: Check **SafeNet/i** request logs for errors and correct. Use on-line testing program to verify your settings are correct.

5. Have you made changes to server function Security Levels or user authority tables?

If a particular request was working, and now it is not, make sure you have not inadvertently disabled a server function or revoked authorities from a user.

Recovery: Double check changes against the request log, use the on-line transaction program to test your authority settings.

Error Message Received on the Client

If you receive an error message indicating a problem with a client or a communications request, or an exit program rejection and **SafeNet/i** is active:

Check the request log for a 'REJECTED' response

1. Use the date and time along with the user ID to find the request that was rejected. Use **PCREVIEW** or check the Security Report.
2. When you find the request that was rejected, the log will indicate the reason for the rejection. You will find a list of error codes and their descriptions at the end of this chapter.
3. If you need to make changes to authorities you can test your changes with the on-line transaction program before you implement them. See Chapter 7 in this guide, 'Testing your Security Settings.'

If the request does not appear in the log or the Review screen

These steps should help you determine if the problem is network related, client related or **SafeNet/i** related.

1. Try the same request with a user ID that has rights to all servers and has all object and all folder authority. User profile QSECOFR is set up with all rights in **SafeNet/i** by default.
2. Check the log file for the request and response.
3. Make changes to authorities if necessary.
4. Try the request again with the original client or with the on-line transaction program.
5. Try a different client or user ID.

If you are unsure that SafeNet/i is the source of the problem

1. Reset the Security Level in **SafeNet/i** by following these directions:
 - From the SafeNet/i Main Menu select **Option 1 – Work with Server Security Settings** or use **WRKSRV** command
 - If you know which server function the request is using, change the server's Security Level to 1. If you cannot determine which server function the request is attempting to access, set all the servers to Security Level 1.
 - Try the client request again
 - If the request is successful, change the server (or servers) back to the original Security Level, Logging Level All. This will log all the client requests.
2. Try the client request again.
 - If the request is successful, run the request log report and review the client request.
 - If the request is rejected, check PCREVIEW to view the actual transaction.
 - Make the required authority table changes. Test your changes with the on-line transaction program.
 - Try the client request again and review the logs again.

Verify most recent IPL

If you receive a message on the IBM i about a **SafeNet/i** or PCSECLIB program, or you still cannot resolve a client error or client application error, check to see if the system was IPL'd since you:

- Initially installed **SafeNet/i**
- Applied PTFs to **SafeNet/i**

If not, you must IPL your system for the changes to take effect.

If you still cannot resolve the problem

1. Check all the joblogs for the jobs in the subsystems:

QSYSWRK
QSERVER

2. You may have to change the QDFTJOB job description to capture the joblogs of certain jobs initiated by client requests.

CHGJOB QDFTJOB LOGLVL(4 00 *SECLVL) LOGCLPGM(*YES)

Note: Remember to change this back to its default when you have resolved the problem or you may generate an excessive number of joblogs.

CHGJOB QDFTJOB LOGLVL(4 00 *NOLIST) LOGCLPGM(*NO)

3. End then start both subsystems:

QSYSWRK
QSERVER

4. Try the client request again

5. Check for joblogs and errors

6. You may have to end and re-start QSYSWRK and QSERVER to force joblog creation.

Also try **ENDTCPSVR *ALL, ENHOSTSVR *ALL;** then **STRTCP** and **STRHOSTSVR *ALL.**

To determine if the problem is with the server or a client, try this process with another client application that may access the same server.

Examples of Client Error Messages

Some common error messages you may see on a Windows95 client:

This message was received on the client when the server function was set to Level 2 - Function Disabled/No Access.

This message was received on the client when the user was not authorized to the server.

This message was received on the client when the user was not authorized to the SQL Select statement.

Error Codes which Appear in the Log

1	Accepted	
0	Rejected	Reason unavailable
A	Rejected	Server is turned off
B	Rejected	No authority to server
C	Rejected	No authority to object
D	Rejected	No authority to library
E	Rejected	Invalid Data Rights authority
F	Rejected	Invalid Object Management Rights
G	Rejected	Unauthorized path statement
H	Rejected	No authority to SQL statement
I	Rejected	Incoming commands *OFF
J	Rejected	No authority to Root Directory
K	Rejected	Unauthorized FTP Logon
L	Rejected	Unauthorized FTP Command
N	Rejected	Unauthorized REXEC Logon
O	Rejected	Unauthorized TFTP Logon
P	Rejected	Unauthorized IP Address
Q	Rejected	Invalid Op-Specific Request

R	Rejected	Auto-signon requires password
S	Rejected	TELNET requires password
T	Rejected	Encrypted password required
U	Rejected	No devices available
V	Rejected	Unauthorized CL command
X	Rejected	Error with Swap Profile
Y	Rejected	Error during Profile Swap
Z	Rejected	User/Server Reject Code (Specific *REJECT in WRKUSRSRV)
@	Rejected	Time of Day control
#	Rejected	Function requires SafeNet/i regular Admin authority
\$	Rejected	Function requires SafeNet/i Super Admin authority
%	Rejected	FTP Encryption is required
c	Rejected	No authority to Spool File
d	Rejected	No authority to OUTQ

Additional Troubleshooting Tips

PCREVIEW Command

Use the PCREVIEW commands to easily view historical network transactions. You can select various filters to display only the records from the log file you are interested in. From this screen you can request details of the information.

TRAPOD File

When testing network requests through **SafeNet/i** you can see each transaction being written to the **TRAPOD** file in library PCSECDTA.

Use the operating system command DSPPFM (Display Physical File Member) to look at the contents of the **TRAPOD** file. Type **B** on the *Control line* and press **ENTER**. This will take you directly to the bottom of the file and enable you to see the last request recorded in the file.

As a network request is processed by **SafeNet/i**, a record is written to the **TRAPOD** file. The name of the **SafeNet/i** program that processed the request is in position 1-10; the status of the request is in position 11 (1= Accepted, all others are rejections); the user profile is in position 12-21.

The rest of the record contains specific information based on the request type. Detailed information is available in IBM's TCP/IP Configuration and Reference Guide or the specific licensed program manual.

Chapter 13 - DE-ACTIVATING AND REMOVING SAFENET/i

You must be signed on as a Super Admin in SafeNet/i to perform any Activate/De-Activate processes. See 'SafeNet Administrator' in Chapter One of this guide.

De-activating SafeNet/i

Under some circumstances you may want to de-activate **SafeNet/i**. It may be necessary when troubleshooting network problems to make sure they are not being caused by an application such as **SafeNet/i**, or when you need to remove **SafeNet/i** from your system.

If after you have de-activated **SafeNet/i** you still have problems with network requests or connections, you may want to IPL your IBM i or **ENDSBS *ALL** to uncover any autostart jobs or other IPL-initiated i OS activities that may still be allocating **SafeNet/i** objects and programs. This is not required if you do not need to de-allocate all the **SafeNet/i** programs.

Once you have been successful in isolating your network problem, you can re-activate **SafeNet/i**.

Before de-activating

Optionally, rather than de-activating SafeNet/i you can remove one or more exit points if required.

For example, if you have a problem with the *FILESRV server function use the **WRKREGINF** command to:

1. Locate the IBM i exit point for the *FILESRV server function
2. Remove the SafeNet/i exit program
3. Stop and restart the file server

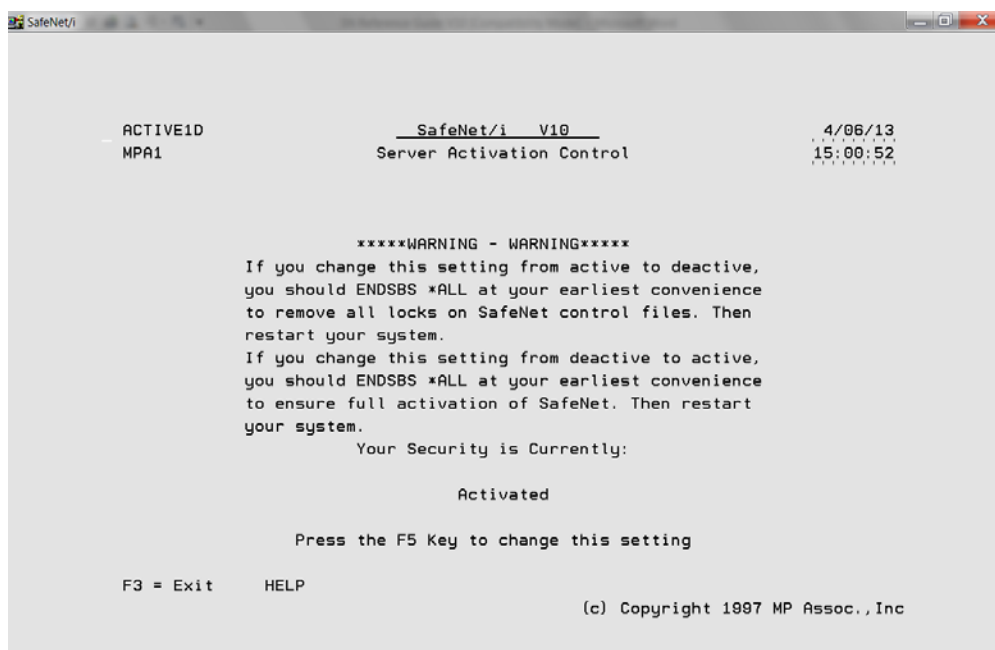
This will prevent the IBM i file server job from using **SafeNet/i** but continue to protect the other server jobs in IBM i with **SafeNet/i**. This way you can eliminate a performance problem or IBM i problem from one server but continue to protect your other access points with **SafeNet/i**.

To activate or de-activate SafeNet/i:

Remember, you must be a **SafeNet/i** Super Admin to perform this step.

1. From the Install Menu select **Option 50 - Activate/De-Activate SafeNet/i**

The *Server Activation Control* screen is displayed, indicating the current setting.



2. **Press F5** to change the setting and return to the Install Menu.
3. After performing these steps, end all subsystems then restart them to maintain security integrity.
4. Try your network request again. If **SafeNet/i** is active, and your request is not successful, review your request log and correct the problem based on the error code on the report.

Removing SafeNet/i from your system

If it becomes necessary to completely remove **SafeNet/i** from your IBM i, follow these steps.

1. Sign on to the system as QSECOFR or SAFENET.

2. De-activate **SafeNet/i**.

Follow the instructions on the previous pages to de-activate the program.

3. Exit all **SafeNet/i** menus

4. Remove PCSECLIB and PCSECDTA from your jobs library list

5. Put your system into a Restricted state.

ENDSBS *ALL *IMMED

6. After all the jobs have ended, restart your system. You can use

STRSBS QCTL

7. Delete library PCSECLIB and PCSECDTA

8. Delete the SAFENET authorization list from your system

SafeNet/i is now completely removed from your system.

Appendix A - SERVER FUNCTION DESCRIPTIONS

Original Servers

These servers have been provided by IBM since PC Support/400 became available. Support for these original servers was designed for and is still used to service the original clients: DOS, Extended DOS and OS/2.

Distributed Data Management

Description: Distributed Data Management - 100

Security checking is performed when a remote user or system accesses an IBM i file or issues an incoming remote command via DDM. The remote user must be authorized to perform the operation (open, close, read or write, for example) or the DDM request is rejected.

Where used: IBM i Access for Windows
Client Access for Windows
Client Access for OS/2
Client Access for DOS with Extended Memory
Client Access for DOS
IBM i to IBM i, System/38™ or System/36™ Communication

Server Identifier: *DDM

Format Name: *DDM

Levels Supported: Basic (Levels 1, 2,)
Intermediate (Level 3)
Advanced (Level 4)
Plus special setting for remote command processing
CL command authority checking is performed at Level 4

Limitations: - See the Special Jobs Menu for incoming remote commands
- Cannot check authority of files, objects or commands imbedded in the command string

Recommended Setting: Level 4, Log All

Notes:

1. Commands are allowed only if specified from Special Jobs Menu, Option 2 (**CHGSPCSET** command). DDM commands, NOT file requests, can be stopped by saying “NO” to *Allow DDM Commands* parameter. The **SafeNet/i** default is “YES” to allow commands. Review existing requirements prior to changing this setting. At Level 4, users must be authorized to commands.
2. Does not support *SPC type transactions.

3. For Version 4 of **SafeNet/i**, if *DDM is set to Level 4, you must authorize each user to the CL commands they may issue to the IBM i.
4. Most IBM i systems, by default, use the QUSER profile for the communications conversation. QUSER must have authority to all files that are being accessed and must be authorized to the *DDM server function.

To change from QUSER as the default, a change to the default communications entry must be made in the QCMN subsystem description. See your system administrator for assistance.

Original Data Queue Server

Description: Original Data Queue Server - 100

A data queue is an IBM i object that is used by IBM i application programs for communications. Applications can use data queues to pass data between jobs. Multiple IBM i jobs can send or receive data from a single data queue.

Where used: Client Access for Windows
Client Access for OS/2
Client Access for DOS with Extended Memory
Client Access for DOS

Server Identifier: *DQSRV

Format Name: DTAQ0100

Levels Supported: Basic (Levels 1, 2)
Intermediate (Level 3)
Advanced (Level 4)

Limitations: None

Recommended Setting: Level 1, Log All

Notes:

1. At Levels 3 and 4 users must be granted access to the server function.
2. At Level 4 users must be granted access to specific data queues and libraries.
3. Supports generic (wildcard) data queue names. (DATAQ* = all data queue names starting with the letters DATAQ)

Original Transfer Function Server

Description: Original File Transfer Function - 100

The Client Access transfer function transfers data between the IBM i system and a personal computer.

Where used: Client Access for Windows

- *PC5250 Transfers*
- *Automatic file transfer functions (RTOPCB, etc.)*
- *Interactive and automatic file transfer functions*
- *File transfer from within a RUMBA emulation session*

Server Identifier: *TFRFCL

Format Name: TRAN0100

Levels Supported:

Basic	(Levels 1, 2)
Intermediate	(Level 3)
Advanced	(Level 4)

Recommended Setting: Level 4, Log All

Notes:

1. Specific users must be granted access to the server function at Levels 3 and 4.
2. Users must be granted access to specific files and libraries at Level 4.
3. Supports generic (wildcard) file names. (FI* = all file names starting with the letters FI)
4. Full control of library, object and data rights allowed.
5. At Level 4, to select or extract a list of objects from within a library, you must enter the name of the library and use *ALL in the *Object or Sub-Flr* column. The user will need Read data rights to the library.

Example 1: To get a list of all files in *USRLIBL there must be an entry for the user requesting the list:

<u>Library or Folder</u>	<u>Object or Sub-Folder</u>	<u>Read</u>
*USRLIBL	*ALL	X

Example 2: To get a list of all files in the library PAYROLL enter:

<u>Library or Folder</u>	<u>Object or Sub-Folder</u>	<u>Read</u>
*PAYROLL	*ALL	X

6. CRTFILE(*YES) CRTMBR(*YES)

To do a “REPLACE” with a CREATE FILE(*YES) or a CREATE MEMBER(*YES), Existence Rights must be given to the user for the FILE/LIBRARY being created.

To do a “REPLACE” with a CREATE FILE(*NO) or CREATE MEMBER(*NO), Delete and Write Data Rights must be specified to the object.

Original License Management Server

Description: Original License Management Server - 100

The license management server ensures valid licenses are available for Client Access, IBM and non-IBM licensed applications when requested from a client. The license management server performs this process every time a Client Access client requests a license for an application, typically upon session initiation. When a Client Access client disconnects from the IBM i, the license is released and is available for another client to use.

Where used: Client Access for Windows
Client Access for OS/2
Client Access for DOS with Extended Memory
Client Access for DOS

Server Identifier: *LMSRV

Format Name: LICM0100

Levels Supported: Basic (Levels 1, 2)
Intermediate (Level 3)

Limitations: None

Recommended Setting: Level 1, Log All

Notes:

1. At Level 3 the user must be authorized to the server function.
2. Level 4 is not required or supported.

Original Message Server

Description: Original Message Server - 100

The message function server allows users to communicate with each other by sending messages. Users can communicate with other users at IBM i workstations or with users at personal computers that are attached to the IBM i system.

The message function server routes messages sent from PC users to the appropriate user and receives messages for PC users and sends them to the PC workstation.

Where used: Client Access for OS/2
Client Access for DOS with Extended Memory
Client Access for DOS

Server Identifier: *MSGFCL

Format Name: MESS0100

Levels Supported: Basic (Levels 1, 2)
Intermediate (Level 3)

Limitations: None

Recommended Setting: Level 1, Log All

Notes:

1. At Levels 3 and 4, the user must be authorized to the server function.
2. Generic (wildcard) names are supported for Level 4.

Original Remote SQL Server

Description: Original Remote SQL Server - 100

The remote SQL server processes requests that are received from Client Access products that are using the high-level language remote SQL API. The API allows applications running on the clients to run SQL statements on a remote IBM i system. The databases accessed may be either SQL database files or native IBM i database files.

Where used: Client Access for Windows
Client Access for OS/2
Client Access for DOS with Extended Memory
Client Access for DOS

Server Identifier: *RQSRV

Format Name: RSQL0100

Levels Supported: Basic (Levels 1, 2)
Intermediate (Level 3)
Advanced (Level 4)

Limitations: ODBC support on Windows 3.1 and Client Access for DOS with Extended Memory clients **DO NOT** use this server

Recommended Setting: Level 4, Log All

Notes:

1. Levels 3 and 4 require the user to be authorized to the server function.
2. Level 4 checks SQL statements and Object/Library for authority.
3. User must have authority to SQL statement and Object/Library.

Original Virtual Print Server

Description: Original Virtual Print Server - 100

The virtual print server is used to print data from PC application programs on IBM i printers.

Where used: Client Access for Windows
Client Access for OS/2
Client Access for DOS with Extended Memory
Client Access for DOS

Server Identifier: *VPRT

Format Name: Always Blanks

Levels Supported: Basic (Levels 1, 2)
Intermediate (Level 3)
Advanced (Level 4)

Limitations: None

Recommended Setting: Level 3 or 4, Log All

Notes:

1. At Levels 3 and 4 users must be authorized to the server function.
2. At Level 4, for each printer that is opened the user must have authority to the printer.

Example 1: To grant authority to all printers that begin with the letters PRT in library QUSRSYS enter:

<u>Library or Folder</u>	<u>Object or Sub-Folder</u>	<u>Read</u>
QUSRSYS	PRT*	X

Example 2: To grant authority to only the PAYROLL printer, enter:

<u>Library or Folder</u>	<u>Object or Sub-Folder</u>	<u>Read</u>
QUSRSYS	PAYROLL	X

Optimized Servers

This server support, provided by IBM with Client Access (now IBM i Access for Windows) beginning with OS/400 Version 3 Release 1, services optimized clients: Windows 3.1 (16 bit applications), Optimized OS/2 (32 bit applications) and Windows98, Windows 2000, Windows XP, Windows 7.

Additional servers are supplied by IBM for each new release of i OS.

Central Server - Client Management

Description: Central Server - client mgmt - 100

The central server provides the ability to update the client management database on the IBM i. IBM i Access for Windows uses this function when new or existing IBM iAccess clients attach to the server.

Where used: IBM i Access for Windows

Server Identifier: *CNTRLSRV

Format Name: ZSCS0100

Levels Supported: Basic (Levels 1, 2)
Intermediate (Level 3)

Limitations: None

**Recommended
Setting:** Level 1, Log All

Notes:

1. At Level 3 users must be authorized to the server function.
2. Level 4 is not required or supported.

Central Server - Conversion Map

Description: Central Server - conversion map - 100

The central server provides support for retrieving conversion maps for clients that need them. These conversion maps are usually used on the client for ASCII to EBCDIC conversions and EBCDIC to ASCII conversions.

Where used: IBM i Access for Windows

Server Identifier: *CNTRLSRV

Format Name: ZSCN0100

Levels Supported: Basic (Levels 1, 2)
Intermediate (Level 3)

Limitations: None

Recommended Setting: Level 1, Log All

Notes:

1. At Level 3 users must be authorized to the server function.
2. Level 4 is not required or supported.

Central Server - License Management

Description: Central Server - license mgmt - 100

The license management support provided by this server is very similar to the support in the original license management server for IBM i Access for Windows clients. The initial request from a client checks out a license for each IBM i Access for Windows user and the server remains active until the client is no longer communicating with the IBM i.

Where used: IBM i Access for Windows

Server Identifier: *CNTRLSRV

Format Name: ZSCL0100

Levels Supported: Basic (Levels 1, 2)
Intermediate (Level 3)

Limitations: None

Recommended Setting: Level 1, Log All

Notes:

1. At Level 3 users must be authorized to the server function.
2. Level 4 not required or supported.

DB2 for IBM i Database Access Request - DRDA

Description: DRDA DB2/400 Database Access Request

This server is used whenever a client requests a DRDA conversation connection.

Where used: Rumba Access
DB2 for IBM i™
DB2 for OS/390™
DB2 Connect™

And more . . .

Server Identifier: *DRDA

Format Name: *DRDA

Levels Supported: Basic (Levels 1, 2)
Intermediate (Level 3)

Limitations: None

**Recommended
Setting:** Level 3, Log All

Notes:

1. At Levels 3 and 4 users must be authorized to the server function.

Database Server - Data Base Access - 100

Description: Database Server - data base access - 100

This server function manipulates data base files on the IBM i. It allows operations to data base files, such as: create physical file, add database file member, delete file.

Where used:

IBM i Access for Windows

- *Access to IBM i database through ODBC interface*
- *File transfers*

Used by ODBC*, Microsoft Access* and Microsoft Query* for object manipulation

Used by functions

- Create source physical file
- Create database file, based on existing file
- Add, clear, delete database file member
- Override database file
- Delete database file override
- Delete file

Server Identifier:

*NDB

Format Name:

ZDAD0100

Levels Supported:

Basic	(Levels 1, 2)
Intermediate	(Level 3)
Advanced	(Level 4)

Limitations:

None

Recommended

Setting:

Level 4, Log All

Notes:

1. At Levels 3 and 4 users must be authorized to the server function.
2. Supports generic (wildcard) object names.

Database Server - Data Base Access - 200

Description: Database Server - data base access - 200

This server function enables the addition of library list entries.

Where used: IBM Client Access for Windows for Windows95
- Access to *IBM i* database through *ODBC* interface
- File transfers

Used by various ODBC, DRDA™, SQL packages such as Microsoft Access, Microsoft Query, etc.

Server Identifier: *NDB

Format Name: ZDAD0200

Levels Supported: Basic (Levels 1, 2)
Intermediate (Level 3)
Advanced (Level 4)

Limitations: - Does not support generic library names
- Does not support long object names

Recommended Setting: Level 4, Log All

Notes:

1. At Levels 3 and 4 users must be authorized to the server function.
2. At Level 4 the user must be granted authority for each library to add to the library list.

Database Server - Entry

Description: Database Server - Entry - 100

This server function is used at server initiation request. It is the request that always comes first. All other database server requests come after a request to this entry point. This is called whenever a new connection to the database server is started and a new QZDASOINIT job is initiated to service client database requests, such as calling a stored procedure.

Where used: IBM i Access for Windows
- Access to IBM i database through ODBC interface
- File transfers

Server Identifier: *SQL

Format Name: ZDAI0100

Levels Supported: Basic (Levels 1, 2,)
Intermediate (Level 3)

Limitations: None

Recommended Setting: Level 3, Log All

Notes:

1. At Level 3 users must be authorized to the server function.
2. **ALL DATABASE SERVER REQUESTS REQUIRE THIS SPECIFIC SERVER TO BE ACCESSIBLE.** A request to this server precedes all other kinds of database server requests.
3. Level 4 is not required or supported.

Database Server - Object Information - 100

Description: Database Server - object information - 100

This server function is used for requests to retrieve information about certain objects from the data base server.

Where used: IBM i Access for Windows
- *Access to IBM i database through ODBC interface*
- *File transfers*

Server Identifier: *RTVOBJINF

Format Name: ZDAR0100

Levels Supported: Basic (Levels 1, 2)
Intermediate (Level 3)
Advanced (Level 4)

Usage: Used to retrieve information for the following objects:

- Library (or collection)	- SQL package
- File (or table)	- SQL package statement
- Field (or column)	- File member
- Index	- Record format
- Relational database (or RDB)	- Special columns

Limitations: You must restrict access to the user's default library list through user profile parameter changes or i OS object security.

Recommended Setting: Level 4, Log All

Notes:

1. List retrievals from *USRLIBL automatically allowed.
2. Data rights enforced.
3. At Levels 3 and 4 users must be authorized to the server function.
4. At Level 4 the user must be authorized to the OBJECT/LIBRARY.

Database Server - Object information - 200

Description: Database Server - object information - 200

This server function is used for requests to retrieve additional information about certain objects from the data base server, such as primary and foreign key information.

Where used: IBM i Access for Windows
- *Access to IBM i database through ODBC interface*
- *File transfers*

Server Identifier: *RTVOBJINF

Format Name: ZDAR0200

Levels Supported: Basic (Levels 1, 2)
Intermediate (Level 3)

Usage: Used for requests to retrieve information for the following objects:
- Foreign keys - Primary keys

Limitations: - You must restrict access to the user's default library list through user profile parameter changes.

Recommended Setting: Level 3, Log All

Notes:

1. At Level 3 the user must be authorized to the server function.
2. Level 4 is not required or supported.

Database Server - SQL Access

Description: Database Server - SQL access - 100

Database Server – SQL access – 200 (for V4R1 and above)

This server function is used when certain SQL requests are received for the data base server.

The QIBM_QZDA_SQL2 exit point takes precedence over the QIBM_QZDA_SQL1 exit point. If a program is registered for the SQL2 exit point, it will be called, and a program for the SQL1 point will not be called.

Where used:

IBM i Access for Windows

- Access to IBM i database through ODBC interface
- File transfers

Called by these functions:

ALTER TABLE	DROP PACKAGE
CALL	DROP TABLE
COMMENT ON	DROP VIEW
COMMIT	GRANT
CREATE COLLECTION	INSERT
CREATE DATABASE	LABEL ON
CREATE INDEX	LOCK TABLE
CREATE TABLE	REVOKE
CREATE VIEW	ROLLBACK
DELETE	SELECT
DROP COLLECTION	SET TRANSACTION
DROP DATABASE	UPDATE
DROP INDEX	

Server Identifier: *SQLSRV

Format Name: ZDAQ0100
ZDAQ0200

Levels Supported: Basic (Levels 1, 2)
Intermediate (Level 3)
Advanced (Level 4)

Limitations: Does not check binary field or DBPKG/DBDLIB fields.

Recommended Setting: Level 4, Log All

Notes:

1. At Levels 3 and 4 users must be authorized to the server function.
2. At Level 4 the user must be authorized to the OBJECT/LIBRARY and the SQL statement. Data authority requirements are determined by the authorized SQL statements for the user.
3. Due to a restriction within IBM's OS/400 for **versions prior to V4R1**, OS/400 delivers SQL requests to **SafeNet/i** with a limit of 512 characters in length. Since most SQL statements are normally much less than this limit, this is not a concern for most users. However, if this limit is exceeded, **SafeNet/i** will log a truncated request string into the history file. For V4R1 and above, this restriction does not apply.

PTFs are available for earlier releases of OS/400 to enable long SQL strings. Contact IBM for details.

Data Queue Server

Description: Data Queue Server - 100

A data queue is an IBM i object that is used by IBM i application programs for communications. Applications can use data queues to pass data between jobs. Multiple IBM i jobs can send or receive data from a single data queue.

Where used: IBM i Access for Windows

Server Identifier: *DATAQSRV

Format name: ZHQ00100

Levels Supported:	Basic	(Levels 1, 2)
	Intermediate	(Level 3)
	Advanced	(Level 4)

Limitations: None

Recommended Setting: Level 1, Log All

Notes:

1. At Levels 3 and 4 users must be granted access to the server function.
2. At Level 4 users must be granted access to specific data queues and libraries.
3. Supports generic (wildcard) data queue names. (DATAQ* = all data queue names starting with the letters DATAQ)

DHCP Address Binding Notify

Description: DHCP Address Binding Notification - 100

This server assigns IP addresses to specific client hosts.

Where used: Any device on a TCP/IP network whenever it requests an IP address from the IBM i when the IBM i is set to be the local network DHCP server

Server Identifier: *DHCPB

Format name: DHCA0100

Levels Supported: Basic (Level 1)

Limitations: None

Recommended Setting: Level 1, Log All

DHCP Address Release Notify

Description: DHCP Address Release Notification - 100

This server releases an IP address from its specific client host assignment binding.

Where used: Any device on a TCP/IP network whenever it requests an IP address from the IBM i when the IBM i is set to be the local network DHCP server

Server Identifier: *DHCPR

Format name: DHCR0100

Levels Supported: Basic (Level 1)

Limitations: None

Recommended Setting: Level 1, Log All

File Server

Description: File Server - 100

The file server function allows clients to store and access information, such as files and programs, on the IBM i in various formats. This server replaces the shared folder type 2 server that was used prior to Version 3 Release 1. The i OS file server interfaces with the integrated file system on the IBM i. It provides file serving capabilities equivalent to shared folders, but also allows clients to access information in any of the new file systems within operating system.

Where used: IBM i Access for Windows
- *Access to entire file system*
- *Windows Explorer and other applications*

Server Identifier: *FILESRV

Format Name: PWFS0100

Levels Supported: Basic (Levels 1, 2)
Intermediate (Level 3)
Advanced (Level 4)

Limitations:

- Directory structure has a maximum of 20 deep
- Does not differentiate between upper and lower case file names
- Does not support long file names. Names over 10 characters are truncated
- Allows setting of global authority to IBM supplied folders and file systems
- Authority is granted to a folder and all data that it contains.
Different object/file authorities within the same folder is not available.

Recommended Setting: Level 4, Log All

Notes:

1. When set to Levels 3 or 4, each IBM i Access for Windows user must be specifically authorized to this server to access their shared folder and update functions.
2. To grant authority to all folders and all file systems use:

<u>Library or Folder</u>	<u>Object or Sub-Folder</u>
*ALLFLR	*ALL

To enter *ALLFLR/ *ALL you must be signed on as QSECOFR.

Proper Data Rights must be selected also.

3. At Level 4, to authorize a user for access to a non-IBM folder within the QDLS file system (shared folders), you must enter two records in the OBJECT/USER security file.

Example 1: A user requires access to a folder called PERSONNEL within QDLS.

Network Request: /QDLS/PERSONNEL

Entries Required:

	<u>Library or Folder</u>	<u>Object or Sub-Folder</u>	<u>Read</u>
Entry #1	QDLS	PERSONNEL	X
Entry #2	PERSONNEL	*ALL	X

Example 2: You can add specific folder names in place of *ALL to further extend the directory path.

Network Request: /QDLS/PERSONNEL/PAYROLL/SALARY

Entries Required:

	<u>Library or Folder</u>	<u>Object or Sub-Folder</u>	<u>Read</u>
Entry #1	QDLS	PERSONNEL	X
Entry #2	PERSONNEL	*ALL	X
Entry #3	PAYROLL	SALARY	X
Entry #4	SALARY	*ALL	X

4. This is a typical IBM i Access for Windows user security set up if automatic read to IBM folders is not enabled (found on Special Jobs Menu, Option 2):

<u>Library or Folder</u>	<u>Object or Sub-Folder</u>	<u>Read</u>
QDLS	QIWSFLR	X
QIWSFLR	*ALL	X

5. **SafeNet/i** does not support the full long file names or lower case names, SafeNet/i will truncate each request to a maximum of 10 characters. To allow access to file systems

Qopensys, Qfilesys.400 and home, key in the first 10 positions of each file system name only.

Example:

Network Request: /Qfilesys.400/QSYS.LIB/PAYROLL.LIB/SALARY.FIL

Entries Required:

	<u>Library or Folder</u>	<u>Object or Sub-Folder</u>	<u>Read</u>
Entry #1	QFILESYS.4	QSYS.LIB	X
Entry #2	QSYSLIB	PAYROLL.LI	X
Entry #3	PAYROLL.LI	SALARY.FIL	X

SafeNet/i will convert all requests to uppercase, then check the first ten characters in each directory name for a match.

Note: When native libraries or objects are accessed via the file server, .LIB, .file, etc. are added to the end of the name. You must enter the .LIB or .file in the user to object control file. If the same user accesses these same objects through another server also, (SQL, for example) you must also enter the authorities without the .LIB and .file.

Example:

For the path through the file server: home/TEST.LIB/abc.file you must enter:

<u>Library</u>	<u>Object</u>	<u>Auth</u>
home	TEST.LIB	X
TEST.LIB	*ALL	X

For SQL or other access you also need:

<u>Library</u>	<u>Object</u>	<u>Auth</u>
TEST	*ALL	X

FTP Client Request Validation

Description: FTP Client Request Validation

This function is used whenever the IBM i is a client, issuing FTP commands to a remote system.

Where used: IBM i command lines, interactive and batch jobs can initiate an FTP client request

Server Identifier: *FTPClient

Format Name: VLRQ0100

Levels Supported:	Basic	(Level 1, 2)
	Intermediate	(Level 3)
	Advanced	(Level 4)

Usage Notes/Limitations:

At Level 3 or Level 4 you can implement IP address controls. This will allow you to limit what target addresses/systems an FTP client can connect to. See commands:

CHGFTPSET IPCTLC(*YES) and WRKTCPIPA *FTPCLIENT

You can also review 'Setting up TCP/IP Address Controls' in Chapter 3 of this guide.

Recommended

Setting: Level 4, Log All

Important Note:

When the FTP Client point is set to Level 4, only the GET and PUT FTP sub-commands are required. The other commands, when using the FTP Client, are for the TARGET SYSTEM ONLY (sent to/run on the target system).

When authorizing users to the GET/PUT sub-commands, the assumed object authority is reversed from authorities required for the FTP Server point and the same objects.

See the following examples.

Using FTP Client:

- Sending an object to a remote system
An FTP PUT of object ABC in an FTP Client session requires *READ authority to object ABC on the local machine.
- Get an object from a remote system
An FTP GET of object ABC in an FTP Client session requires *OBJMGT authority to the object ABC on the local machine.

Using FTP Server:

- Send an object to local system
An FTP PUT of object ABC in an FTP Server session requires *OBJMGT authority to the object ABC on the LOCAL machine.
- Get an object from the local system
An FTP GET of object ABC in an FTP Server session requires *READ authority to the object ABC on the LOCAL machine.

FTP Logon Server

Description: FTP Logon Server 1 - 100

This server is used any time the IBM i answers an FTP start request from another system or user. It is available in OS/400 versions V3R7 through V4R1

Where used:	Internets and Intranets MS Windows DOS And most other operating systems	
Server Identifier:	*FTPLOGON	
Format Name:	TCPL0100	
Levels Supported:	Basic Intermediate	(Level 1, 2) (Level 3)
Limitations:	None	
Recommended Setting:	Level 3, Log All	

FTP Logon Server

Description: FTP Logon Server 2 - 200

This server is used any time the IBM i answers an FTP start request from another system or user. It is available in OS/400 versions V4R2 and above.

Where used:	Internets and Intranets MS Windows DOS And most other operating systems	
Server Identifier:	*FTPLOGON2	
Format Name:	TCPL0200	
Levels Supported:	Basic Intermediate	(Level 1, 2) (Level 3)
Limitations:	None	
Recommended Setting:	Level 3, Log All	

FTP Logon Server

Description: FTP Logon Server 3 – 300

This server is used any time the IBM i answers an FTP start request from another system or user. It is available in OS/400 versions V5R1 or above.

Where used:	Internets and Intranets MS Windows DOS And most other operating systems	
Server Identifier:	*FTPLOGON3	
Format Name:	TCPL0300	
Levels Supported:	Basic Intermediate	(Level 1, 2) (Level 3)
Limitations:	None	
Recommended Setting:	Level 3, Log All	

FTP Server Request Validation

Description: FTP Server Request Validation

This function is used whenever the IBM i receives an FTP command it must act upon.

Where used: Internets and Intranets
MS Windows
And most other operating systems

Server Identifier: *FTPSERVER

Format Name: VLRQ0100

Levels Supported: Basic (Level 1, 2)
Intermediate (Level 3)
Advanced (Level 4)

Limitations: None

Recommended Setting: Level 4, Log All

Notes:

1. At Level 4, users must be authorized to the objects and the FTP statements they require and the CL commands they may issue to the IBM i.
3. Only at Level 4 are 'ANONYMOUS' logons allowed. This is in conjunction with the special FTP security settings. See Chapter 4 in this guide, 'Setting up FTP' (**CHGFTPSET** command).
4. You can limit FTP connections from specific IP Addresses. See commands:

CHGFTPSET IPCTL(*YES) and WRKTCPIPA *FTPSERVER

You can also review 'Setting up TCP/IP Address Controls' in Chapter 3 of this guide.

Network Print Server - Entry

Description: Network Print Server - entry - 100

This server function is used when the network print server is started.

Where used: IBM i Access for Windows

Server Identifier: QNPSEVR

Format Name: ENTR0100

Levels Supported: Basic (Levels 1, 2)
Intermediate (Level 3)

Limitations: None

**Recommended
Setting:** Level 3, Log All

Notes:

1. At Level 3 users must be granted access to the server function.
2. Level 4 is not required or supported.

Network Printer Server - Spool File

Description: Network Print Server - spool file - 100

This server function is used after the network print server receives a request to process an existing spooled output file.

Where used: IBM i Access for Windows

Server Identifier: QNPSEVR

Format Name: SPLF0100

Levels Supported: Basic (Levels 1, 2)
Intermediate (Level 3)
Advanced (Level 4)

Limitations: Level 4 grants spool file management rights to the owner of the spool file only.

Recommended Setting: Level 4, Log All

Notes:

1. At Levels 3 and 4 users must be granted access to the server function.
2. Level 4 requires no special set up. (see Limitations above)
3. No specific object authorizations required.

Pre-Power Down

Description: Pre-Power Down Server

This program is called whenever the PWRDWNSYS or ENDSYS command is issued

Where used: Any interface, command line or program that can issue the PWRDWNSYS or ENDSYS command

Server Identifier: PWRDWN

Format Name: PWRD0100

Levels Supported: Basic (Level 1)

Limitations: None

Recommended Setting: Level 1

Notes:

1. To use the pre-power down program call, create a CL program called PWRDWNCL.

Remote Command and Distributed Program Call Server

Description: Remote Command/Program Call - 100

The remote command and distributed program call server is provided to allow client users and applications to issue IBM i CL commands and call programs.

Where used: IBM i Access for Windows

Server Identifier: *RMTSRV

Format Name: CZRC0100

Levels Supported: Basic (Levels 1, 2)
Intermediate (Level 3)
Advanced (Level 4)
And special global control setting

Limitations: Cannot check Library/Object security on imbedded command strings

Recommended Setting: Level 4, Log All

Notes:

1. For X-1002 Remote Command Call, the same rules apply here as for *DDM commands. You must use the Special Jobs Menu to allow or reject remote commands entering via this server. In addition, see Note 3 below.

One setting controls both *RMTSRV X-1002 and *DDM command servers.

2. Used by System i Navigator for system object access.

Each GUI request from system object access triggers a program call. Most are in QUSRSYS or QGY libraries. By allowing QGY/*ALL and QUSRSYS/*ALL Read Data Rights, you let users access GUI interfaces.

3. At Level 4 you must authorize each user to the CL commands they may issue through this server.

REXEC Logon Server

Description: REXEC Logon Server 1 - 100

This server is used to validate a client request to start the REXEC Server. It is available in all versions of i OS.

Where used: Windows and OS/2 Desktop Add-in Applications
Other Clients using REXEC Applications

Server Identifier: *REXLOGON

Format name: TCPL0100

Levels Supported: Basic (Levels 1, 2)
Intermediate (Level 3)

Limitations: None

Recommended Setting: Level 3, Log All

Usage Notes:

You can limit FTP connections from specific IP Addresses. See commands:

CHGFTPSET IPCTL(*YES) and WRKTCPIPA *FTPSEVER

You can also review 'Setting up TCP/IP Address Controls' in Chapter 3 of this guide.

REXEC Logon Server

Description: REXEC Logon Server 2 - 200

This server is used to validate a client request to start the REXEC Server. It is available in OS/400 versions V5R1 and above.

Where used: Windows and OS/2 Desktop Add-in Applications
Other Clients using REXEC Applications

Server Identifier: *REXLOGON2

Format name: TCPL0300

Levels Supported: Basic (Levels 1, 2)
Intermediate (Level 3)

Limitations: None

Recommended Setting: Level 3, Log All

Usage Notes:

You can limit FTP connections from specific IP Addresses. See commands:

CHGFTPSET IPCTL(*YES) and WRKTCPIPA *FTPSERVER

You can also review 'Setting up TCP/IP Address Controls' in Chapter 3 of this guide.

REXEC Request Validation Server

Description: REXEC Request Validation Server

This server is initiated whenever a client issues a REX statement to the IBM i.

Where used: Windows and OS/2 Desktop Add-in Applications
Other Clients using REXEC Applications

Server Identifier: *REXSERVER

Format name: VLRQ0100

Levels Supported: Basic (Levels 1, 2)
Intermediate (Level 3)
Advanced (Level 4)

Limitations: None

**Recommended
Setting:** Level 3, Log All

Usage Notes:

You can limit FTP connections from specific IP Addresses. See commands:

CHGFTPSET IPCTL(*YES) and WRKTCPIPA *FTPSERVER

You can also review 'Setting up TCP/IP Address Controls' in Chapter 3 of this guide.

ShowCase™ Validation Server

Description: Showcase Validation Server

This server is initiated by a client utilizing the Showcase™ product with the proper exit point added to i OS.

Please follow the instructions from Showcase™ to properly register the ShowCase Exit Program. You MAY have to use the ADDEXITPGM command to add the exit point for ShowCase™ to your IBM i Server.

Where used: Any client utilizing Showcase™ Application

Server Identifier: *SHOWCASE

Format name: SRCS0100

Levels Supported:

Basic	(Levels 1, 2)
Intermediate	(Level 3)
Advanced	(Level 4)

Limitations: None

**Recommended
Setting:** Level 4, Log All

****Important Notes on setting up a user for ShowCase****

Although Showcase uses SQL statements to access i OS data, SafeNet/i does NOT verify the SQL statement authority. SafeNet/i ONLY verifies the user to server and user to objects. The SQL Statement is NOT interrogated for authority. If the user issues a SELECT statement, the object authority required is *READ. If the user issues a DELETE statement, data *DELETE authority is required.

You DO NOT have to set up SQL statement authority for the Showcase users.

Spooled File Security

Description: Spooled File Security - 100

The spooled file security exit point allows SafeNet/i to control access to spooled files in specific output queues.

This is a system-wide setting. Once an exit program is assigned to the exit point all system OUTQ activity will call the exit program. If the SafeNet/i security level for this server is at level 3 or higher, SafeNet/i will perform additional security lookups.

Where used: During any access to output queues or spooled files, whether remote or via 5250 emulation

Server Identifier: *SPLAUT

Format Name: SPSY0100

Levels Supported:	Basic	(Level 1, 2)
	Intermediate	(Level 3)
	Advanced	(Level 4)

Limitations: This exit point is available on IBM i V7.1 and above

Recommended Setting: Level 1, Log None – unless additional output queue control is required by your installation

Usage Notes:

Exit point QIBM_QSP_SECURITY gives SafeNet/i the ability to control access to spooled files in individual output queues.

1. At Level 1, the default, no spooled file activity will be logged
2. At Level2, no access to ANY OUTQ except spool file creations
3. At Level3, IF the specific entry of OutQ_Lib/OutQ_Name is found for ANY user in the WRKUSROBJ control file, the user who is accessing the spool file within the output queue MUST have *SPLAUT server authority

To clarify, once you have added QGPL/QPRINT as a specific entry using the WRKUSROBJ command, ALL access to entries within that OUTQ are restricted to only those system users who have been assigned the *SPLAUT server in SafeNet/i (WRKUSRSRV). If someone does not have *SPLAUT authority in SafeNet/i, they will have no access to the spool files on that specific output queue.

4. At Level 4, Level 3 rules apply. In addition, the user must have the specific data or management rights assigned.

For instance, if the user is trying to delete a spooled file in the output queue, they must have Delete Rights to the OUTQ/LIB assigned with WRJUSROBJ.

Example: A user is trying to delete a spool file in QGPL/QPRINT OUTQ

- Spooled File Security Server set to level 1
 - a. If logging for server point is on, record is logged; otherwise, accept and continue
- Spooled File Security Server set to level 3
 - a. Check to see if an entry is found for QGPL/QPRINT for any user. If found the OUTQ is restricted. Next, check for the specific user-to-server *SPLAUT. Check group profiles for specific *SPLAUT entry.
 - b. If found, accept
- Spooled File Security Server set to level 4
 - a. Perform level 3 checks
 - b. Check specific user-to-object QGPL/QPRINT entry and check required Read or Management authority
 - c. Check group profiles to specific object entry (QGPL/QPRINT) and check required authority

Notes and Exclusions:

The exit programs will be called at the beginning of each IBM i spool command or API, except under any of the following conditions:

1. The job or thread has spool control (*SPLCTL) special authority. The special authority may originate from the user profile, group profile, or adopted authority.

2. The job or thread has job control (*JOBCTL) special authority and the spooled file resides on an output queue with OPRCTL(*YES). The special authority may originate from the user profile, group profile, or adopted authority.
3. The command or API is executed in a system job (including SCPF), a subsystem monitor job, or any job that is running under one of the following system user profiles:

QUATPROF	QNETSPLF
QCLUMGT	QNFSANON
QCOLSRV	QNTF
QDBSHR	QPEX
QDBSHRDO	QPM400
QDFTOWN	QRJE
QDIRSRV	QSNADS
QDLFM	QSPL
QDOC	QSPLJOB
QDSNX	QSRVAGT
QFNC	QSYS
QGATE	QTCP
QLPAUTO	QTFTP
QLPINSTALL	QTSTRQS
QMSF	

TCP Signon Server

Description: TCP Signon Server - 100

The sign-on server provides security for clients that use TCP/IP communications support. This security function prevents access to the IBM i for users with expired passwords or allows entry to only specific users.

Where used: IBM i Access for Windows

Server Identifier: *SIGNON

Format Name: ZSOY0100

Levels Supported: Basic (Level 1, 2)
Intermediate (Level 3)

Limitations: None

Recommended Setting: Level 1, Log All

Notes:

1. Level 3 requires specific authority to the server function.
2. Level 4 is not required or supported.

TELNET Device Initialization

TELNET Device Termination

Description: TELNET Device Initialization - *TELNETON
TELNET Device Termination - *TELNETOFF

The TELNET servers provide for security when using TCP/IP and TELNET clients. This point allows the restriction by IP address and password type. Auto-sign-on can also be configured. TELNET Device Termination allows for session logging and device management upon session termination. *TELNETOFF is dependent upon the setting of *TELNETON.

Where used: Any TN5250 (TELNET client)
MS Windows
IBM i Access for Windows

Server Identifier: *TELNETON
*TELNETOFF

Format Name: INIT0100
TERM0100

Levels Supported: Basic (Level 1, 2)
Intermediate (Level 3)

Limitations: See Chapter 3 in this guide, 'TELNET, TCP/IP Address Controls'

Recommended Setting: Level 3, Log All

Notes:

1. Level 3 requires correct IP addressing in control file (WRKTCPIPA *TELNET)
2. You can limit FTP connections from specific IP Addresses. See commands:

CHGFTPSET IPCTL(*YES) and WRKTCPIPA *FTPSERVER

You can also review 'Setting up TCP/IP Address Controls' in Chapter 3 of this guide.

TFTP Server Request Validation

Description: TFTP Server Request Validation

Clients utilizing TFTP (Trivial File Transfer Protocol), such as the IBM Net Station use this server.

Where used: IBM Net Station Boot

Server Identifier: *TFTPSRVR

Format name: VLRQ0100

Levels Supported: Basic (Levels 1, 2)
Intermediate (Level 3)

Limitations: None

Recommended Setting: Level 3, Log All

User Profile Servers

Description: Add User Profile
Change User Profile
Delete User Profile
Restore User Profile

These servers are called each time a user profile command is issued.

Where used: Any interface or command line that can issue a user profile associated i
OS command

Server Identifier:	Format:
*CHGPRF	CHGP0100
*CRTPRF	CRTP0100
*DLTPRFA	DLTP0100
*DLTPRFB	DLTP0200
*RSTPRF	RSTP0100

Levels Supported: Basic (Levels 1)

Limitations: None

**Recommended
Setting:** Level 1, Log All

Notes:

1. This point simply logs which user profile was affected, who performed the action, and when it was done.

INDEX

A

Administrator 1.3
Alert notification 9.9, 10.1, 10.2
Anonymous 4.2, 4.3, 4.4, 4.5
Anonymous FTP 4.6
Authorities
 User to CL commands 1.19
 User to FTP Statements 1.16
 User to Objects 1.9
 User to SQL Statements 1.14
Auto signon 3.5

B

Backup procedure 7.7

C

CHGFTPSET 4.2
Commands 9.9
Customer Exit Programs 2.11, 9.3

D

De-activating SafeNet/400 13.1
DHCP 11.1
Distribution lists 10.2

E

ENDTRP 7.2, 7.7, 9.9
Error Codes 12.8
Exclusions 1.11, 1.12, 1.26, 1.27, 1.28
Exit points 2.11, 9.3

F

Files
 Contained in SafeNet 9.7
FTP 1.16, See Chapter 4

H

Help 6.11
Historical transactions 5.4, 6.1, 6.2, 6.7, 6.8
History file 24, See also TRAPOD

I

IP address controls 3.7
IP addresses 11.6

L

Level 5 Re-set 9.3
Logging Levels 1.6, 2.4
Long path name 1.21, 5.2

M

MAC address 11.5

P

PCREVIEW 6.11, 6.12, 9.9, 12.3, 12.4, 12.10
PCTESTR 6.1, 6.2, 6.10, 9.9
Ping 11.8
Pre-Power Down Program Point 9.4
PTF 12.1
Purges
 DHCP addresses 11.7
 TRAPOD 7.1

R

Rejections See Error Codes
Removing SafeNet/400 13.3

S

Servers 2.1
 Logging Levels 1.6, 2.4
 Optimized 12
 Original 1
 Recommended Levels 2.6
 Security Levels 2.2
Settings
 Server 2.6, 5.1, 6.8
 Special 9.9
ShowCase Strategy 45
Super Admin 1.3
Super Trusted Users 1.5

T

TCP/IP 2.2, 3.7, 49, 50, See Chapter 3, See Chapter 3
TELNET See Chapter 3

Testing your settings.....	6.1, 6.10
Time of Day	1.26, 6.3
TRAPOD	2.11, 3.6, 7.1, 7.2, 7.3, 9.8, 12.10
Purging.....	7.1, 7.4
Troubleshooting.....	13.1

U

User Profiles	
*PUBLIC.....	1.7, 1.9, 1.12, 1.13, 1.14, 1.16, 1.19, 1.21

Swapping.....	9.5, 9.6, 12.9
Users	
Copying	1.23
Removing	1.23
Security Levels	1.7
Setting logging levels.....	1.6

W

WRKUSRSEC.....	1.25
----------------	------



Información del Distribuidor

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