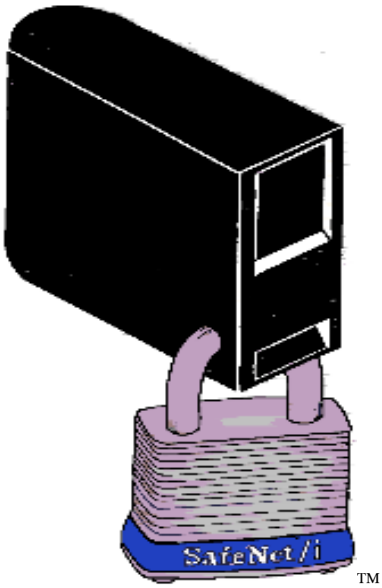
SafeNet/i

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
Email: support@kisco.com

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

Table of Contents

Chapter 1 - SafeNet 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.

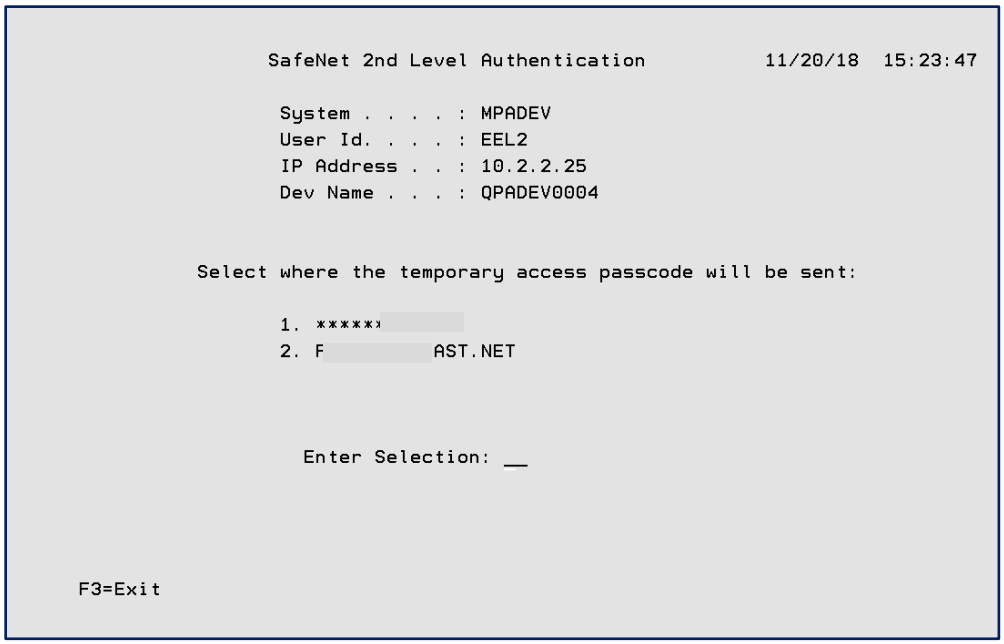
1. User signs on to a 5250 session as normal

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

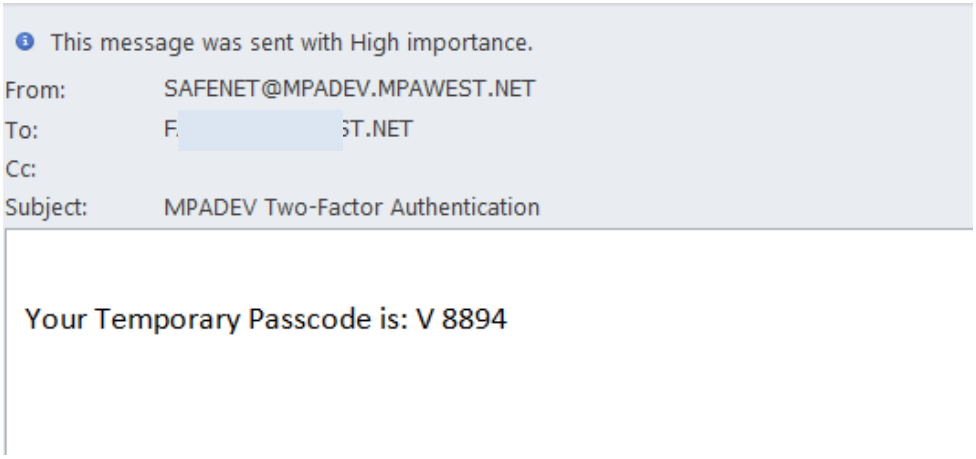


When the user receives the passcode they must enter it in the form provided.

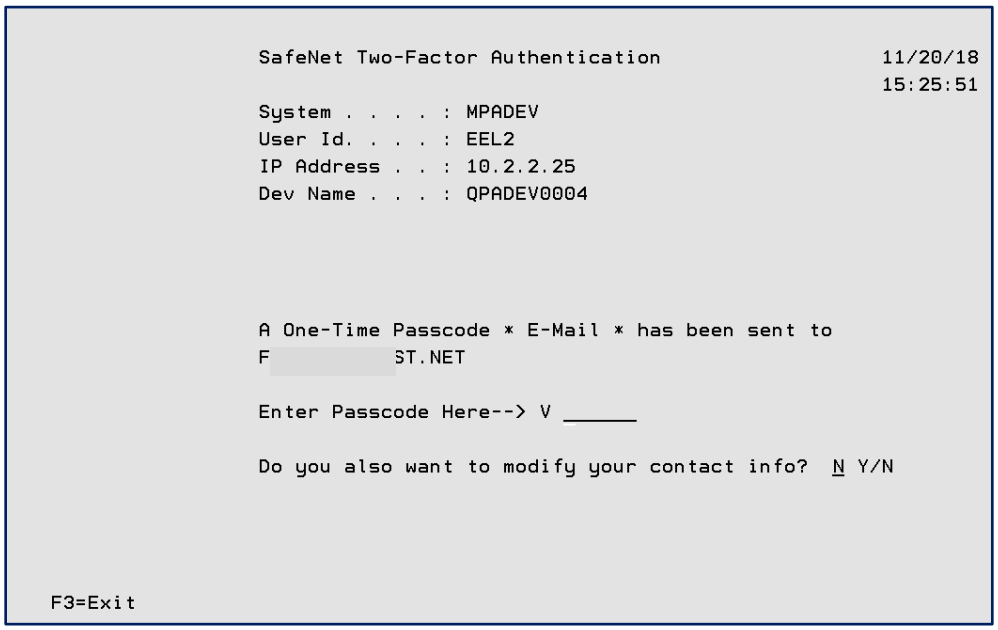
The passcode is assigned a “session” prefix that is automatically appended to the email and entry page.

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**

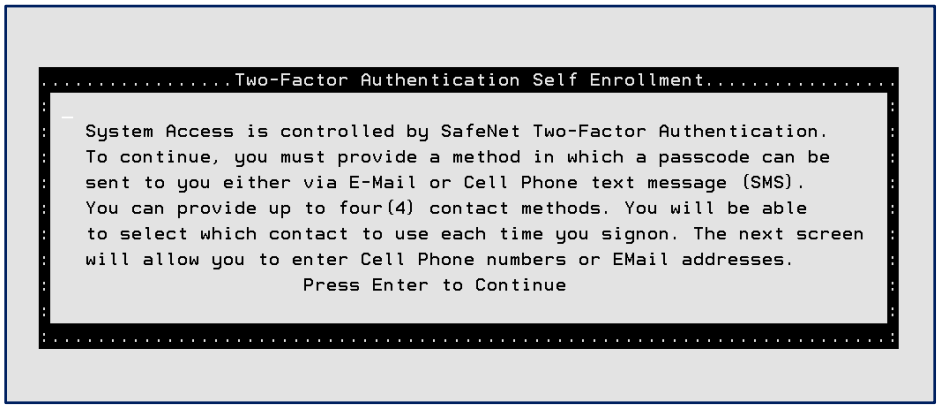


When the user receives the passcode, they will key it on the passcode entry screen

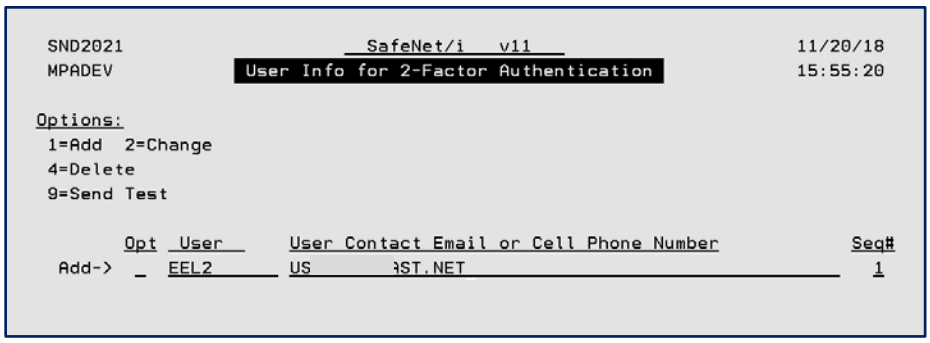


3. If the user does NOT have any contact entries on file, and if the system is set for Self-Enrollment, they will have the opportunity to enter their contact information upon successful sign on.

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

Chapter 2 - SafeNet Two-Factor Authentication Setup

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

Installation Process

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.

If your current SafeNet/i PTF level is below PTF1158, follow steps 1 and 2. OTHERWISE, skip to Step #3.

1. 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

2. Run the install program **INSTSN2FA**

   CALL PCSEC2FAI/INSTSN2FA

   This program:

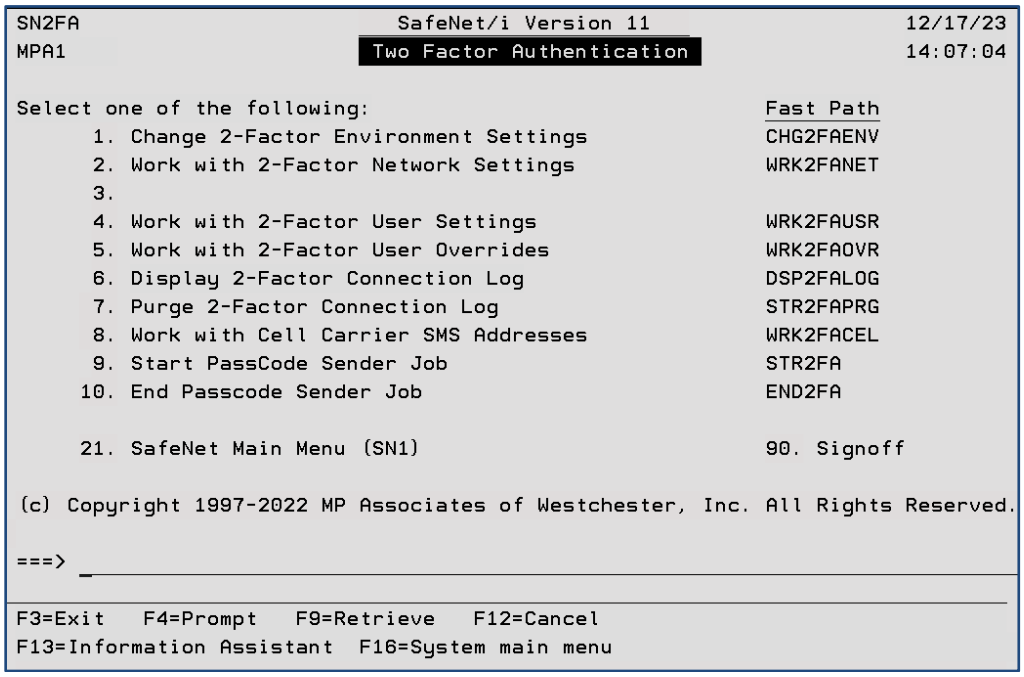
   - Creates the required user profile SN2FAUSER for 2FA processes
   - Creates a data area in PCSECLIB that contains the pointers to 2FA library
   - Saves a backup copy of the current PCSEC2FA library into library PCSEC2FAOL
   - Restores the new PCSEC2FA library. You may want to add this library to your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

3. If your current SafeNet/i PTF level is PTF1158 or above:

   Run the command **PCSECLIB/SN2FAINST**

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

GO PCSEC2FA/SN2FA



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/SN2FA1CL**.

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)

Emailer Job

You must have the emailer job **SN2FASENDR** 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 SN2FASENDR job is not active, no passcodes will emailed or texted and 2FA will be bypassed. Use command **STR2FA** to start emailer job. Failure to start the emailer 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.

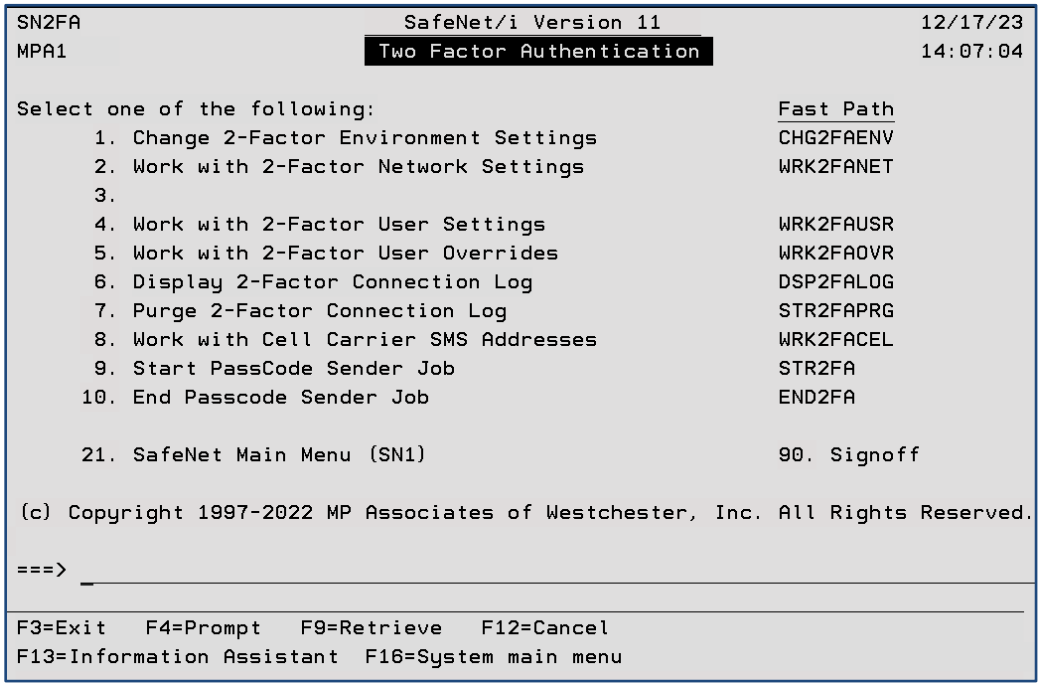
If the correct cell phone carrier is not shown in the prompt display, you can add a new one using **Option 8** on the Two Factor Authentication Menu (SN2FA) or **WRK2FACEL** command.

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:

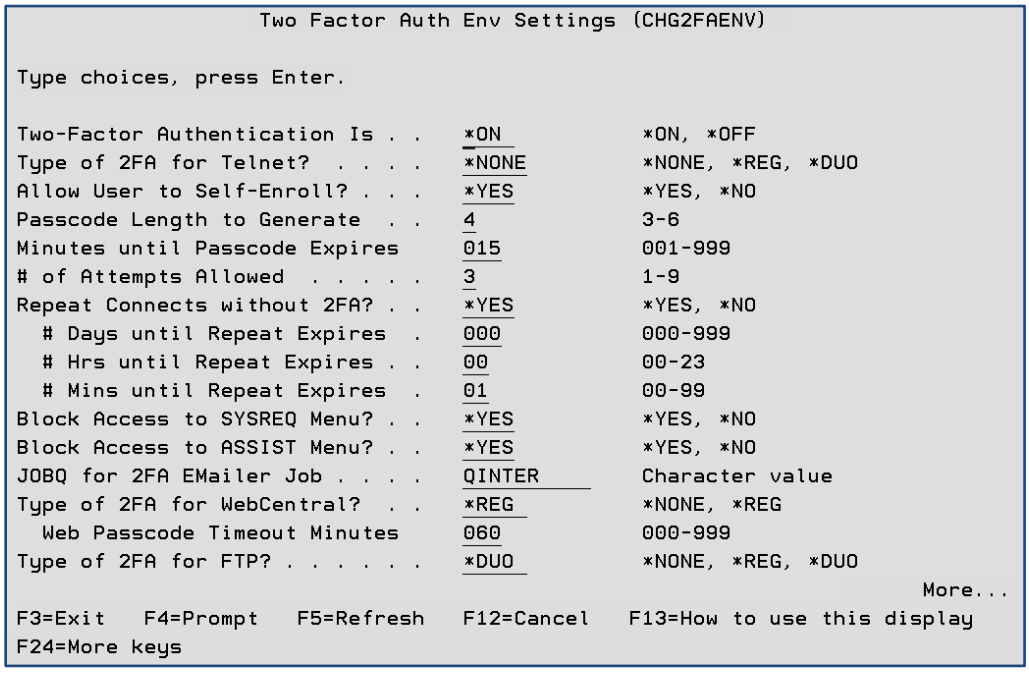
https://avtech.com/articles/138/list-of-email-to-sms-addresses/

GO PCSEC2FA/SN2FA

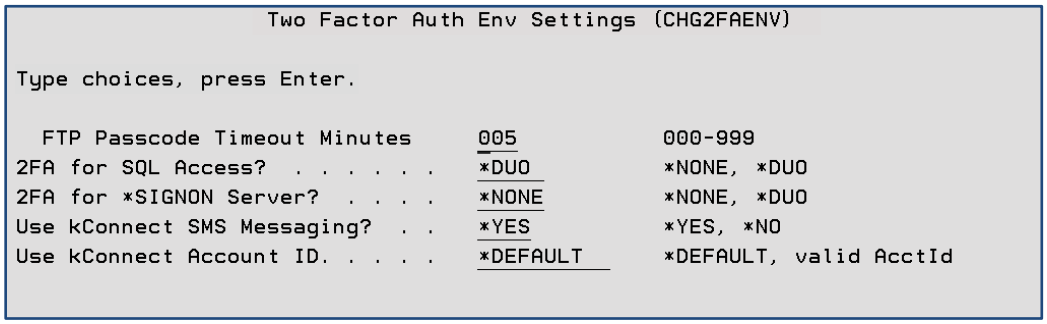


You may want to add library **PCSEC2FA** to your library list to make using 2FA commands easier.

Menu Option 1 – Change 2-Factor Environment Settings



Page down to additional parameters



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

See Help text for explanation of parameters

Considerations:

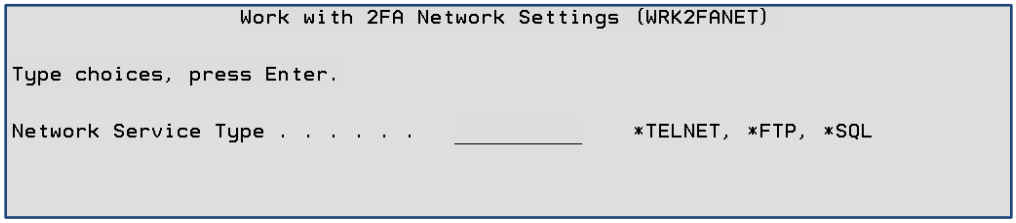
1. The DUO option is only allowed when using **Kisco kConnect** and DUO.

2. SQL 2FA is ONLY available when using DUO. 2FA for SQL is not available with standard SafeNet 2FA.

Menu Option 2 – Work with 2-Factor Network Settings

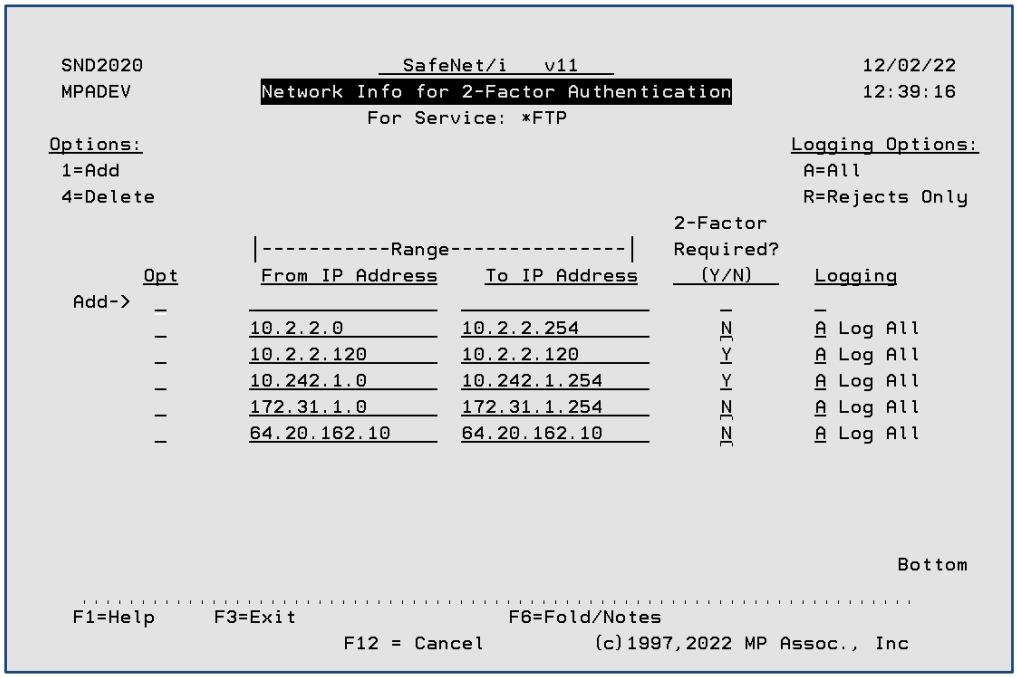
Network rules are enforced differently based on which server is being used to access the system.

On this screen choose either *TELNET, *FTP or *SQL.



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

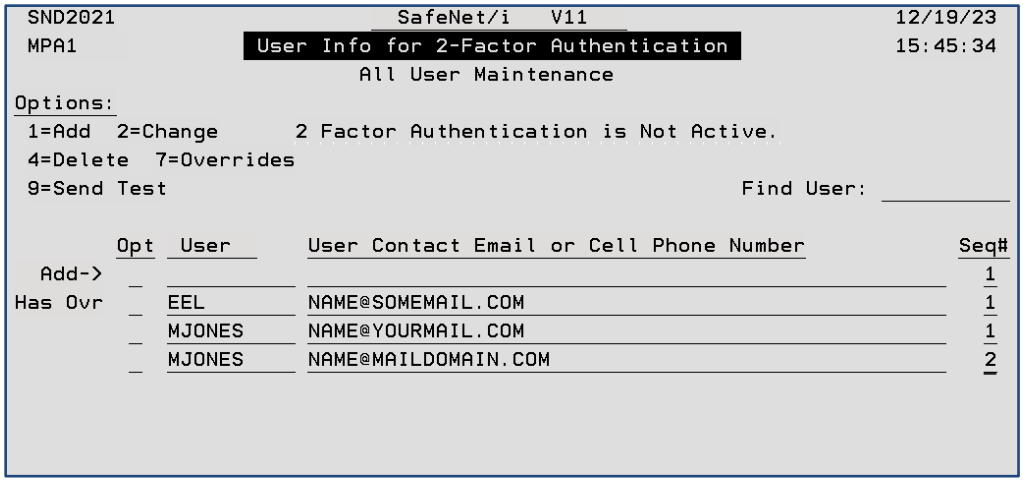
You can specify a single IP address or a range or IP addresses.



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



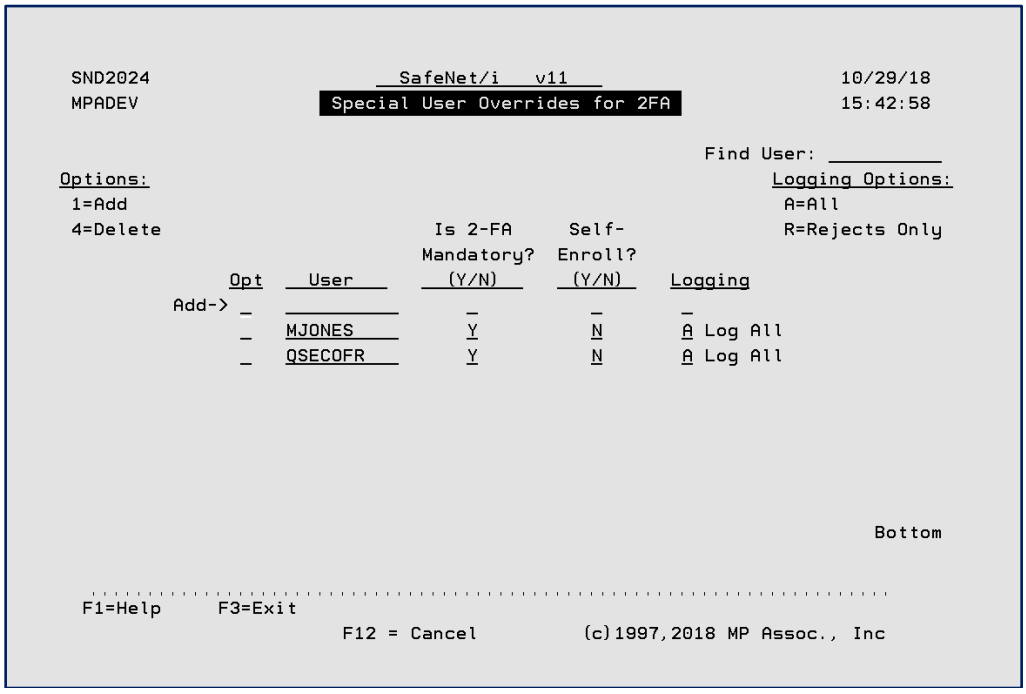
Use this screen to enter user 2FA contact information.

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.

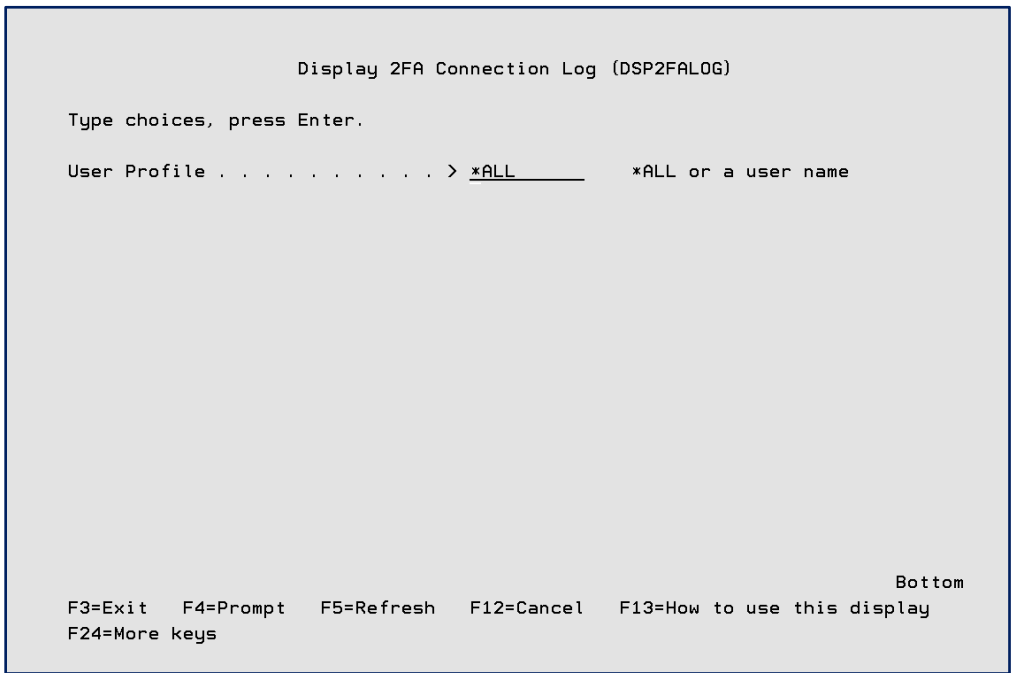
Menu Option 5 – Work with 2-Factor User Overrides



Use this screen to override user defaults. You can:

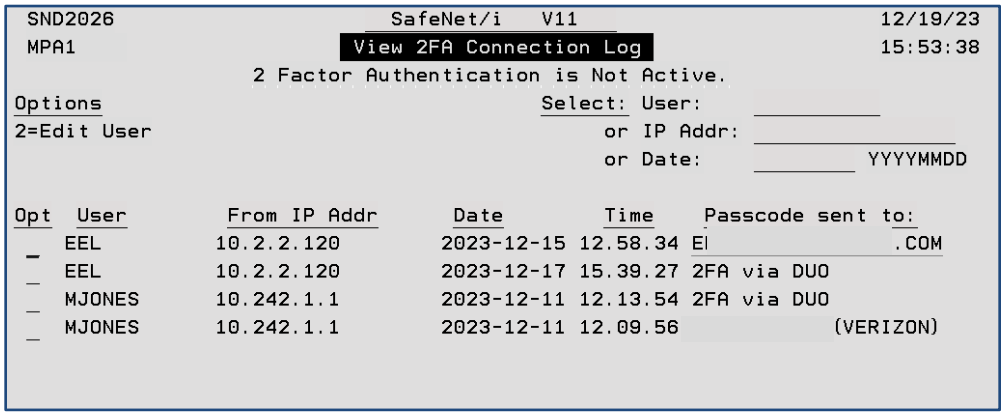
- Specify that a user ALWAYS needs to use 2FA regardless of the network.
- Override self-enrollment ability to limit access to user maintenance when a user signs on.
- Also override any logging values for the user.

Menu Option 6 – Display 2-Factor Audit Log

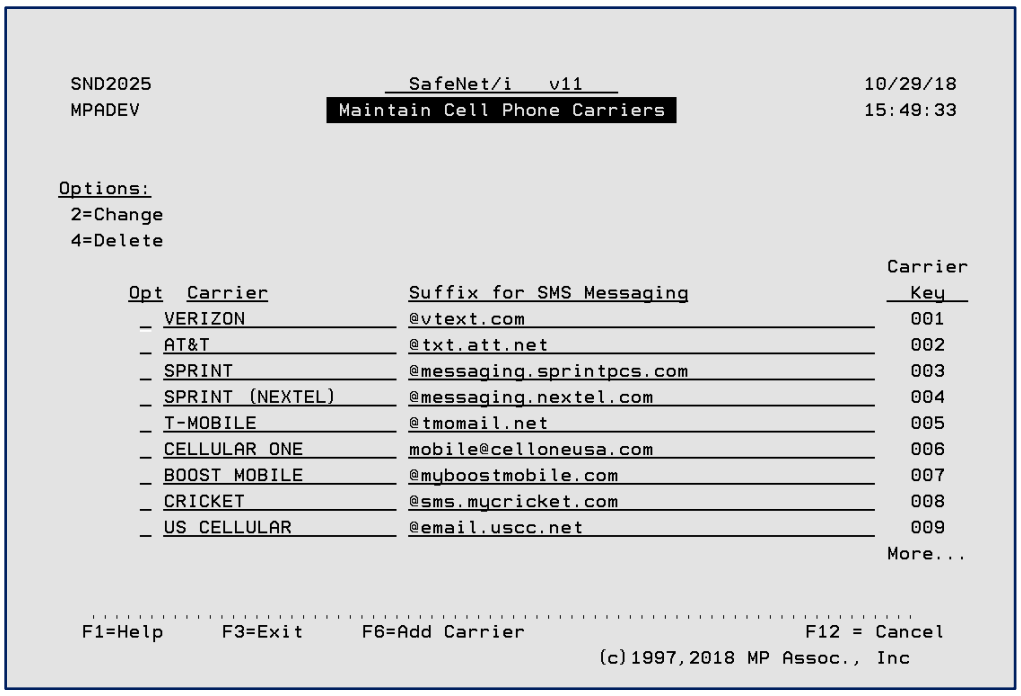


You can view an individual user or all log entries.

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



Menu Option 8 - Work with Cell Carrier SMS Addresses

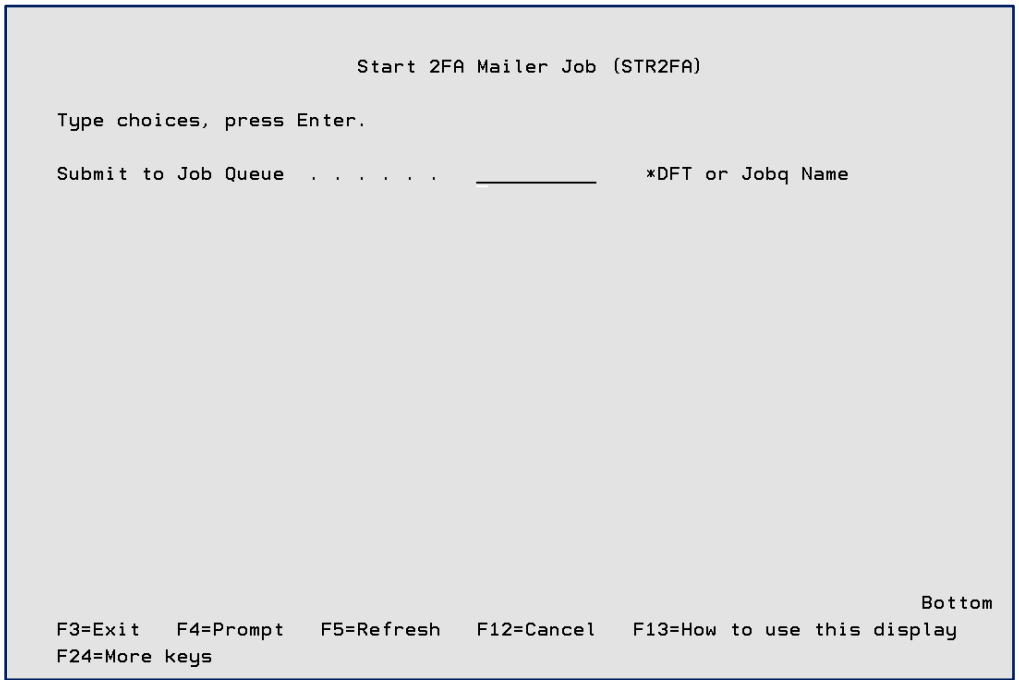


If you need to add a new cell carrier, use F6 to add a new entry.

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

https://avtech.com/articles/138/list-of-email-to-sms-addresses/

Menu Option 9 – Start Passcode Sender Job



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

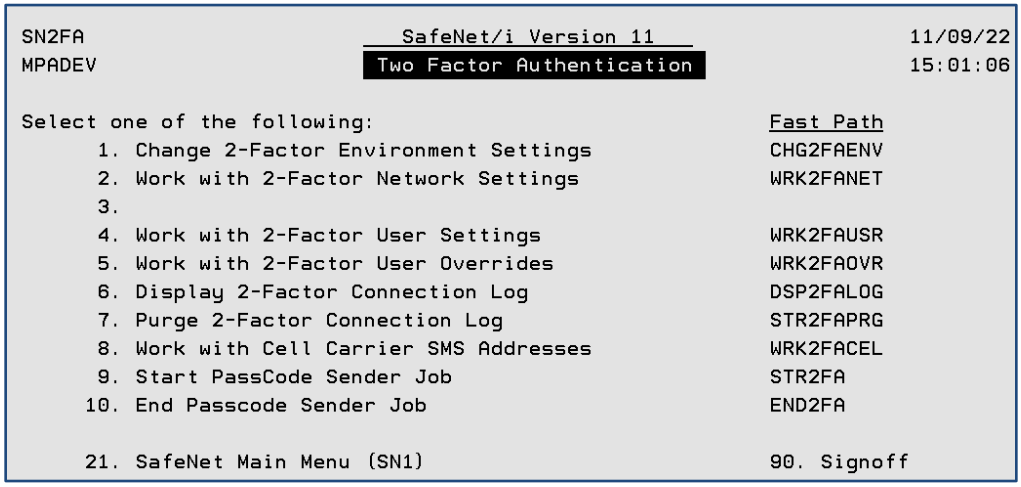
SN2FA01PF -	User controls
SN2FA02PF -	User Overrides
SN2FA10PF -	Cell phone Carrier codes
SN2FA20PF -	Network settings for 2FA
SN2FA99PF -	Historic Log file of 2FA connections
SN2FA98PF -	Contains Log of 2FA connections for FTP sessions

Chapter 3 - Two-Factor Authentication for SafeNet Web-Central

You can control access to Web-Central using **SafeNet/i** 2FA

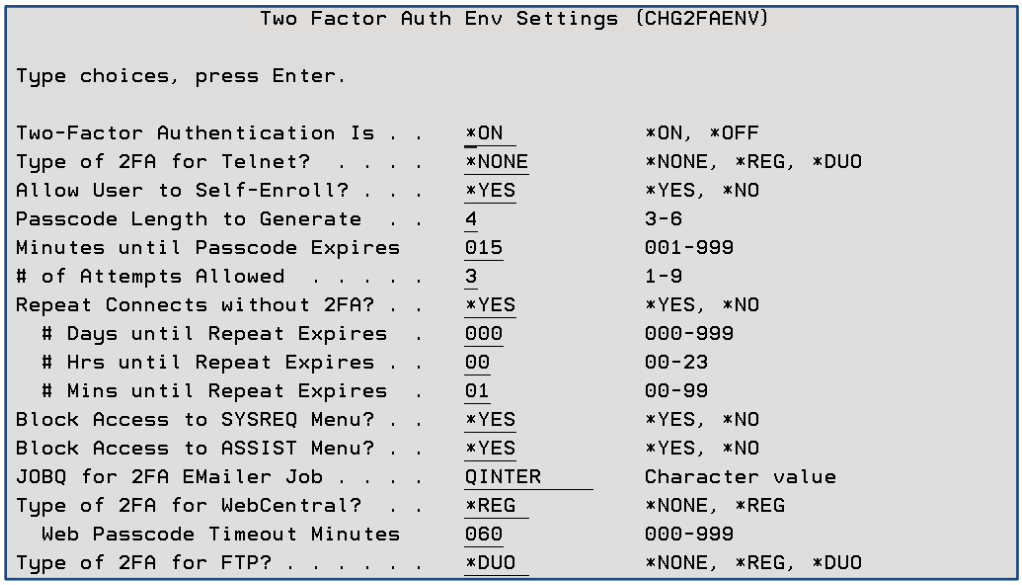
1. Configure 2FA settings for your network and users

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



2. Enabling and Activating Two-Factor Authentication for Web-Central

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



- Set *Two-Factor Authentication* to **ON*

- Set *Type of 2FA for WebCentral* to **REG*

  Or use command **CHG2FAENV WEB2FATYP(*REG)**

  2FA for Web-Central is ONLY available with standard SafeNet 2FA.

3. To add users to 2FA for Web-Central select **Menu Option 4 – Work with 2-Factor User Settings (WRK2FAUSR)**

4. Using the same CHG2FAENV command, you can set a session timeout value with *Web Passcode Timeout Minutes* (parameter **WEBTIMEOUT)**. Once this time limit is reached, the user will be required to re-do the 2FA process.

5. Restart Web-Central if active, or just start Web-Central

   a. ENDTCPSVR SERVER(*HTTP) HTTPSVR(WEBCENTRAL)
   b. STRTCPSVR SERVER(*HTTP) HTTPSVR(WEBCENTRAL)

6. Sign on to Web-Central with a user that has 2FA contact info already entered. If the user does NOT have 2FA contact info, they will be unable to sign on.

   User will either be sent a passcode or a selection list of addresses will be presented.

When *Sign in* is clicked, the user will be prompted for a passcode

The passcode will be sent to their email or their phone, depending on how they are set up for 2FA in **SafeNet/i**.

Multi-Address selection prompt:

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

After the passcode is entered, the user will see the *Web-Central Welcome Screen*

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

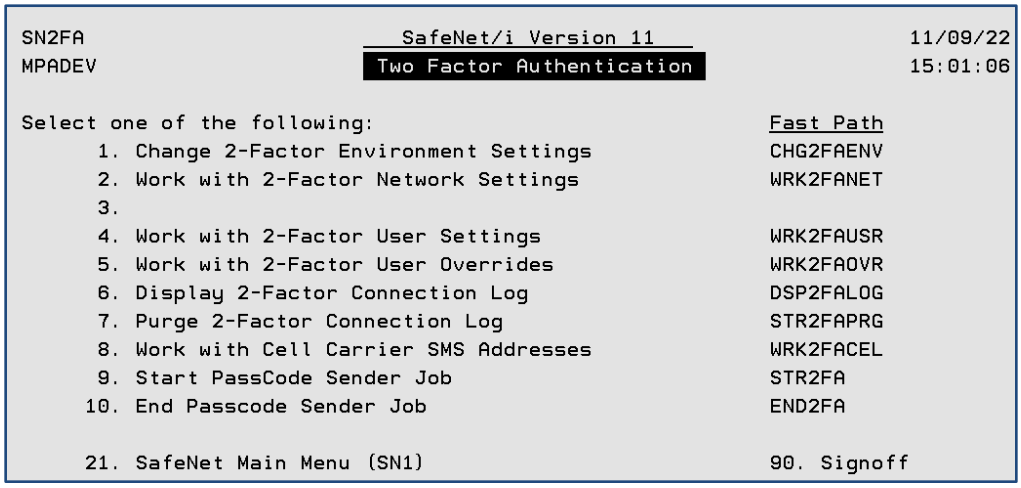
Chapter 4 - Two-Factor Authentication for FTP

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

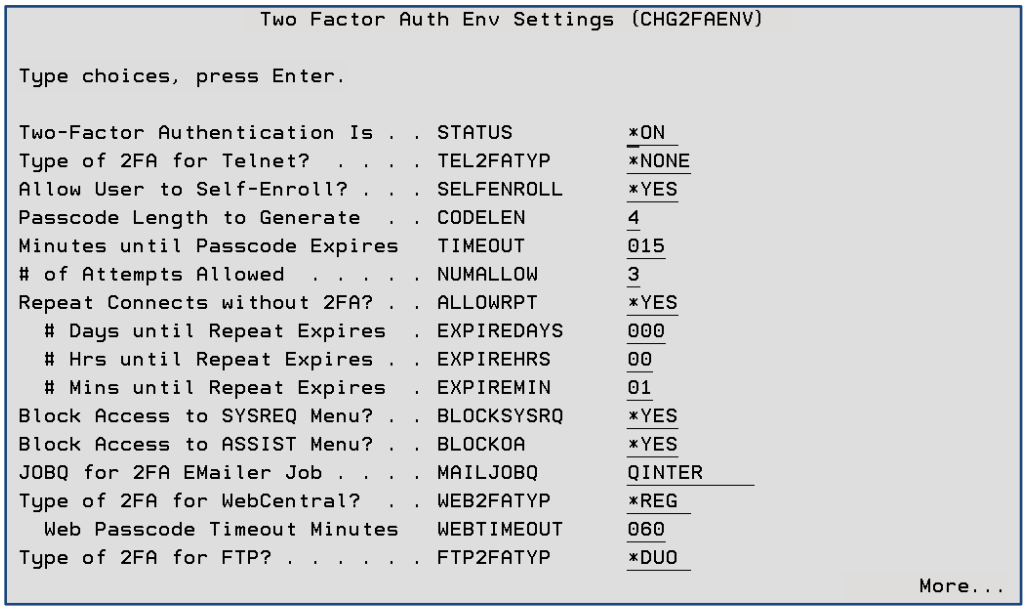
   - From the SafeNet/i Main Menu, select **Option 25 – Two Factor Authentication**



   - 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**
   - Set Two-Factor Authentication to **ON*
   - Set *Type of 2FA for FTP* to **REG* or **DUO*



- Or use commands

  Enable: **CHG2FAENV STATUS(*ON)**

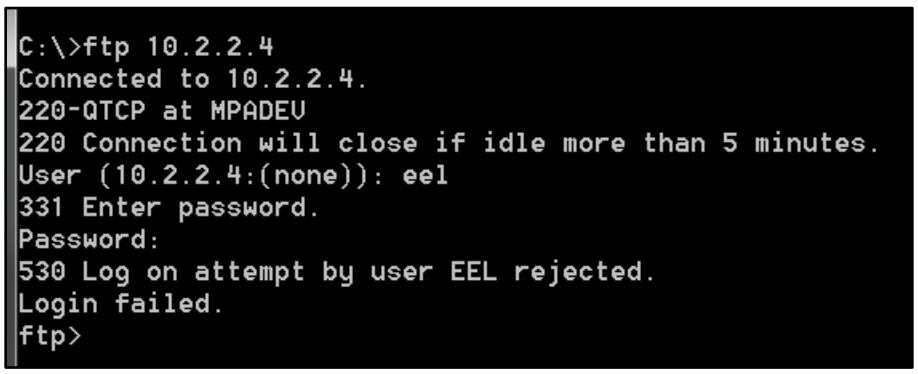
  Activate: **CHG2FAENV FTP2FATYP(*DUO)**

- **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.**



- 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 kConnect** with Twilio® SMS messaging to send alerts.

Please visit the Kisco Systems website for information on Kisco kConnect and how to obtain the software.

Once Kisco kConnect 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

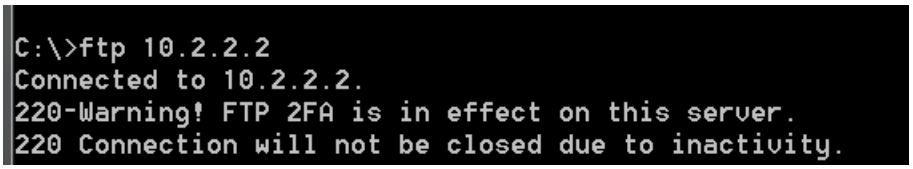
You can change the message to whatever you want, but remember the message will be reset when you do an OS upgrade.

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

To customize the message:

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

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



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/QTCPMSGF) 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 - Two Factor Authentication for SQL

1. Configure the *SafeNet SQL* server to use 2FA

   Use the **WRKSRV** command to set the **SQL Database Server - entry* to Security Level 3.

   Normal Server, User and SQL setup is required within SafeNet before using 2FA for SQL. See the SafeNet/i Reference Guide for specifics.

   Users must be configured in 2FA setup before activating 2FA for SQL.

2. Configure 2FA settings for your network and users

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

   Make sure *Two Factor Authentication* is set to **ON*

   Page Down and set *2FA for SQL* to **DUO*

```
                  Two Factor Auth Env Settings (CHG2FAENV)

Type choices, press Enter.

  FTP Passcode Timeout Minutes     005           000-999
2FA for SQL Access?  . . . . . .   *DUO          *NONE, *DUO
2FA for *SIGNON Server?  . . . .   *NONE         *NONE, *DUO
Use kConnect SMS Messaging?  . .   *YES          *YES, *NO
Use kConnect Account ID. . . . .   *DEFAULT      *DEFAULT, valid AcctId
```

   Configure additional settings for SQL

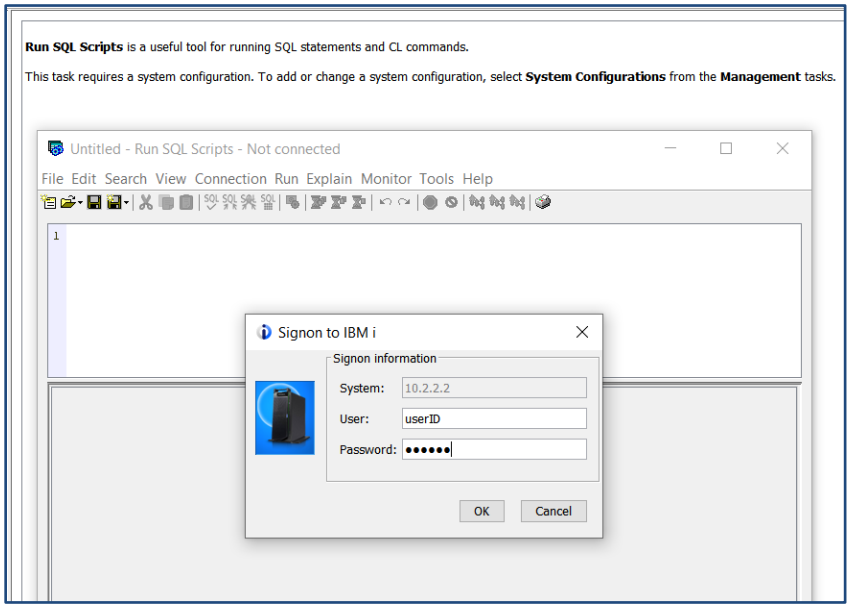
   Network - **Menu Option 2 – Work with 2-Factor Network Settings (WRK2FANET)**

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

3. After activating 2FA for SQL, users will be required to respond to 2FA prompting

   For example, using *IBM i Access Client Solutions*

   - Select *Run SQL Scripts*



   - When prompted, enter credentials

     The user will receive a DUO push

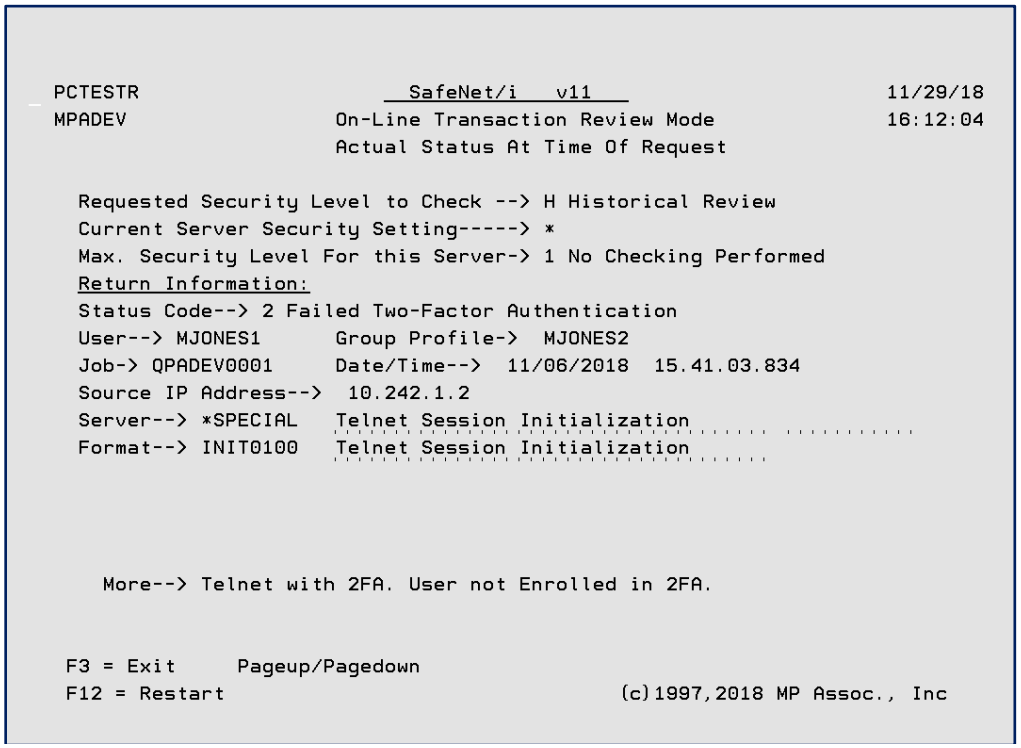
     When the user responds to the push, they will be granted access to SQL scripts

Chapter 6 - SafeNet 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



Chapter 7 – Deciding How to Use 2FA with SafeNet

There are three ways that you can choose to set up and use Two-Factor Authentication with SafeNet/i:

- Option 1 - Use regular 2FA within SafeNet/i
- Option 2 - Use kConnect and SMS for 2FA
- Option 3 - Use kConnect with DUO for 2FA

Each of these options is described in the following pages.

Option 1: Use Regular 2FA with SafeNet (Sends Numeric Passcodes)

This option does not use Kisco's kConnect product. The 2FA passcodes will be sent using regular SMTP email or SMTP email to SMS.

This method can only be used to control Telnet and FTP access.

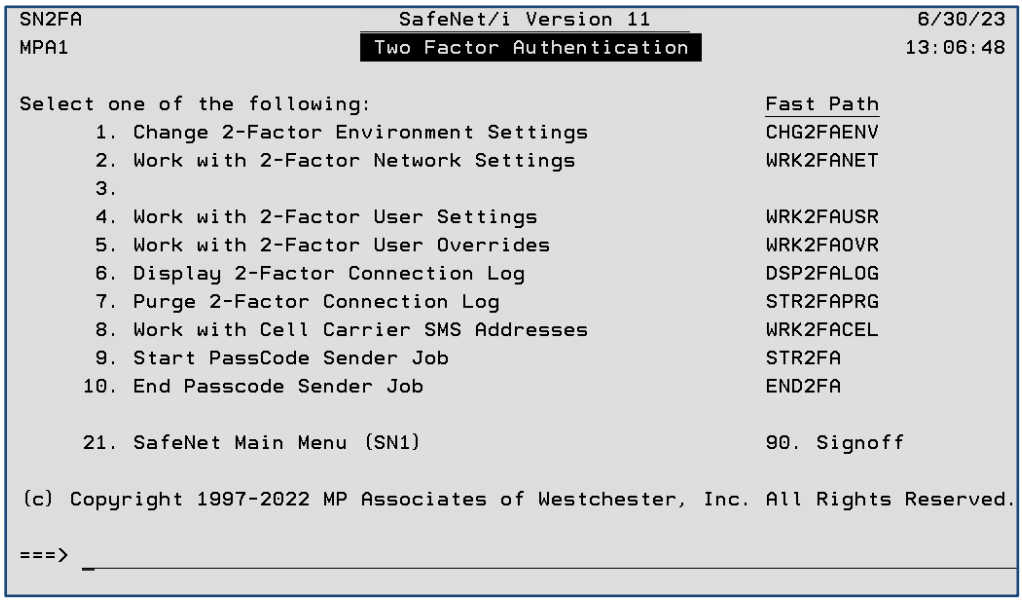
Software required:

1. Install and configure SafeNet/i using regular instructions
2. Install optional SafeNet/i 2FA module. See Chapter 2 in this guide for instructions.

Steps to set up and configure 2FA

After installing the optional SafeNet/i 2FA module, go to the 2FA main menu:

GO PCSEC2FA/SN2FA



Use Menu Options in this order:

- Option 2 - Setup Network Settings for 2FA controls
- Option 4 - Setup Users in 2FA
- Option 5 - Setup any User Overrides for 2FA
- Option 8 - Update or add Cell Carrier SMS info
- Option 9 - Start the Passcode Sender job and add same to system startup.
- Option 1 - Make changes to the 2FA Environment Settings

Notes:

- Do not use *DUO options for this type of setup
- 2FA for *SQL access is **NOT** supported with regular 2FA
- kConnect is not to be used in this configuration
- See Chapter 2 in this guide for additional information on setup and configuration
- Finally, TURN ON 2FA by changing the first parameter in CHG2FAENV to *ON

Considerations:

1. If you are using 2FA for *Telnet, change each user profile's initial program to PCSEC2FA/SN2FA1CL if they will be using 2FA for system access.

   Only change the profile if using 2FA for Telnet. This is not required for 2FA over FTP.

   You may want to test with one profile first before changing all your profiles.

2. If you are going to use 2FA to control FTP access, make sure you review the SafeNet/i 2FA section in this guide for an overview of the logon process needed with FTP.

3. For Telnet access, test access for a single user to verify the SMTP passcodes sender is operational.

Option 2: Using kConnect and SMS for 2FA with SafeNet (Sends Numeric Passcodes)

This option uses Kisco Systems kConnect product to send the 2FA passcodes via SMS thru Twilio® or Telesign®.

This method can only be used to control Telnet and FTP access using 2FA.

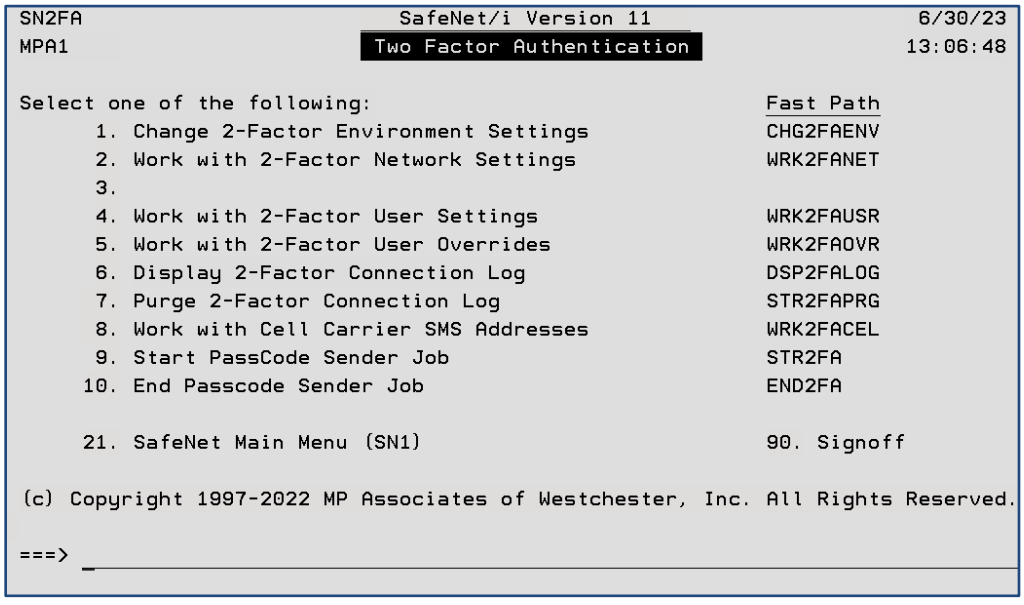
Software required:

1. Install and configure SafeNet/i using regular instructions
2. Install the SafeNet 2FA module; see instructions in Chapter 2 of this guide
3. Install Kisco's kConnect product and configure SMS messaging (using Twilio® or Telesign®)

Steps to set up and configure 2FA

After installing SafeNet/i, the SafeNet/i 2FA module and kConnect, go to the 2FA main menu:

GO PCSEC2FA/SN2FA



Verify SMS messaging is operational by using the command **KCONNECT/KSNDSMS**

Use Menu Options in this order:

- Option 2 - Setup Network Control Settings for 2FA
- Option 4 - Setup Users in 2FA

- Option 5 - Setup any User Overrides for 2FA
- Option 9 - Start the Passcode Sender job and add same to system startup program
- Option 1 - Make any required changes to the 2FA environment settings

  Specifically, you will need to change the value of the *KCONNECT* parameter to **YES* to use SMS messaging via kConnect.

Notes:

- Do not use any *DUO options for this type of setup.
- 2FA for *SQL access is not supported with regular 2FA. It is only available when using DUO authentication.
- See SafeNet 2FA documentation for additional information on setup and configuration of 2FA.
- Finally, turn *ON 2FA by changing the first parameter in CHG2FAENV to ***ON**.

Considerations:

1. If you are using SafeNet/i 2FA for *Telnet, change each user profile's initial program to PCSEC2FA/SN2FA1CL if that user will be using 2FA for system access.

   Only change the profile if using 2FA for Telnet. This is not required for 2FA over FTP.

   You may want to test with one profile first before changing all your profiles.

2. If you are going to use 2FA to control FTP access, make sure you review Chapter 4 in this guide for an overview of the "double" logon process needed with 2FA and FTP.

3. For Telnet access, test a single user access to verify the SMTP Passcodes Sender is operational.

Option 3: Using kConnect with DUO® for 2FA with SafeNet (Uses DUO® Mobile Authenticator App)

This option uses Kisco Systems' **SafeNet/i** and kConnect products with the DUO® Mobile Authenticator for actual 2FA.

This method can be used to control **Telnet, FTP and *SQL** access using 2FA.

Software required:

1. Install and configure SafeNet/i using the regular SafeNet/i instructions
2. Install the SafeNet/i 2FA module
3. If you will be using regular SMTP emails for DUO user invitations, activate the SafeNet/i 2FA Passcode Sender job. See Chapter 2 in this guide for instructions.
4. If you plan on using the kConnect SMS messaging feature for sending DUO® user invitations, you will need to install and configure Kisco Systems' kConnect product and activate a Twilio® or a Telesign® SMS account.
5. For DUO® 2FA, if you haven't already done so, install Kisco Systems' kConnect product, activate a DUO® account and configure the DUO Authentication feature. See kConnect documentation.

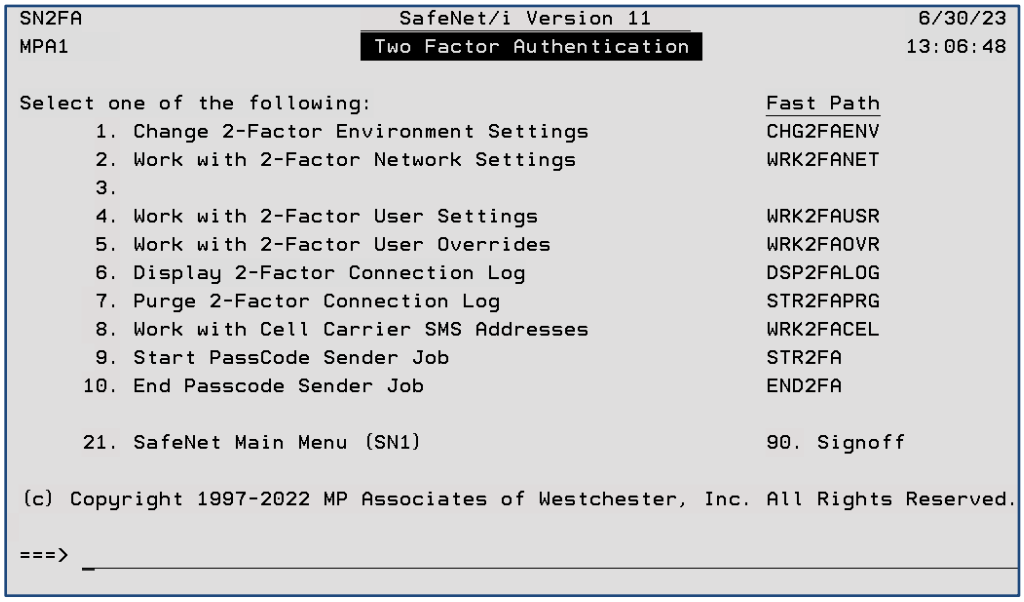
Steps to set up and configure 2FA with SafeNet and kConnect DUO

Verify SMS messaging is operational by using the command **KCONNECT/KSNDSMS**

Verify DUO is active and working.

Go to the 2FA main menu:

GO PCSEC2FA/SN2FA



Use Menu Options in this order:

- Option 2 - Setup Network Control Settings for SafeNet/i 2FA
- Option 4 - Setup Users in SafeNet/i 2FA
- Option 5 - Setup any needed User Overrides for SafeNet/i 2FA
  It is **NOT** necessary to setup a user's cell#, email address or the cell carrier information in SafeNet/i 2FA (Menu SN2FA options 4 & 8) if you are using kConnect SMS messaging for 2FA.
- Option 9 - Start the Passcode Sender job and add same to system startup program
- Option 1 - Make any required changes to the SafeNet/i 2FA environment settings. Specifically, you will need to change the value of the *KCONNECT* parameter to ***YES** to use SMS messaging via kConnect.

Notes:

- You can use the *DUO 2FA options for Telnet, FTP and SQL. You can also use *REG 2FA passcodes for any of the services as well.
- See Chapter 2 in this guide for additional information on setup and configuration of 2FA.
- Finally, turn *ON 2FA by changing the first parameter in CHG2FAENV to ***ON**.

Considerations:

1. If you are using SafeNet/i 2FA for *Telnet, change each user profile's initial program to PCSEC2FA/SN2FA1CL if that user will be using 2FA for system access.

2. If you will be using Kisco's i2Pass product for Telnet 2FA, only change the profile if using 2FA for *Telnet. This profile change is not required for 2FA over FTP or 2FA for SQL.

   You may want to test with one profile first before changing all your profiles.

3. For Telnet access, test a single user's access to verify that 2FA using DUO is operational.

Chapter 8 – 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 SN2FASENDR job 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
  f. Is the security level for the Exit Point set to level 3 or higher in SafeNet/i? Server point must be set to a security level of 3 or higher. Use command WRKSRV to check current server security level.

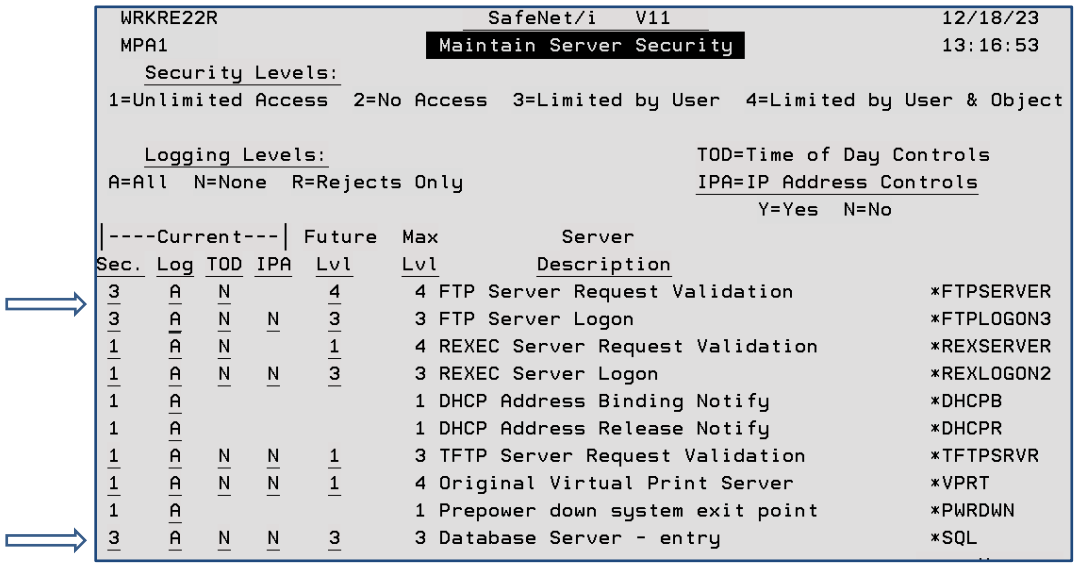
- The user can't access their own contact information when signing on
  a. Self-Enrollment is not active. See command CHG2FAENV parameter SELFENROLL

- **SafeNet/i** Web-Central is not prompting for passcode
  a. Make sure 2FA is activated for Web-Central – see command CHG2FAENV parameter WEB2FATYP

Check Server Settings in SafeNet/i WRKSRV

Issue - Users are logging in without getting a *DUO or *REG prompt

Make sure the FTP and SQL servers are set to limit user access



```
 WRKRE22R                        SafeNet/i    V11                    12/18/23
 MPA1                        Maintain Server Security                13:16:53
   Security Levels:
1=Unlimited Access  2=No Access  3=Limited by User  4=Limited by User & Object

   Logging Levels:                                  TOD=Time of Day Controls
A=All  N=None  R=Rejects Only                       IPA=IP Address Controls
                                                         Y=Yes  N=No
|----Current---| Future  Max          Server
Sec. Log TOD IPA  Lvl    Lvl        Description
 3    A   N        4      4 FTP Server Request Validation          *FTPSERVER
 3    A   N   N    3      3 FTP Server Logon                       *FTPLOGON3
 1    A   N        1      4 REXEC Server Request Validation        *REXSERVER
 1    A   N   N    3      3 REXEC Server Logon                     *REXLOGON2
 1    A                   1 DHCP Address Binding Notify           *DHCPB
 1    A                   1 DHCP Address Release Notify           *DHCPR
 1    A   N   N    1      3 TFTP Server Request Validation        *TFTPSRVR
 1    A   N   N    1      4 Original Virtual Print Server         *VPRT
 1    A                   1 Prepower down system exit point       *PWRDWN
 3    A   N   N    3      3 Database Server - entry               *SQL
```