

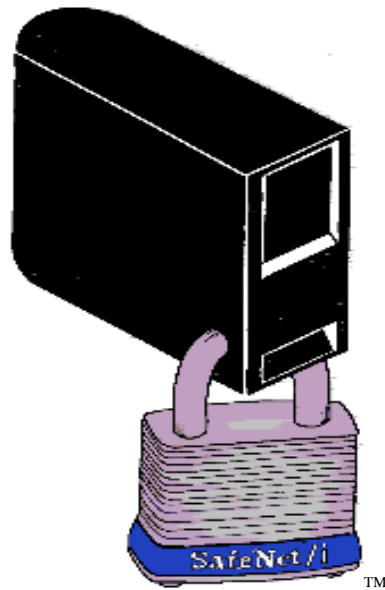
SAFENET/i

FOR IBM i

MEMO TO USERS

Changes Included in PTF 10.25

Version 10.25



How to contact us

Direct all inquiries to:

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

Phone: (518) 897-5002

Fax: (518) 897-5003

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

CHANGES TO SAFENET IN VERSION 10.25 1
IP ADDRESS CONTROLS ENHANCEMENT..... 2
SETTING UP SAFENET FOR IP CONTROL..... 3
IP CONTROL PROCESS FLOW..... 4
NEW SAFENET COMMANDS 6

SafeNet/i

Memo to Users

Changes to SafeNet/i in Version 10.25

This document outlines the changes included in SafeNet/i Version 10.25.

Special Note to customers who currently use SafeNet/i IP Address controls for FTP:

Make sure you review the “Prerequisites” section on page 3 for the steps you **MUST** consider before installing this update.

Exit Point Server IP Address Controls

Prior to this PTF, SafeNet/i allowed IP controls for the FTP and TELNET host servers only. To adapt to changing system security requirements, the IP address Controls within SafeNet/i have been enhanced.

With this release of SafeNet/i Version 10.25, it is now possible to control most Exit Point servers by source IP address and User IDs.

- Enhancements to IP Address Controls, Maintenance Programs and Reports
 - New commands added
 - WRKSRVIP - Work with Server IP Addresses
 - WRKUSRIP - Work with Authorized IP Addresses for User
 - PRTUSRIP - User to IP Address Listing
 - PRTIPUSG - IP Address Usage Report
- Enhancements to TELNET Controls to optionally restrict access only to SSL connections

New type of SafeNet/i Administrator for Read Only

- These users will be able to view all the SafeNet/i settings and screens, but will not be able to make any changes. Using the Work with SafeNet/i Administrator command (WRKSNADM), you can specify SafeNet/i Administrators as Read-Only.

IP Address Controls Enhancement

New Options for IP Address Controls

CHGSPCSET – Change SafeNet/i Special Settings

A new parameter has been added

CTLBYIP - Will access to any Exit Point Servers be controlled by IP addresses?

- ***NO** (default) - No IP address controls will be used within SafeNet/i
- ***YES** - Some Exit points may have access controlled by IP addresses within SafeNet/i

WRKSRV - Server Security Settings

A new field parameter for switching ON/OFF the SafeNet/i IP controls by Exit Point has been added

- **N (No/Off)** (default) – This Exit Point Server access is NOT controlled by IP address
- **Y (Yes/On)** – This Exit Point may have IP address controls active within SafeNet/i

WRKUSRIP – Work with Authorized IP Addresses for User

New command to Work with User to IP address entries

- Add an entry for each server to be controlled by IP
- Can specify *Reject the operation if required
- Supports Group profiles and *Public entries

WRKSRVIP – Work with Server IP Addresses

New command and maintenance screen to manage the Users and IP addresses at the server level

- Enter all the users at once for a specific server's IP entries
- Copy all at once the entries from one server to another

PRTIPUSG – IP Address Usage Report

A new usage report has been added. Print IP Usage. This will assist you in reviewing historical data for IP addresses by User and Server.

Pre-Requisite for IP Controls

1. This function can be activated only at SafeNet/i security levels of 3 or 4 (Medium or High) for each exit point server that supports IP controls. See *WRKSRV* maintenance screens.
2. This enhancement will make **OBSOLETE** all prior SafeNet/i **FTP** IP address control maintenance and implementation. If your installation currently utilizes SafeNet/i IP Controls you will have to convert any entries to this new IP address format immediately after upgrading to this newer version.

BEFORE upgrading to this version of SafeNet/i, you should print the TCP/IP Address Control Listing on your current version. You will need this report to re-enter the IP controls into this new version. Use the *PRTTCPIPA* command to print the report.

3. This enhancement does NOT impact the current TELNET IP address controls in SafeNet/i. Any TELNET IP address control entries will remain in effect after upgrading to this newer version of SafeNet/i.

Setting Up SafeNet/i for IP Control

There are three steps to implementing the IP Controls in SafeNet/i:

1. Set up source IP address for each user
 - For each Server you want to control access by source IP address, set up each user's associated source IP address. Use *WRKUSRIP* or *WRKSRVIP* commands.
You may also use Group and *Public profile entries if you wish.
2. Turn **ON** IP address checking for each server
 - Use *WRKSRV* to work with the server settings.
 - Each server that supports IP address controls will be indicated by the column listed as "IPA".
 - Set the desired servers to Y for IP control (column IPA)

Note: You can only turn ON servers for IP Control if their current security Level is 3 or above.

3. Turn **ON** the Global IP control setting on the Change SafeNet/i Special Settings command
 - *CHGSPCSET CTLBYIP(*YES)*

IP Control Process Flow

This applies to every transaction for certain exit points set to SafeNet/i Security Level 3 or higher

BEGIN: Check **CHGSPCSET CTLBYIP** to see if global function is ***YES/*NO**

If ***NO** - Allow

> Exit IP checking process

If ***YES** - Continue Checking

> Check the "Specific Exit Point" for status of IP checking.



If ***NO** (IP checking is not active at the server level) - Allow

> Exit IP checking process

If ***YES** (IP checking IS active at the server level) – Continue IP checking

> Check if **ANY** IP address is present for this exit point server



If IP addresses are **NOT PRESENT** for this server- Allow

> Exit IP checking process

If IP addresses are **PRESENT** – Continue ip checking

> Check the UserID & Source IP for an authorized IP address.

If UserID is found **IN** IP address Range with **REJECTION** Entry

> Reject and Exit process



If UserID is found **AND IN** the IP Range - Allow

> Exit IP checking process

If UserID is **NOT** found– Continue IP checking

> Check the GroupID & Source IP for an authorized IP address for this exit point server



If GroupID is found **IN** IP address Range with **REJECTION** Entry

> Reject and Exit process

If GroupID is found **AND IN** the IP Range - Allow

> Exit IP checking process



If GroupID **NOT** found – Continue ip checking

Check the ***PUBLIC** & Source IP for an authorized IP address

If ***PUBLIC** is found in the IP address Range with **REJECTION** Entry

> Reject and Exit process



If ***PUBLIC** is found **AND** in the IP Range - Allow

> Exit IP checking process

If Source IP **NOT** found –Reject

> **Exit SafeNet/i with Rejection**

NOTES:

1. Valid IP Range is 0.0.0.0 thru 255.255.255.254
2. Wildcard IP entries(ALL IP addresses) are entered as: 0.0.0.0 thru 255.255.255.254
3. All Source IP addresses will be validated against an IP address Range (FROM – TO).
4. Some requests may show as having a source IP of 127.0.0.1 or even a blank IP address. This is normal for some IPL and internal processes. Any access thru the loopback device address will be automatically accepted by SafeNet/i.

New SafeNet/i Commands

1. Work with Server IP Controls (WRKSRVIP)

Option 5 on Menu SN1

```
Work with Server IP Addresses (WRKSRVIP)

Type choices, press Enter.

Enter Server ID . . . . . _____ Exit Point Server Short Name
```

Use F4 to see a list of valid server function names

```
Specify Value for Parameter SERVER

Type choice, press Enter.

Type . . . . . : CHARACTER
Enter Server ID . . . . . _____

*DDM *DATAQSRV
*DRDA *RMTSRV
*DQSRV *SIGNON
QNPSERV *SHOWCASE
*FILESRV
*RQSRV
*TFRFCL
*FTPCLIENT
*FTPLGON3
*REXLOGON2
*TFTPSRVR
*VPRT
*SQL

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

Enter the name of the server function to work with

```
Work with Server IP Addresses (WRKSRVIP)

Type choices, press Enter.

Enter Server ID . . . . . > *FTPCLIENT Exit Point Server Short Name
```

Enter the user profiles and IP addresses to be controlled

```
IP2SETD          SafeNet/i V10          4/08/15
MPADEV          Authorized IP Addresses for Server: 15:22:55
                FTP Client Request Validation
                *FTPCLIENT VLRQ0101

Options
3=Copy 4=Delete
7=View User Entries |-----Target Address Range-----| Accept
                Profile From IP Address To IP Address Reject
-   SAFENET 0.0.0.0 255.255.255.254 A
-   _____
-   _____
-   _____
-   _____
```

2. Work with User to IP addresses (WRKUSRIP)

Option 7 on Menu SN7

Enter a specific User Profile, *PUBLIC or *ALLDFN to see all currently defined users on the *Work with Authorized IP Addresses by User* screen

```

IPSET3D                               SafeNet/i   V10                               4/08/15
                                      Maintain Authorized IP Addresses          15:26:44

Type choice, press Enter.

User Profile . . . . . SAFENET Character value, *ALLDFN
  
```

```

IP3SETD                               SafeNet/i   V10                               4/08/15
MPADEV                               Authorized IP Addresses for User: SAFENET  15:28:24
                                      Safenet Profile

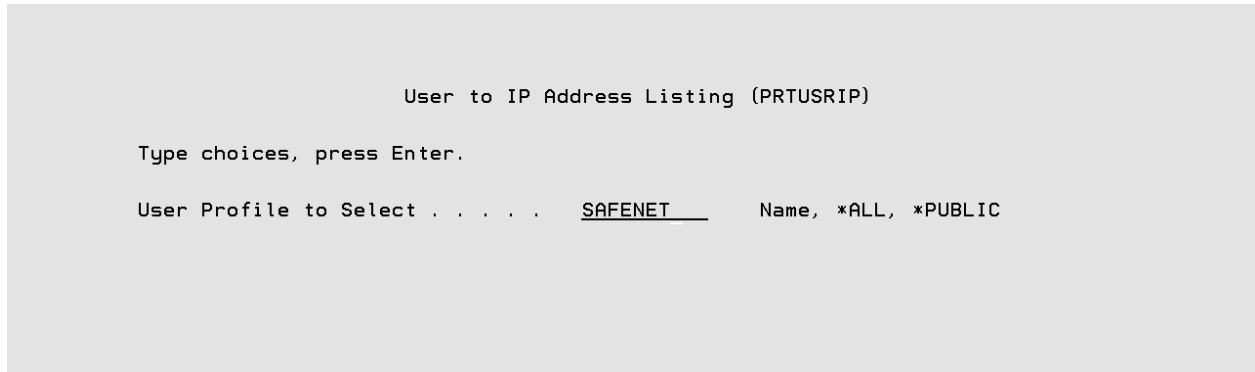
Options
3=Copy 4=Delete

  |-----Range-----| Accept or
  |-----|            | Reject? (A/R)
  Opt  Server  From IP Address  To IP Address
  ---  *DDM    10.242.1.2      10.242.1.2      A
  ---  *FILESRV 0.0.0.0          255.255.255.254 A
  ---  *FTPCLIENT 0.0.0.0        255.255.255.254 A
  ---  *FTPLOGON3 0.0.0.0        255.255.255.254 A
  ---  _____  _____  _____  _____  -
  
```

3. Print User to IP Address Control List (PRTUSRIP)

Option 8 on Menu SN3

Select the User Profile you want to print



Resulting Report

User Id	ServerID	From/To IP	Accept/Reject	Page-Run By-SAFI

SAFENET Group-		Safenet Profile		
	*DDM	10.242.1.2-10.242.1.2	Accept	
	*FILESRV	0.0.0.0-255.255.255.254	Accept	
	*FTPCLIENT	0.0.0.0-255.255.255.254	Accept	
	*FTPLOGON3	0.0.0.0-255.255.255.254	Accept	
	*RMTSRV	0.0.0.0-255.255.255.254	Accept	
	*SQL	0.0.0.0-255.255.255.254	Accept	
			Total Entries For User:	6
			Total Users Enrolled In SafeNet/i:	2
(C) Copyright 1997-2015 MP Associates, Inc. All Rights Reserved.				

4. Print IP Usage Report

Option 8 on Menu SN4

PRTIPUSG command will produce a report showing all the IP addresses used by each user to access the exit point.

Summary reports by Group profile and auto-enrollment reports are also available. This new usage report follows the standard SafeNet/i usage report architecture.

```

Print IP Address Usage Report (PRTIPUSG)

Type choices, press Enter.

Selection From Date . . . . . *BEGIN_____ Date, *BEGIN,
      To Date . . . . . *END_____ Date, *END,
User Profile(s) To Select . . . *ALL_____ Name, *ALL
      + for more values _____
User Profile(s) To OMIT . . . . *NONE_____ Name, *NONE
      + for more values _____
Servers to Select . . . . . *ALL_____ Exit Point Server Short Name
      + for more values _____
Output . . . . . *PRINT_____ *PRINT, *OUTFILE
Job queue . . . . . *JOB_____ Name, *JOB
      Library. . . . . _____ Name,
Output Queue . . . . . *CURRENT_____ Name, *CURRENT
      Library. . . . . _____ Name,
Print Summary Group Report . . . *NO_____ *YES, *NO
Auto-Enrollment Report? . . . . *NO_____ *YES, *NO, *ONLY

Bottom
F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More keys
Function key not allowed.

```

Resulting Report

```

4/08/15 16:44:36 User To IP Address Usage Listing On System: MPADEV Page: 1
SNR0068 Run By: SAFENET
Criteria Selected:
Users: *ALL
From Date: 04/01/15 To Date: *END

User: QSECOFR Security Officer
      Servers IP Addresses
      *FILESRV 127.0.0.1
      *RMTSRV

User: SAFENET Safenet Profile
      Servers IP Addresses
      *FTPCCLIENT 172.31.1.1
      *SIGNON 10.2.2.100

SafeNet (C) Copyright 1997-2015 MP Associates, Inc.

```