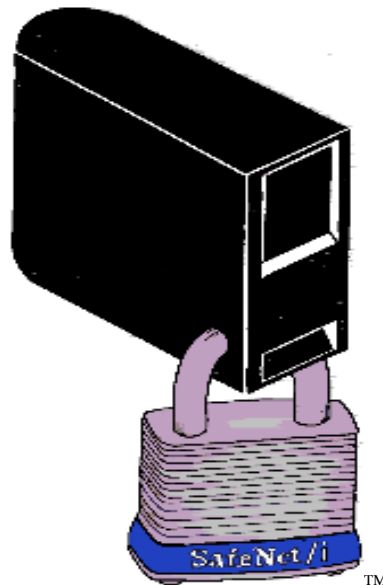


**SafeNet/i**

**FOR IBM i**

**TWO-FACTOR  
AUTHENTICATION**

**Version 11**



## **How to contact us**

Direct all inquiries to:

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

Phone: (518) 897-5002

Kisco Website: [www.kisco.com/safenet](http://www.kisco.com/safenet)  
[www.kisco.com/safenet/support](http://www.kisco.com/safenet/support)

SafeNet/i Website: [www.safeneti.com/safenet](http://www.safeneti.com/safenet)  
SafeNet/i Support Website: [www.safeneti.com/safenet/support](http://www.safeneti.com/safenet/support)

## *Table of Contents*

<b>CHAPTER 1 - SAFENET/I TWO-FACTOR AUTHENTICATION .....</b>	<b>1-1</b>
<i>TWO-FACTOR AUTHENTICATION OVERVIEW.....</i>	<i>1-1</i>
<i>TWO-FACTOR AUTHENTICATION PROCESS FOR 5250 EMULATION.....</i>	<i>1-2</i>
<b>CHAPTER 2 - SAFENET/I TWO-FACTOR AUTHENTICATION SETUP .....</b>	<b>2-1</b>
<i>INSTALLATION PROCESS .....</i>	<i>2-1</i>
<i>INITIAL SETUP .....</i>	<i>2-3</i>
<i>SPECIAL 2FA SETUP CONSIDERATIONS .....</i>	<i>2-4</i>
<i>TWO FACTOR AUTHENTICATION MENU OPTIONS.....</i>	<i>2-6</i>
<i>2FA PROBLEM DETERMINATION .....</i>	<i>2-14</i>
<b>CHAPTER 3 - TWO-FACTOR AUTHENTICATION FOR SAFENET/I WEB-CENTRAL.....</b>	<b>3-1</b>
<b>CHAPTER 4 - TWO-FACTOR AUTHENTICATION FOR FTP .....</b>	<b>4-1</b>
<i>USING TWILIO® SMS MESSAGING WITH 2FA.....</i>	<i>4-4</i>
<i>ADVANCED SETUP TECHNICAL TIPS .....</i>	<i>4-5</i>
<b>CHAPTER 5 - SAFENET/I TWO-FACTOR AUTHENTICATION TRANSACTION LOGGING .....</b>	<b>5-1</b>

# Chapter 1 - SafeNet/i Two-Factor Authentication

## *Two-Factor Authentication Overview*

**Multi-factor authentication (MFA)** is a method of confirming a user's claimed identity in which a user is granted access to a system only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism. This evidence to prove one's identity is comprised of:

1. Something the user knows

The most common example of this factor is, of course, the password, but it could also take the form of a PIN, or even a passphrase--something only you would know

2. Something the user has

This factor confirms that you are in possession of a specific item. This category includes mobile phones, physical tokens, key fobs and smartcards.

There are a few ways that this authentication works, depending on the item, but some common methods include confirming via text message or pop-up notifications from your mobile phone, typing in a unique code generated by a physical token, or inserting a card (e.g., at an ATM).

3. Something the user is

This factor is commonly verified by a fingerprint scan, but also includes anything that would be a unique identifier of your physical person--a retinal scan, voice or facial recognition, and any other kind of biometrics.

**Two-Factor Authentication**, or **2FA**, is a type of multi-factor authentication. It is a method of confirming a user's claimed identity by utilizing something they know (their password) and a second factor, other than something they have or something they are.

A second factor could be something sent to the user that they must repeat back to the initiating system.

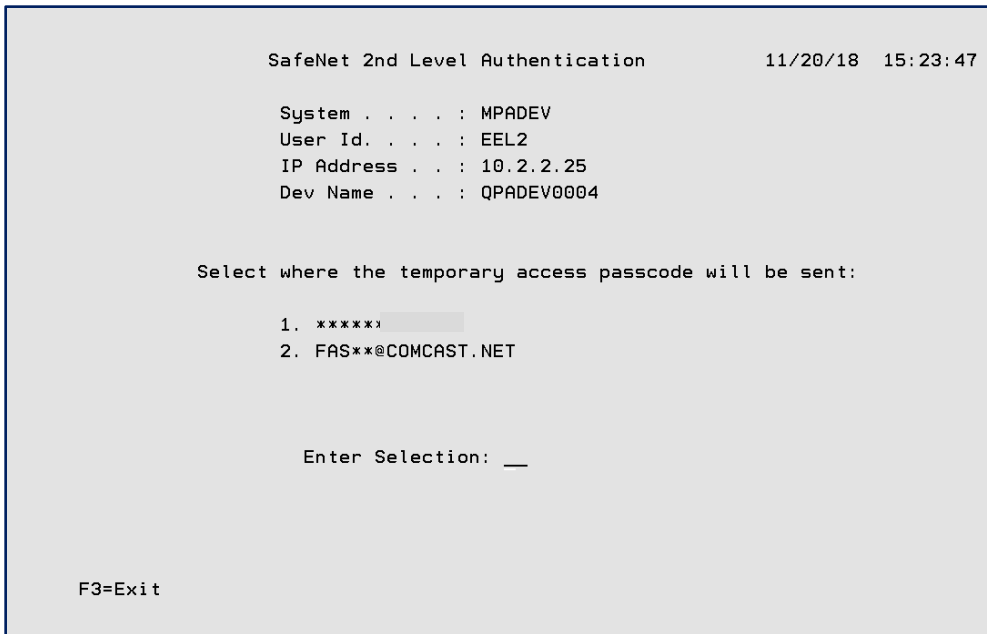
**SafeNet/i Two-Factor Authentication** requires their PASSWORD and entry of a PASSCODE that is sent to the user via text to their phone or in an email.

## ***Two-Factor Authentication Process for 5250 Emulation***

When a user begins the process to sign into a 5250 session, they will be required to provide their user ID, their password and a passcode.

1. User signs on to a 5250 session as normal
2. User will be provided with a passcode
  - If there is only one contact record on file for this user, passcode will be sent immediately
  - If there are multiple contact records, the user will be presented with a list of options to choose from. All contact options are displayed masked for additional security.

Selection screen when there is more than one possible destination



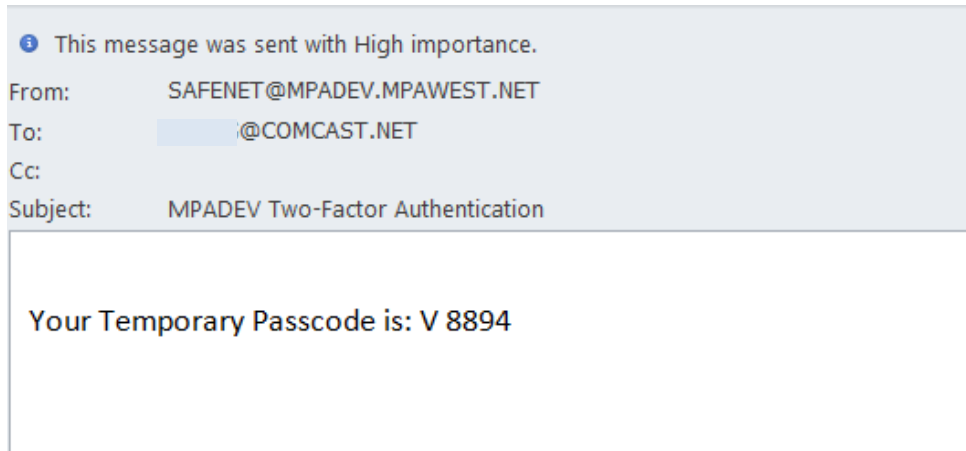
The screenshot shows a terminal window titled "SafeNet 2nd Level Authentication" with a timestamp of "11/20/18 15:23:47". It displays system information: "System . . . : MPADEV", "User Id. . . : EEL2", "IP Address . . : 10.2.2.25", and "Dev Name . . : QPADEV0004". Below this, it asks the user to "Select where the temporary access passcode will be sent:" and provides two options: "1. \*\*\*\*\*" and "2. FAS\*\*@COMCAST.NET". A prompt "Enter Selection: \_\_" is shown. At the bottom left, it says "F3=Exit".

When the user receives the passcode they must enter it in the form provided.

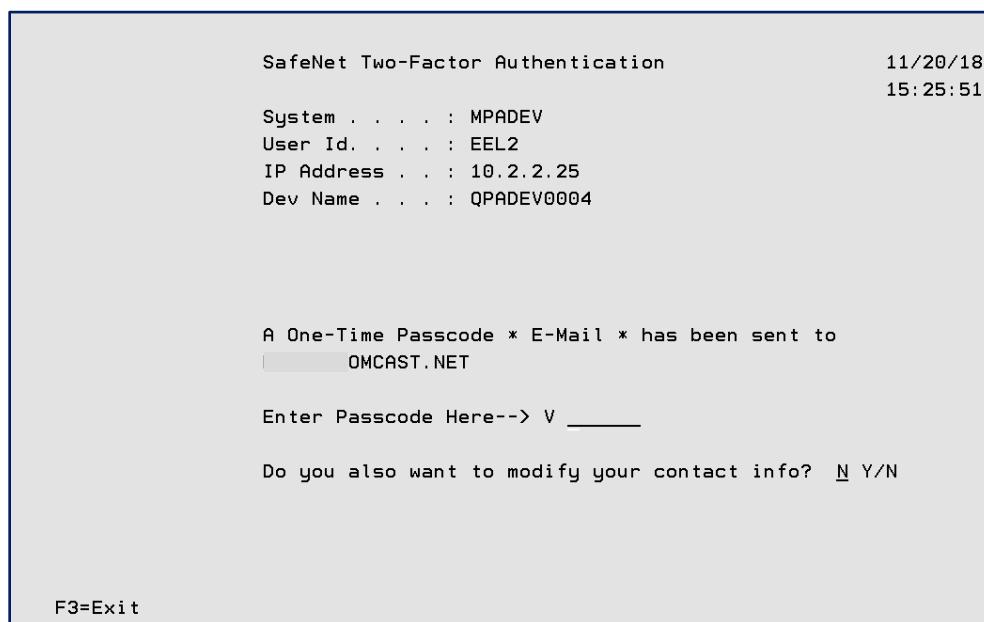
The passcode is assigned a “session” prefix that is automatically appended to the email and entry page.

The user must make sure the passcode prefix matches what is shown on the entry page. This ensures the correct passcode matches the correct session for the user.

Passcode via email: **Your Temporary Passcode is: V 8894**

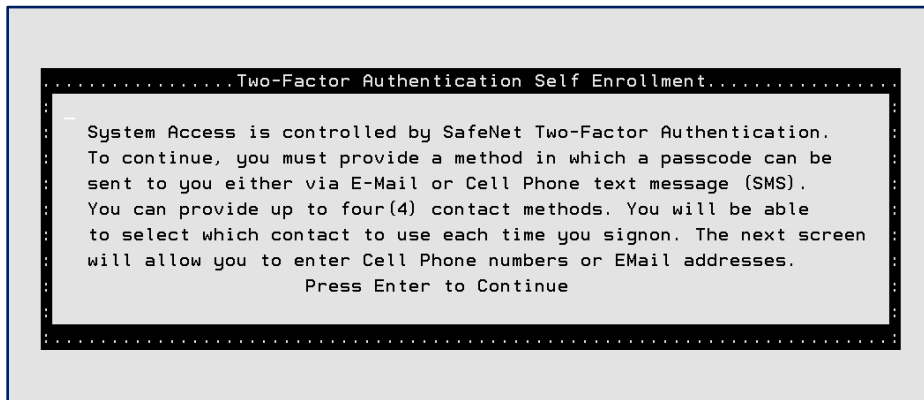


When the user receives the passcode, they will key it on the passcode entry screen

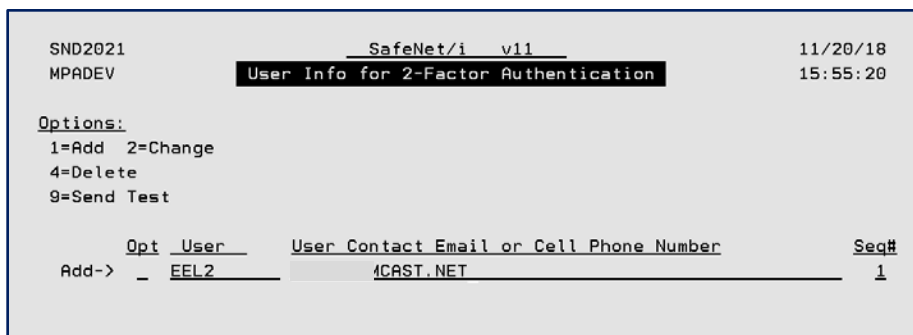


3. If the user does NOT have any contact entries on file, and if the system is set for Self-Enrollment, they will have the opportunity to enter their contact information upon successful sign on.

Message displayed to begin Self-Enrollment process:



The user keys in contact info on the Self-Enrollment maintenance screen and presses ENTER



They receive the passcode via email or phone

The user will also have the ability to manage their own contact info upon future sign-ons.

**Important:** If self-enrollment is not active, the user will not be able to enter or maintain their own contact information.

4. If users normally start more than one 5250 session, make sure you set the REPEAT connections settings in CHG2FAENV.

By allowing repeat connections in a specified time frame, users will only need to do 2FA for one session. Repeat connections are only connections that occur on the same network IP address.

See the section on changing 2-Factor environment settings in Chapter 2 of this guide for details on turning on Self-Enrollment and changing REPEAT connections.

## Chapter 2 - SafeNet/i Two-Factor Authentication Setup

You must install the **SafeNet/i** Two-Factor Authentication programs before you can use this function.

### ***Installation Process***

1. Before you begin, make sure you have the latest PTF level for the base SafeNet/i installed. Visit [SafeNet/i Support](#) to verify the current level available, and install PTF if necessary.
2. Restore the PCSEC2FAI library received from the Kisco distribution media using the following command:

```
RSTLIB SAVLIB(PCSEC2FAI) DEV(*SAVF) SAVF(PCSECLIB/PCSEC2FAI)  
MBROPT(*ALL) ALWOBJDIF(*ALL)
```

The product installation library PCSEC2FAI contains three save files and the install program:

- INSTSN2FA - Install program
- PCSECIFS - \*SAVF - Refresh of Web-Central /PCSECWEBC IFS directory
- PCSECWEBC - \*SAVF - Refresh of Web-Central library PCSECWEBC
- PCSEC2FA - Contains the library for 2FA base install
- QCLSRC – Install program source for 2FA

3. Run the install program **INSTSN2FA**

```
CALL PCSEC2FAI/INSTSN2FA
```

This program:

- Creates the required user profile SN2FAUSER for 2FA processes
- Creates a data area in PCSECLIB that contains the pointers to 2FA library
- Saves a backup copy of the current PCSEC2FA library into library PCSEC2FAOL
- Restores the new PCSEC2FA library. You may want to add this library to your library list.
- Deletes the current PCSECWEBC library and installs new version
- Replaces the IFS directory /PCSECWEBC with a new version

5. When the installation is complete, go to the **SafeNet/i** 2FA menu:

```
GO PCSEC2FA/SN2FA
```



SN2FA	SafeNet/i Version 11	10/29/18
MPADEV	Two Factor Authentication	15:27:03

Select one of the following:	Fast Path
1. Change 2-Factor Environment Settings	CHG2FAENV
2. Work with 2-Factor Network Settings	WRK2FANET
3.	
4. Work with 2-Factor User Settings	WRK2FAUSR
5. Work with 2-Factor User Overrides	WRK2FAOVR
6. Display 2-Factor Audit Log	DSP2FALOG
7.	
8. Work with Cell Carrier SMS Addresses	WRK2FACEL
9. Start PassCode Sender Job	STR2FA
10. End Passcode Sender Job	END2FA
21. Main Menu (SN1)	
	90. Signoff

Selection or command  
 ===> \_\_\_\_\_

---

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

Use menu **Option 1 – Change 2-Factor Environment Settings (CHG2FAENV)** to set up 2FA environment defaults.

Some of the values you can set:

- Length of the passcode to generate
- Time for passcodes to expire
- Number of invalid attempts allowed
- Allow or prohibit repeat connections, and, if permitted, for what time period

Continue with the initial setup of Two-Factor Authentication

## ***Initial Setup***

Verify that SMTP is already configured on your system

From the Two Factor Authentication Menu (SN2FA):

1. Select **Option 9 - Start Passcode Sender Job** to start the emailer server job or run the **STR2FA** command
  - Make sure you select a JOBQ that will allow this job to run uninterrupted. Consider using either QINTER or QSPL, either of which works fine for this job.
  - You can set the default JOBQ using the CHG2FAENV command and parameter MAILJOBQ

*Note:* You must add **PCSEC2FA/STR2FA** to the system startup program so the passcodes can be emailed or SMS texted to the user. Failure to start the emailer job will cause 2FA to be bypassed.
2. Select **Option 2 – Work with 2-Factor Network Settings** or run the **WRK2FANET** command to set up your “safe” networks where 2FA is not required
3. Select **Option 4 - Work with 2-Factor User Settings** or run the **WRK2FAUSR** command to set up user contact information and test the emailer process
  - A user can have a combination of email addresses and cell phone numbers, up to 4 contact entries
4. Select **Option 5 – Work with 2-Factor User Overrides** or run the **WRK2FAOVR** command to override any user settings from the system 2FA defaults

**IMPORTANT:** Before proceeding with 2FA for 5250 sessions, you **MUST** either add an initial program to the user profile(s) or add the 2FA program to the initial program already assigned to a user. The initial program for 2FA is **PCSEC2FA/PC2FA1CL**.

## ***Special 2FA Setup Considerations***

### **Signon Display file**

Be aware that if you are using the IBM standard default signon display file, there is the potential for users to be able to bypass 2FA. When using the IBM default signon display file a user can enter \*NONE into the program or procedure field of the signon display file and they will be able to BYPASS 2FA.

Before you implement 2FA, you **MUST** decide on what signon display file you will use.

We have provided two alternate display files with the program or procedure field protected, as part of the 2FA product. You can either use the display files we have provided, or you can modify your own.

Once you have decided, you can change your subsystem descriptions to use the correct signon display file.

You will find display files QDSIGNON and QDSIGNON2 in library PCSEC2FA. You can find the source for the two display files in source file QDDSSRC in library PCSEC2FA. The QDSIGNON2 display file is used if you have your system set to long password support (up to 128 characters).

An example of the command to change your subsystem description to use the alternate signon display file:

**CHGSBSD SBSD(QINTER) SGNDSPF(PCSEC2FA/QDSIGNON)**

### **Mailer Job**

You must have the mailer job **SN2FASENDNR** active for 2FA to work

The initial user program for 2FA checks to make sure the sender job is active on the system. If the SN2FASENDNR job is not active, no passcodes will be emailed or texted and 2FA will be bypassed. Use command STR2FA. Failure to start the mailer job will cause 2FA to be bypassed.

### **Email Content**

If needed you can change the language or text of the emails/texts sent

- Data area **FADSTD** contains the subject line for the email or text message
- Data Area **FAPASSL1** contains the body of the passcode email
- Data Area **FATESTL1** contains the body of the TEST passcode email

## **Email Sender ID**

If you need to change the “sender” ID from where the passcode emails are sent, see data area **SENDERID**.

**Note:** The user ID MUST exist in your system directory. Positions 1-10 contain the User ID and positions 11-20 contain the system name to use for the SNDDST command.

## **Cell Phone Carriers**

For passcodes to be sent via SMS texts to cell phones, you must have the correct cell phone carrier assigned to the user entry.

If the correct cell phone carrier is not shown in the prompt display, you can add a new one using Menu SN2FA Option 8 or **WRK2FACEL** command.

Add any new carriers and make sure you also enter the correct SMS email suffix (gateway address) for the carrier.

Use this link for an extensive list of available SMS codes for each carrier:

[https://kb.sandisk.com/app/answers/detail/a\\_id/17056/~list-of-mobile-carrier-gateway-addresses](https://kb.sandisk.com/app/answers/detail/a_id/17056/~list-of-mobile-carrier-gateway-addresses)

## Two Factor Authentication Menu Options

### GO PCSEC2FA/SN2FA

SN2FA	SafeNet/i Version 11	10/29/18
MPADEV	Two Factor Authentication	15:27:03
Select one of the following:		<u>Fast Path</u>
1. Change 2-Factor Environment Settings		CHG2FAENV
2. Work with 2-Factor Network Settings		WRK2FANET
3.		
4. Work with 2-Factor User Settings		WRK2FAUSR
5. Work with 2-Factor User Overrides		WRK2FAOVR
6. Display 2-Factor Audit Log		DSP2FALOG
7.		
8. Work with Cell Carrier SMS Addresses		WRK2FACEL
9. Start PassCode Sender Job		STR2FA
10. End Passcode Sender Job		END2FA
21. Main Menu (SN1)		
		90. Signoff
Selection or command		
==> _____		
_____		
F3=Exit F4=Prompt F9=Retrieve F12=Cancel		
F13=Information Assistant F16=System main menu		

## Menu Option 1 – Change 2-Factor Environment Settings

```
Two Factor Auth Env Settings (CHG2FAENV)

Type choices, press Enter.

Two-Factor Authentication Is . . . *ON          *ON, *OFF
Allow User to Self-Enroll? . . . *YES         *YES, *NO
Passcode Length to Generate . . . 4           3-6
Minutes until Passcode Expires . . 015        001-999
# of Attempts Allowed . . . . . 3           1-9
Repeat Connects without 2FA? . . *YES        *YES, *NO
# Days until Repeat Expires . . . 000        000-999
# Hrs until Repeat Expires . . . 00          00-23
# Mins until Repeat Expires . . . 05          00-99
Block Access to SYSREQ Menu? . . . *YES        *YES, *NO
Block Access to ASSIST Menu? . . . *YES        *YES, *NO
JOBQ for 2FA EMailer Job . . . . QINTER      Character value
Use 2FA with WebCentral? . . . . *YES        *YES, *NO
Web Passcode Timeout Minutes . . . 060        000-999
Use 2FA with FTP? . . . . . *YES          *YES, *NO
FTP Passcode Timeout Minutes . . . 005        000-999

More...

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

Page down to additional parameters

```
Two Factor Auth Env Settings (CHG2FAENV)

Type choices, press Enter.

Use kConnect SMS Messaging? . . . *YES          *YES, *NO
Use kConnect Account ID. . . . . *DEFAULT      *DEFAULT, valid AcctId
```

Configure these settings if you are using **Kisco Connect** for SMS messaging.

See Help text for explanation of parameters

## Menu Option 2 – Work with 2-Factor Network Settings

Network rules are enforced differently based on which server is being used to access the system.

On this screen choose either \*FTP or \*TELNET.

```
Work with 2FA Network Settings (WRK2FANET)

Type choices, press Enter.

Network Service Type . . . . . *FTP      *FTP, *TELNET
```

Use this option to indicate what network segments or IP address ranges you want to enforce 2FA or exclude.

You can specify a single IP address or a range of IP addresses.

```
SND2020                      SafeNet/i v11                      12/02/22
MPADEV                      Network Info for 2-Factor Authentication 12:39:16
                             For Service: *FTP

Options:                      Logging Options:
1=Add                          A=All
4=Delete                       R=Rejects Only

-----Range-----
Opt  From IP Address  To IP Address  2-Factor    Logging
Add->  Required?
      (Y/N)
      -----
      10.2.2.0        10.2.2.254    N           A Log All
      10.2.2.120      10.2.2.120    Y           A Log All
      10.242.1.0      10.242.1.254  Y           A Log All
      172.31.1.0      172.31.1.254  N           A Log All
      64.20.162.10    64.20.162.10  N           A Log All

Bottom

F1=Help  F3=Exit  F6=Fold/Notes
F12 = Cancel  (c)1997,2022 MP Assoc., Inc
```

### Example:

If you do NOT want 2FA on your internal network, enter that network range here and specify “N” for “2-Factor Required?”. Optionally you can set the logging override level.

## Menu Option 4 – Work with 2-Factor User Settings

```
SND2021                      SafeNet/i   v11                      10/29/18
MPADEV                      User Info for 2-Factor Authentication 15:38:19
                             All User Maintenance

Options:
1=Add  2=Change
4=Delete  7=Overrides
9=Send Test                               Find User: _____

  Opt  User      User Contact Email or Cell Phone Number      Seq#
Add->  -         -
      - EEL2      8455555555                                     1
      - EEL2      EMAIL@DOMAIN.COM                             2
      - IBM       8005555555                                     1
Has Ovr - MJONES  EMAIL@DOMAIN.COM                             2
      - MJONES1   8465555555                                     1
Has Ovr - QSECOFR QSECOFR@DOMAIN.COM                             1
      - QSECOFR   6315555555                                     2
      - SAFENET   SAFENET@DOMAIN.COM                           2

                                           Bottom

.....
F1=Help    F3=Exit                      F6=Fold    F7=All User Overrides
                                           (c) 1997, 2018 MP Assoc., Inc
```

Use this screen to enter user 2FA contact information.

A user may have up to four(4) entries.

You can enter any valid email address and cell phone number. Make sure you select the correct cell phone carrier for each phone number entered.

**Press F6** to show the fold information that contains the carrier and last signon use date.



## Menu Option 5 – Work with 2-Factor User Overrides

```
SND2024          SafeNet/i  v11          10/29/18
MPADEV          Special User Overrides for 2FA      15:42:58

Options:
1=Add
4=Delete

Find User: _____
Logging Options:
A=All
R=Rejects Only

      Opt  User      Is 2-FA      Self-      Logging
      Add-> -      (Y/N)      Enroll?      (Y/N)
            -      -      -      -
            -      MJONES      Y      N      A Log All
            -      QSECOFR      Y      N      A Log All

Bottom

.....
F1=Help      F3=Exit
F12 = Cancel      (c)1997,2018 MP Assoc., Inc
```

Use this screen to override user defaults. You can:

- Specify that a user ALWAYS needs to use 2FA regardless of the network.
- Override self-enrollment ability to limit access to user maintenance when a user signs on.
- Also override any logging values for the user.

## Menu Option 6 – Display 2-Factor Audit Log

```

                                Display 2FA Connection Log (DSP2FALOG)

Type choices, press Enter.

User Profile . . . . . > *ALL          *ALL or a user name


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

You can view an individual user or all log entries.

From this screen you can use **Option 2** to go directly to the **WRK2FAUSR** command.

```

SND2026                                SafeNet/i v11                                12/11/18
MPADEV                                View 2FA Connection Log                        15:11:23

Options                                Select: User: _____
2=Edit User                            or IP Addr: _____
                                        or Date: _____ YYYYMMDD

Opt  User      From IP Addr    Date      Time      Passcode sent to:
-   AAA3NET    12.242.1.2    2018-12-09 08.41.22 Repeat logon, none sent.
-   BBB3NET    12.242.1.2    2018-12-09 08.41.22 Repeat logon, none sent.
-   EEL2       10.2.2.25     2018-12-11 15.01.32          :OMCAST.NET
-   MJONES     10.242.1.2    2018-11-06 13.51.54 MJO***@MPAWEST.NET
-   MJONES1    10.242.1.2    2018-11-06 16.00.21          MPAWEST.NET
-   SAFENET    10.2.2.25     2018-11-29 13.24.16 ELE*****@MPAWEST.COM
-   SAFENET    10.242.1.2    2018-11-19 09.28.51 MJO***@MPAWEST.NET
-   SAFENET    10.242.1.2    2018-11-04 13.50.00 MJO***@MPAWEST.NET
-   TEST       12.242.1.2    2018-12-09 08.41.22 Repeat logon, none sent.
-   XAFENET    12.242.1.2    2018-12-09 08.41.22 Repeat logon, none sent.
                                                                    More...

F1=Help   F3=Exit   F6=Fold   F7=Chg Date Seq   F8=Chg IP Seq   F12 = Cancel
(c) 1997, 2018 MP Assoc., Inc
```

## Menu Option 8 - Work with Cell Carrier SMS Addresses

SND2025	SafeNet/i v11	10/29/18
MPADEV	Maintain Cell Phone Carriers	15:49:33

Options:  
2=Change  
4=Delete

Opt	Carrier	Suffix for SMS Messaging	Carrier Key
-	VERIZON	@vtext.com	001
-	AT&T	@txt.att.net	002
-	SPRINT	@messaging.sprintpcs.com	003
-	SPRINT (NEXTEL)	@messaging.nextel.com	004
-	T-MOBILE	@tmomail.net	005
-	CELLULAR ONE	mobile@celloneusa.com	006
-	BOOST MOBILE	@myboostmobile.com	007
-	CRICKET	@sms.mycricket.com	008
-	US CELLULAR	@email.uscc.net	009

More...

F1=Help      F3=Exit      F6=Add Carrier      F12 = Cancel

(c) 1997, 2018 MP Assoc., Inc

If you need to add a new cell carrier, use F6 to add a new entry.

## Menu Option 9 – Start Passcode Sender Job

Start 2FA Mailer Job (STR2FA)

Type choices, press Enter.

Submit to Job Queue . . . . . \_\_\_\_\_ \*DFT or Jobq Name

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

Bottom

You can override the default JOBQ from this screen.

If you do not enter a JOBQ name, the default will be used. Set the default JOBQ value by accessing the **CHG2FAENV** command parameter *MAILJOBQ*.

## Menu Option 10 – End Passcode Sender Job

Taking this option will end the Mailer Job. If this job is ended for any reason, 2FA passcodes will no be sent and 2FA controls will be bypassed.

## Files contained in SafeNet/i Two-Factor Authentication

SN2FA01PF -	User controls
SN2FA02PF -	User Overrides
SN2FA10PF -	Cell phone Carrier codes
SN2FA20PF -	Network settings for 2FA
SN2FA99PF -	Historic Log file of 2FA connections
SN2FA98PF -	Contains Log of 2FA connections for FTP sessions

## **2FA Problem Determination**

- The user is not being prompted for 2FA passcode
  - a. Is 2FA active on your system – use command CHG2FAENV to check.
  - b. Is the EMAILER that sends the passcodes job active - use STR2FA command to start the job and use command WRK2FAENV parameter MAILJOBQ to verify what subsystem the job starts in.
  - c. Is the user enrolled in the 2FA control tables – use command WRK2FAUSR
  - d. Is the network segment the user is on required to use 2FA – see command WRK2FANET and check if there is a network override.
  - e. Does the user have a special 2FA override - see command WRK2FAUSR
  
- The user can't access their own contact information when signing on
  - a. Self-Enrollment is not active - see command CHG2FAENV parameter SELFENROLL
  
- **SafeNet/i** Web-Central is not prompting for passcode
  - a. Make sure 2FA is activated for Web-Central. – see command CHG2FAENV parameter WEBCENTRAL.

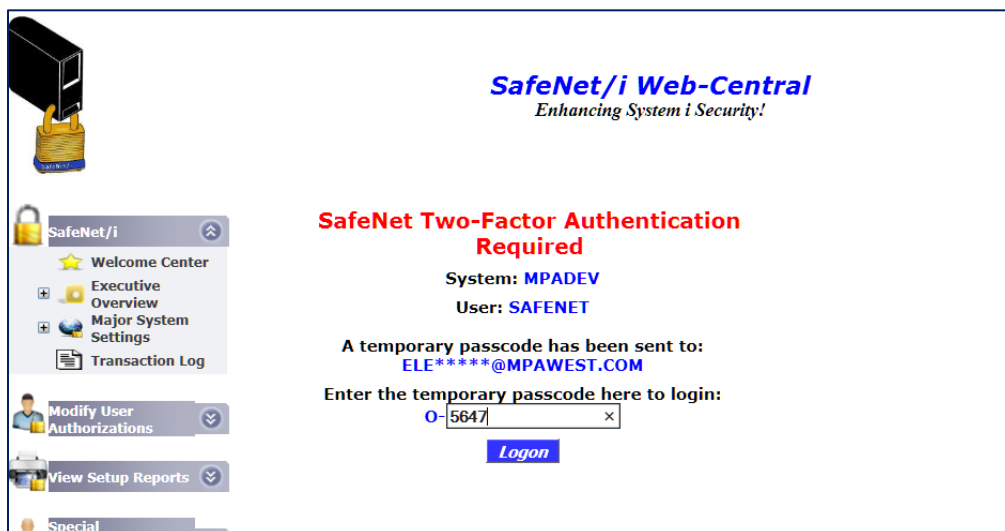


Multi-Address selection prompt:



The screenshot shows the SafeNet/i Web-Central interface. On the left is a navigation menu with icons and labels: 'SafeNet/i', 'Welcome Center', 'Executive Overview', 'Major System Settings', 'Transaction Log', 'Modify User Authorizations', 'View Setup Reports', and 'Special Administration Functions'. The main content area has the title 'SafeNet/i Web-Central' with the tagline 'Enhancing System i Security!'. Below this, it says 'SafeNet Two-Factor Authentication Required'. The system is identified as 'MPADEV' and the user as 'SAFENET'. A prompt asks to 'Select the destination address for the passcode:' followed by four radio button options: '\*\*\*\*\*8833 (VERIZON)', 'MJO\*\*\*@MPAWEST.NET', 'ELE\*\*\*\*\*@MPAWEST.COM', and 'SAL\*\*@KISCO.COM'. A 'Continue' button is at the bottom.

User must enter the passcode provided to continue with Web-Central



This screenshot shows the same SafeNet/i Web-Central interface. The 'SafeNet Two-Factor Authentication Required' section now indicates that a temporary passcode has been sent to 'ELE\*\*\*\*\*@MPAWEST.COM'. It prompts the user to 'Enter the temporary passcode here to login:' and shows a text input field with '0-5647' and a clear button (x). A 'Logon' button is positioned below the input field.

**Note:** Self-Enrollment is NOT available with Web-Central at this time.

## Chapter 4 - Two-Factor Authentication for FTP

### 1. Configure the *SafeNet FTP Logon* server to use 2FA

- Use the **WRKSRV** command to set the \*FTPLOGON3 server to Security Level 3.
- Normal Server, User and FTP setup is required within SafeNet before using 2FA for FTP. See the SafeNet/i Reference Guide for specifics.
- Users must be configured in 2FA setup before activating 2FA for FTP.

### 2. Configure 2FA settings for your network and users

- From the SafeNet/i Main Menu, select **Option 25 – Two Factor Authentication**

SN2FA	SafeNet/i Version 11	11/09/22
MPADEV	Two Factor Authentication	15:01:06
Select one of the following:		<u>Fast Path</u>
1. Change 2-Factor Environment Settings		CHG2FAENV
2. Work with 2-Factor Network Settings		WRK2FANET
3.		
4. Work with 2-Factor User Settings		WRK2FAUSR
5. Work with 2-Factor User Overrides		WRK2FAOVR
6. Display 2-Factor Connection Log		DSP2FALOG
7. Purge 2-Factor Connection Log		STR2FAPRG
8. Work with Cell Carrier SMS Addresses		WRK2FACEL
9. Start PassCode Sender Job		STR2FA
10. End Passcode Sender Job		END2FA
21. SafeNet Main Menu (SN1)		90. Signoff

- Network - **Menu Option 2 – Work with 2-Factor Network Settings (WRK2FANET)**
- Users - **Menu Option 4 – Work with 2-Factor User Settings (WRK2FAUSR)**

### 3. Enabling and Activating Two-Factor Authentication for FTP

- From the Two Factor Authentication Menu (SN2FA) select **Option 1 – Change 2-Factor Environment Settings**
- Change settings to turn *FTP \*ON* and *Use 2FA with FTP \*YES*



Two Factor Auth Env Settings (CHG2FAENV)		
Type choices, press Enter.		
Two-Factor Authentication Is . . .	STATUS	<u>*ON</u>
Allow User to Self-Enroll? . . .	SELFENROLL	<u>*YES</u>
Passcode Length to Generate . . .	CODELEN	<u>4</u>
Minutes until Passcode Expires . . .	TIMEOUT	<u>015</u>
# of Attempts Allowed . . . . .	NUMALLOW	<u>3</u>
Repeat Connects without 2FA? . . .	ALLOWRPT	<u>*YES</u>
# Days until Repeat Expires . . .	EXPIREDAYS	<u>000</u>
# Hrs until Repeat Expires . . .	EXPIREHRS	<u>00</u>
# Mins until Repeat Expires . . .	EXPIREMIN	<u>05</u>
Block Access to SYSREQ Menu? . . .	BLOCKSYSRQ	<u>*YES</u>
Block Access to ASSIST Menu? . . .	BLOCKOA	<u>*YES</u>
JOBQ for 2FA EMailer Job . . . . .	MAILJOBQ	<u>QINTER</u>
Use 2FA with WebCentral? . . . . .	WEBCENTRAL	<u>*NO</u>
Web Passcode Timeout Minutes . . .	WEBTIMEOUT	<u>060</u>
Use 2FA with FTP? . . . . .	FTP	<u>*YES</u>
FTP Passcode Timeout Minutes . . .	FTPTIMEOUT	<u>005</u>

- Or use commands

Enable:           **CHG2FAENV FTP(\*YES)**

Activate:       **CHG2FAENV STATUS(\*ON) FTP(\*YES)**

- **FTPTIMEOUT** parameter sets a session timer. Once this time limit is reached, the temporary passcode will expire and the user will be required to re-do the 2FA process.

4. After activating 2FA for FTP, follow these steps to use FTP.

- Perform a normal FTP into the server and use your normal user ID and password.
- **Your session will terminate, logon will show rejected.**

```
C:\>ftp 10.2.2.4
Connected to 10.2.2.4.
220-QTCP at MPADEV
220 Connection will close if idle more than 5 minutes.
User (10.2.2.4:(none)): eel
331 Enter password.
Password:
530 Log on attempt by user EEL rejected.
Login failed.
ftp>
```

- An email or text containing a temporary passcode will be sent to the destination configured for your user ID in **User Info for 2-Factor Authentication (WRK2FAUSR command)**.

If the user has more than one cellphone or email contact entry, only the first entry will be used with 2FA for FTP.

- FTP into the server again but this time use the temporary passcode you received as the FTP session password.

```
ftp> open 10.2.2.4
Connected to 10.2.2.4.
220-QTCP at MPADEV
220 Connection will close if idle more than 5 minutes.
User (10.2.2.4:(none)): eel
331 Enter password.
Password:
230 EEL logged on.
```

- Repeat connections from the same IP address are allowed for the period configured.

## Using Twilio® SMS messaging with 2FA

New in **SafeNet/i** Version 11.55, you can use **Kisco Connect** with Twilio® SMS messaging to send alerts.

Please visit the [Kisco Systems](#) website for information on Kisco Connect and how to obtain the software.

Once Kisco Connect is installed on your system, you can use it within SafeNet/i.

From the SafeNet Two Factor Menu (SN2FA) select **Option 1 – Change 2-Factor Environment Settings**

```
Two Factor Auth Env Settings (CHG2FAENV)

Type choices, press Enter.

Two-Factor Authentication Is . . . *ON          *ON, *OFF
Allow User to Self-Enroll? . . . *YES         *YES, *NO
Passcode Length to Generate . . 4           3-6
```

Page Down

Here you can turn Twilio® SMS messaging ON or OFF.

You can specify a different Twilio® account for 2FA if you want to use something other than the \*DEFAULT account.

```
Two Factor Auth Env Settings (CHG2FAENV)

Type choices, press Enter.

Use kConnect SMS Messaging? . . . *YES          *YES, *NO
Use kConnect Account ID. . . . . *DEFAULT      *DEFAULT, valid AcctId
```

See the KConnect for IBM i Guide for further information using Twilio® for SMS messaging.

## ***Advanced Setup Technical Tips***

### **Create a custom Welcome Banner when 2FA is active for FTP**

Normally when you connect to a system to log on thru FTP you will see something like this:

*OS/400 is the remote operating system. The TCP/IP version is "V7R3M0"*

If you want to let FTP users know that 2FA is in effect when they attempt to sign on, you can do so by changing the standard IBM-supplied message description.

Use the **CHGMSGD** command to modify a standard IBM-supplied message, taking into consideration the following requirements:

- Positions 1-4 of the message description **MUST** be **220-**
- Positions 5-100 can be any message

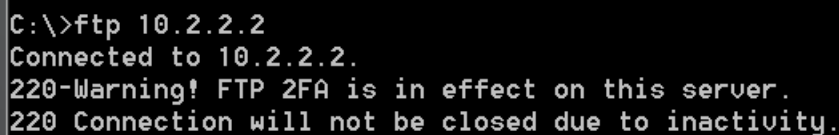
You can change the message to whatever you want, but remember the message will be reset when you do an OS upgrade.

The message file is QTCPPMSGF in library QTCP and the message ID is TCP120D.

To customize the message:

**CHGMSGD MSGID(TCP120D) MSGF(QTCP/QTCPPMSGF) MSG('220- Warning! FTP 2FA is in effect on this server.')**

After you make this change, your users will see this:



```
C:\>ftp 10.2.2.2
Connected to 10.2.2.2.
220-Warning! FTP 2FA is in effect on this server.
220 Connection will not be closed due to inactivity.
```

**Important:** If you change the message, it **MUST** contain **220-** in the first 4 positions. If **220-** is not in the message description, Windows FTP clients as well as other FTP clients may fail to work correctly with this FTP server.

To set the message back to the standard default:

**CHGMSGD MSGID(TCP120D) MSGF(QTCP/QTCPPMSGF) MSG('220- &1 at &2')**

As with any system change, document the change and make sure you **TEST** your FTP server and client connections after making any changes to the message descriptions. Also remember you may need to reset them after any OS upgrades.

## Chapter 5 - SafeNet/i Two-Factor Authentication Transaction Logging

All transactions are logged to the regular SafeNet/i transaction audit file.

- You can specify user overrides to control logging if required.
- You can log all 2FA requests, no 2FA requests or only log rejected 2FA signons.
- To view 2FA transaction in SafeNet, use the PCREVIEW or PCTESTR commands and select \*SPECIAL server transactions.
- In addition, if a 2FA request is rejected, it will trigger an alert from SafeNet/i just like other network transaction rejections.

### Logged 2FA Transaction Example

```
PCTESTR                               SafeNet/i   v11                               11/29/18
MPADEV                               On-Line Transaction Review Mode          16:12:04
                                      Actual Status At Time Of Request

Requested Security Level to Check --> H Historical Review
Current Server Security Setting-----> *
Max. Security Level For this Server-> 1 No Checking Performed
Return Information:
Status Code--> 2 Failed Two-Factor Authentication
User--> MJONES1      Group Profile-> MJONES2
Job-> QPADEV0001     Date/Time--> 11/06/2018 15.41.03.834
Source IP Address--> 10.242.1.2
Server--> *SPECIAL   Telnet Session Initialization
Format--> INIT0100   Telnet Session Initialization

More--> Telnet with 2FA. User not Enrolled in 2FA.

F3 = Exit      Pageup/Pagedown
F12 = Restart                                     (c)1997,2018 MP Assoc., Inc
```