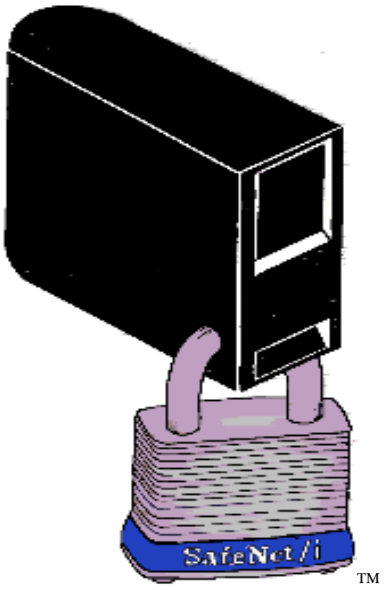
SafeNet/i

FOR IBM i

TWO-FACTOR AUTHENTICATION

Version 11



™

© 2018 MP Associates of Westchester, Inc.

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
SafeNet/i Support Website: www.safeneti.com/safenet/support

Table of Contents

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 normal system PASSWORD and entry of a PASSCODE that is sent to the user via text to their phone or in an email.

© Copyright 2018 MP Associates of Westchester, Inc.

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 temporary passcode.

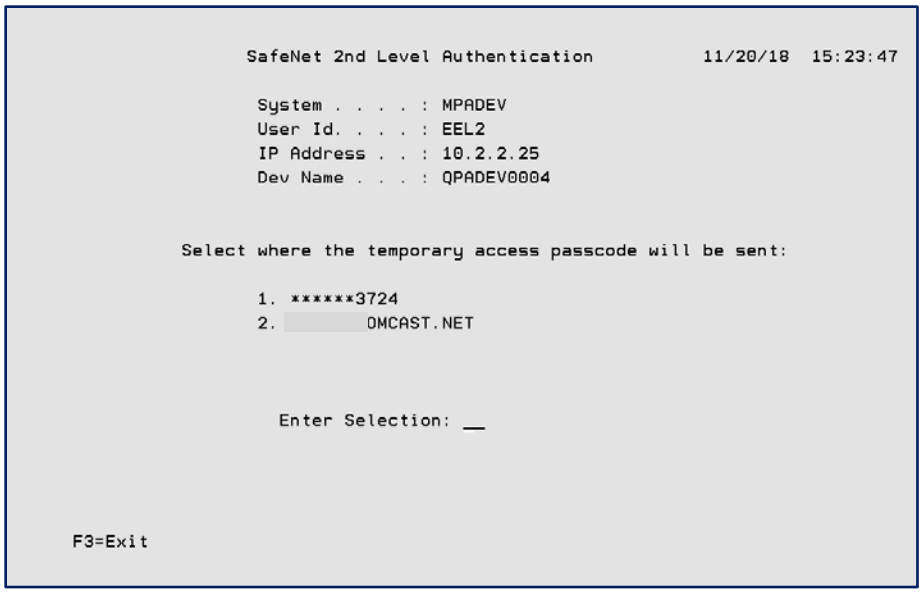
1. User signs on to a 5250 session as normal.

2. User will be sent a passcode either via email or SMS text message.

   - 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.

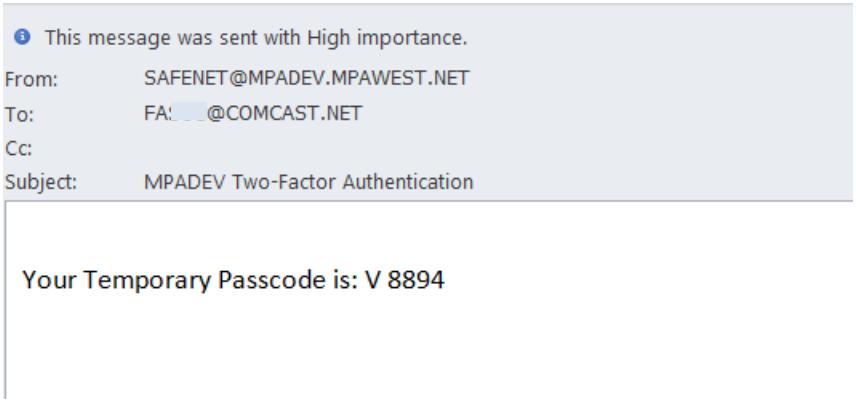
The passcode is assigned a “session” prefix that is automatically appended to the email and entry page.

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.

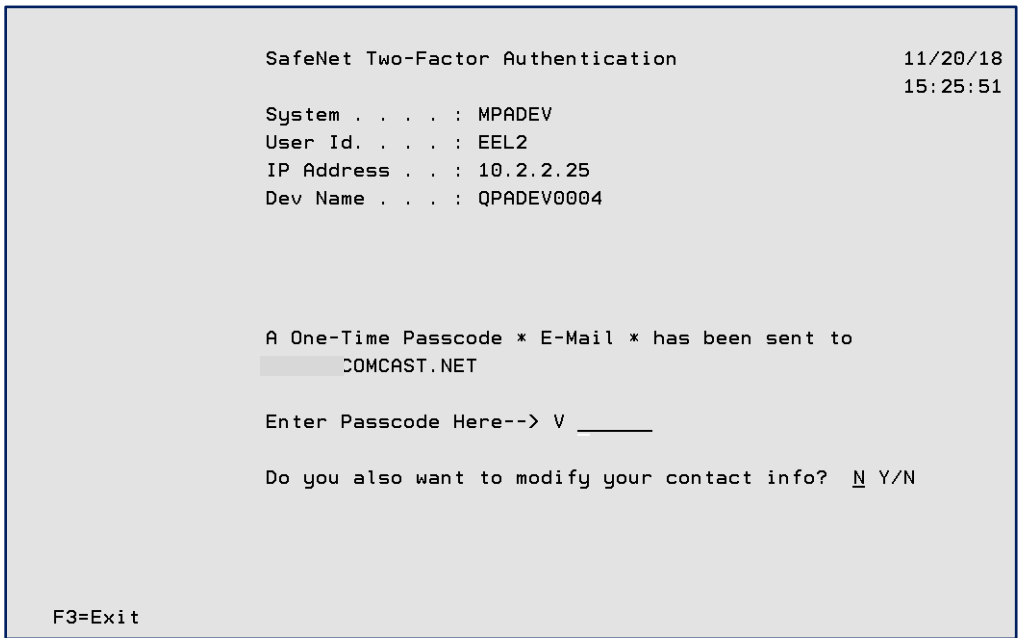
© Copyright 2018 MP Associates of Westchester, Inc.

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

Sample of a temporary passcode email:



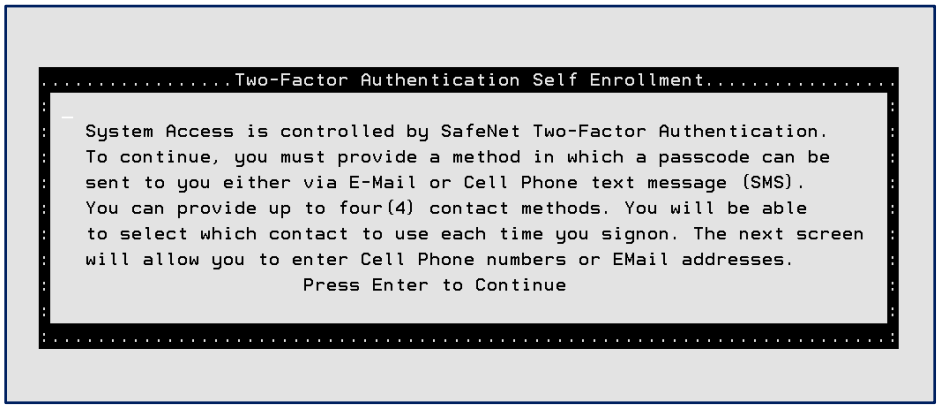
When the user receives the passcode, they will key it on the passcode entry screen



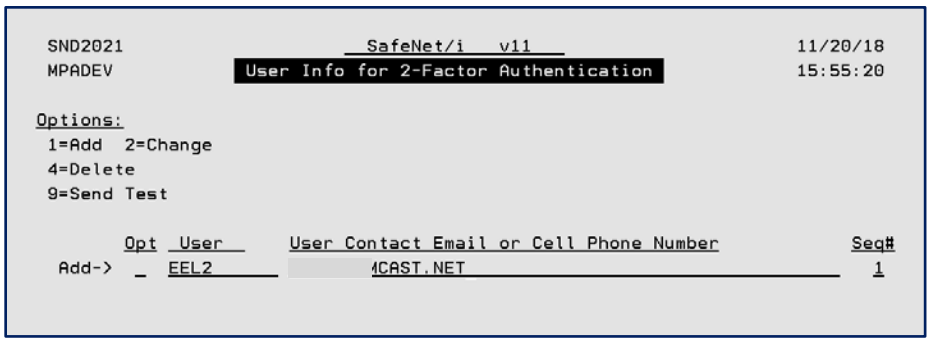
3. If the user does NOT have any contact entries on file, and if the system is set for Self-Enrollment, they will have the opportunity to enter their contact information upon successful sign on.

© Copyright 2018 MP Associates of Westchester, Inc.

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

You can allow users to manage their own contact information any time after a successful passcode entry by activating the Self-Enrollment feature. See command CHG2FAENV.

Important: If Self-enrollment is not active, users will not be able to enter or maintain their contact information themselves.

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.

© Copyright 2018 MP Associates of Westchester, Inc.

Chapter 2 - SafeNet/i Two-Factor Authentication Setup

Before you can use **SafeNet/i** Two-Factor Authentication (2FA) you must:

1. Perform the steps in the ***Installation Process***
2. Perform the ***Post-installation Steps***
3. Complete the tasks in ***Initial Setup***

Installation Process

1. Before you begin, make sure you have the latest PTF level for the base SafeNet/i code installed. Visit the SafeNet/i website to verify the current level available, and install PTF if necessary.

2. Run the install program **INST2FA** from the **PCSECLIB** library.

   CALL PCSECLIB/INST2FA

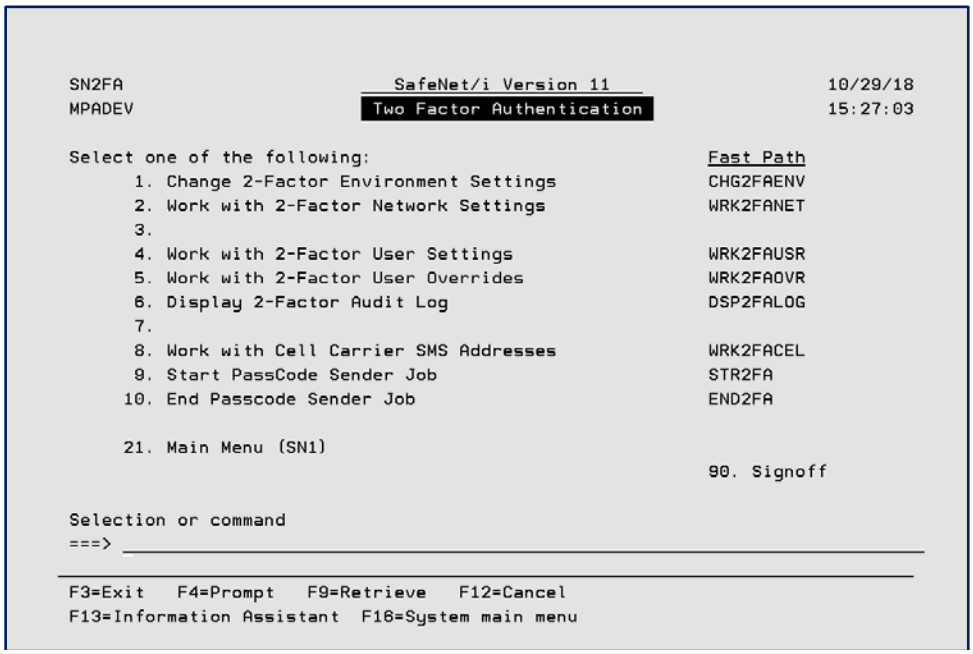
   This program:
   - Creates the required user profile SN2FAUSER for 2FA processes
   - Creates a data area in PCSECLIB that contains the pointers to 2FA library
   - Saves a backup copy of the current PCSEC2FA library into library PCSEC2FAOL
   - Restores the new PCSEC2FA library
   - Copies in any user data from the backup library created during the install.

When the installation is complete, go to the **SafeNet/i** Two-Factor Authentication menu:

GO PCSEC2FA/SN2FA

© Copyright 2018 MP Associates of Westchester, Inc.

SafeNet/i Two-Factor Authentication – Menu SN2FA



From the Two Factor Authentication Menu (SN2FA) select **Option 1 - Change 2-Factor Environment Settings** or use **CHG2FAENV** command

Some of the two-factor environment values you can set:

- The 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.
- Specify the JOBQ where the passcode sender job will be submitted.

Continue with the SafeNet/i 2FA ***Post Installation Steps***

© Copyright 2018 MP Associates of Westchester, Inc.

Post-Installation Steps

For 2FA to operate correctly the following steps MUST be done. **Details regarding each of these steps/programs are provided later in this guide.**

1. On each user profile that requires 2FA, you must change that user profiles' initial program to call the 2FA program. (PCSEC2FA/SN2FA1CL)

2. Start the 2FA passcode sender job (PCSEC2FA/STR2FA) and add that command to your system startup program.

3. Change the interactive subsystem(s) signon display file to protect the "Program or Procedure" field or use one provided by us.

   See *Special 2FA Setup Considerations* on page 2.5 for details.

Continue with *Initial Setup*.

© Copyright 2018 MP Associates of Westchester, Inc.

Initial Setup

Using the Two Factor Authentication Menu (SN2FA):

1. Select **Option 9 - Start Passcode Sender Job** or use **STR2FA** command to start the emailer server job. The submitted job is call **SN2FASNDR** and by default will be submitted to QINTER.

   - 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

     Important: 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 use **WRK2FANET** command to set up your "safe" networks where 2FA is not required.

3. Select **Option 4 - Work with 2-Factor User Settings** or use **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. Use **Option 5 - Work with 2-Factor User Overrides** or use **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**.

This 2FA program should be one of the very FIRST items called if you are going to include it in your own custom initial program.

© Copyright 2018 MP Associates of Westchester, Inc.

Verify and test SMTP sending

SMTP must be configured and active on your system for 2FA to operate. Please verify that SMTP is already configured on your system.

You can test a two-factor passcode email/SMS text by doing the following **after** you have completed the initial installation and start the email sender job.

1. Make sure the passcode sender job (SN2FASNDR) is active. See command STR2FA.
2. Setup a users' contact information using **Option 4 - Work with 2-Factor User Settings** from menu SN2FA or use **WRK2FAUSR** command.
3. Put an option "9" next to one of the user contact records to send a test and press enter.

If you don't receive the test passcode email or text message, see the *2FA Problem Determination* section of this manual.

© Copyright 2018 MP Associates of Westchester, Inc.

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)
```

Remember: you must restart the QINTER subsystem for this change to take effect. To avoid impacting your users, please confirm that no one is signed on before restarting.

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 this job.

Failure to start the emailer job will cause 2FA to be bypassed.

© Copyright 2018 MP Associates of Westchester, Inc.

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 the Two Factor Authentication Menu (SN2FA) **Option 8 – Work with Cell Carrier SMS Addresses** or **WRK2FACEL** command.

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

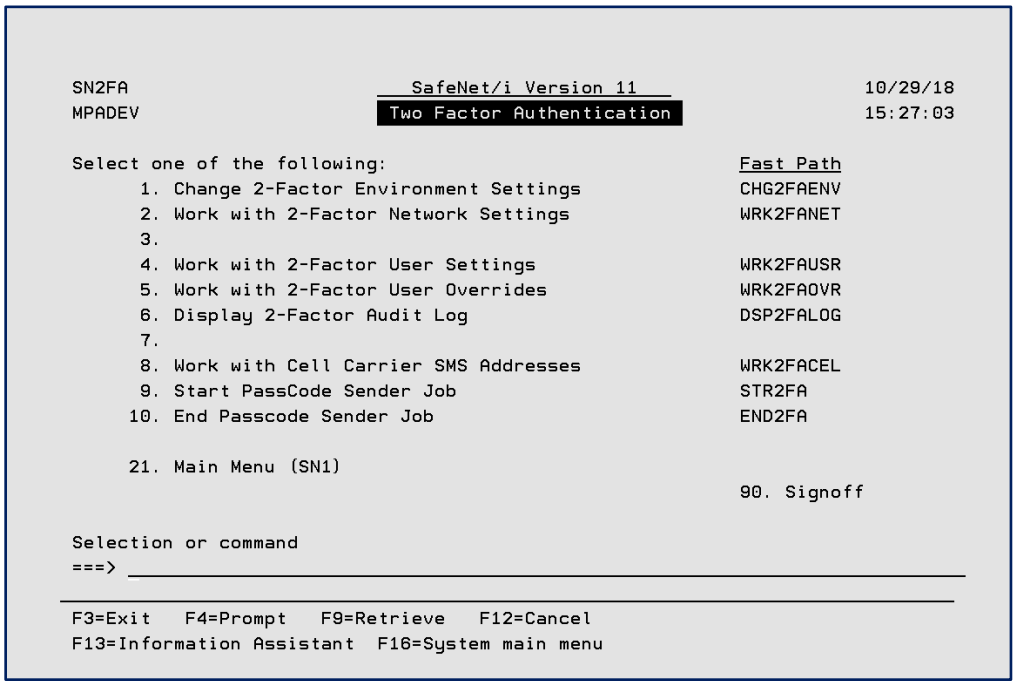
Use this link for an extensive list of available SMS codes for each carrier:

https://kb.sandisk.com/app/answers/detail/a_id/17056/~/list-of-mobile-carrier-gateway-addresses

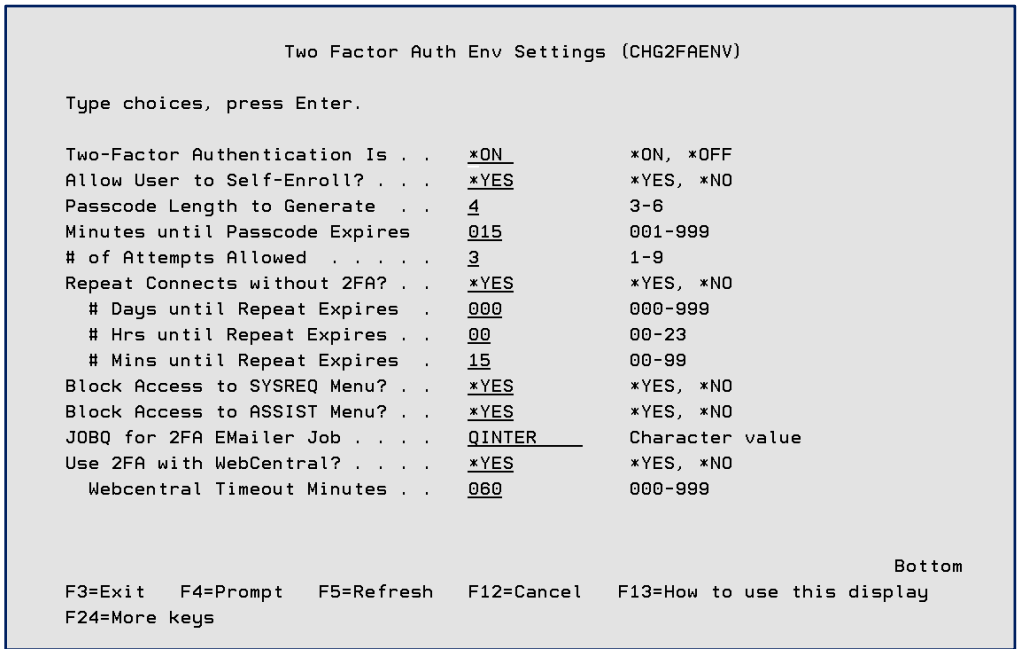
© Copyright 2018 MP Associates of Westchester, Inc.

Two Factor Authentication Menu (SN2FA) Options

GO PCSEC2FA/SN2FA



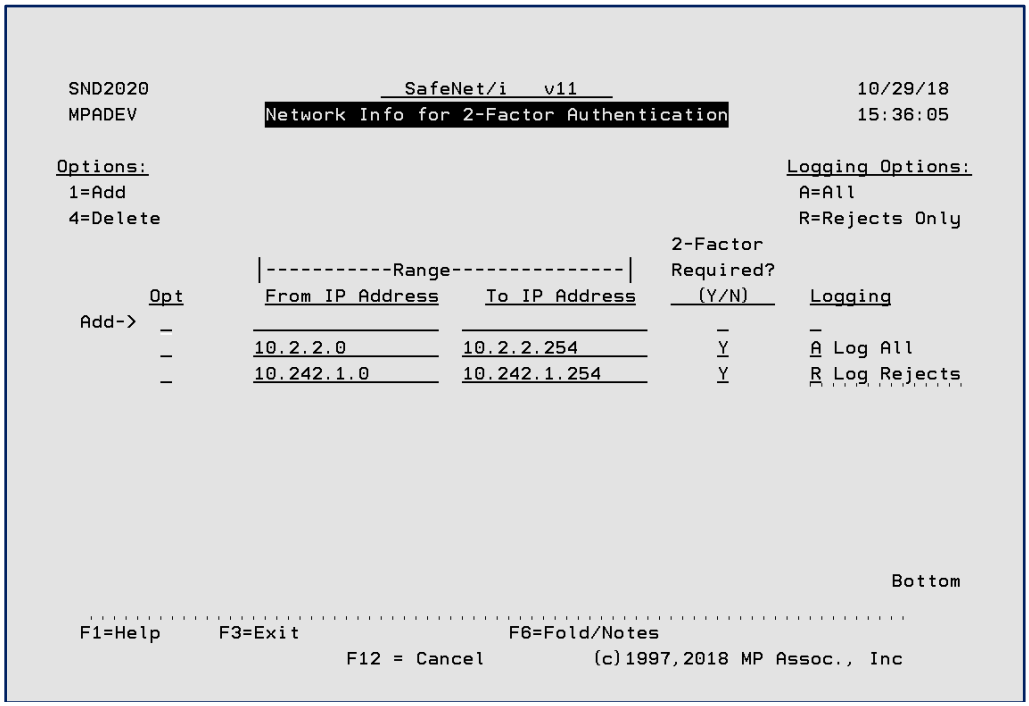
Menu Option 1 – Change 2-Factor Environment Settings



See Help text for explanation of parameters

© Copyright 2018 MP Associates of Westchester, Inc.

Menu Option 2 – Work with 2-Factor Network Settings



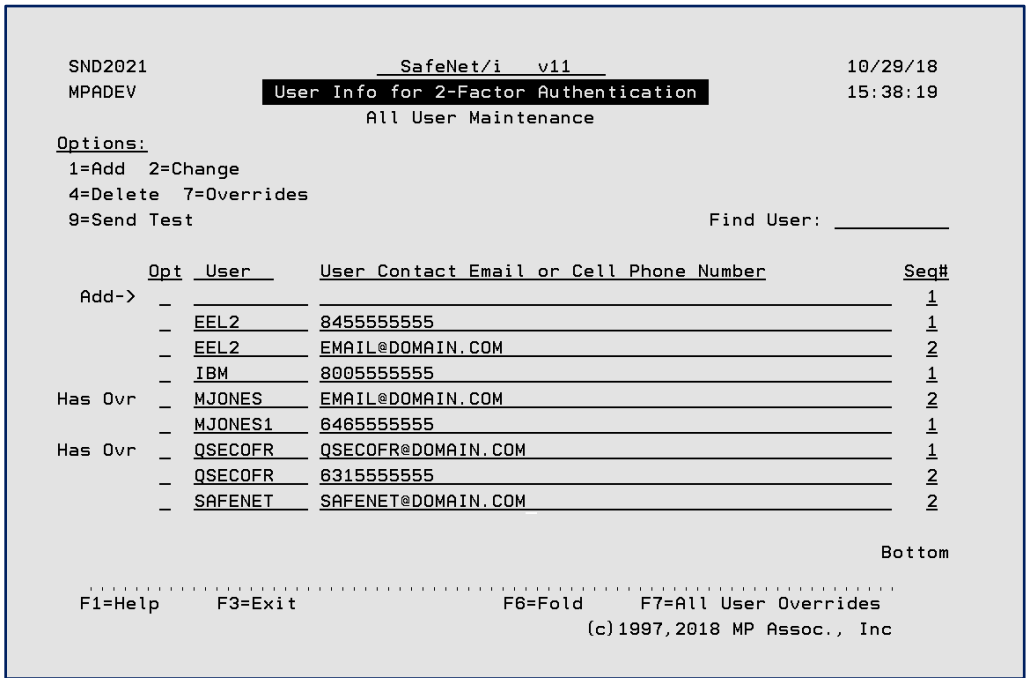
Use this option to indicate what network segments or IP address ranges you want to enforce 2FA or not.

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

Example:

If you do NOT want 2FA on you 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



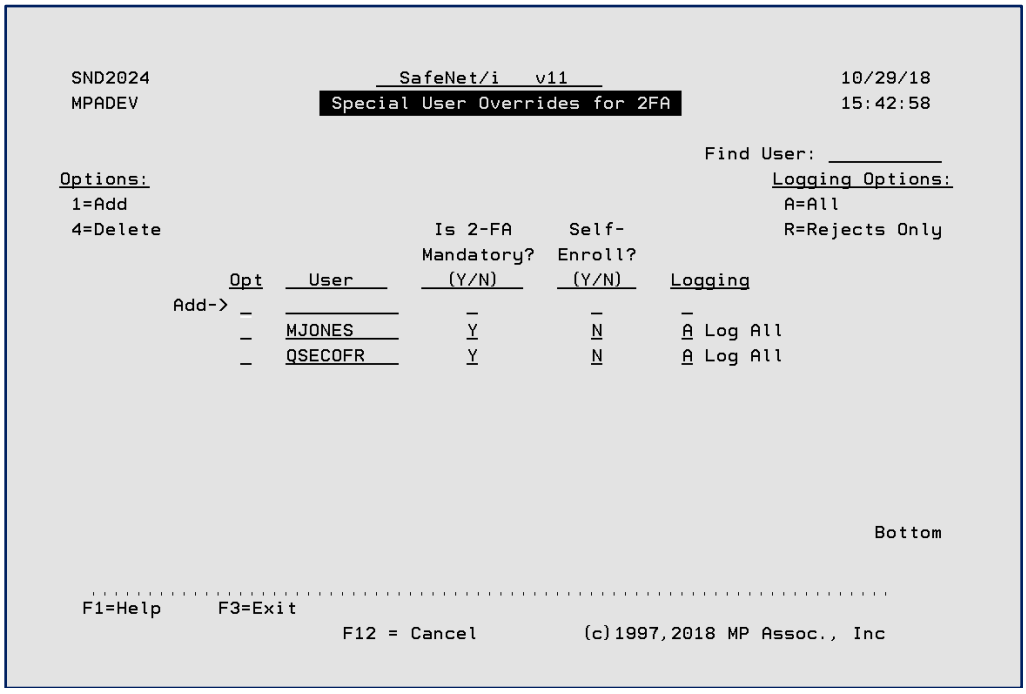
Use this screen to enter user 2FA contact information.

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.

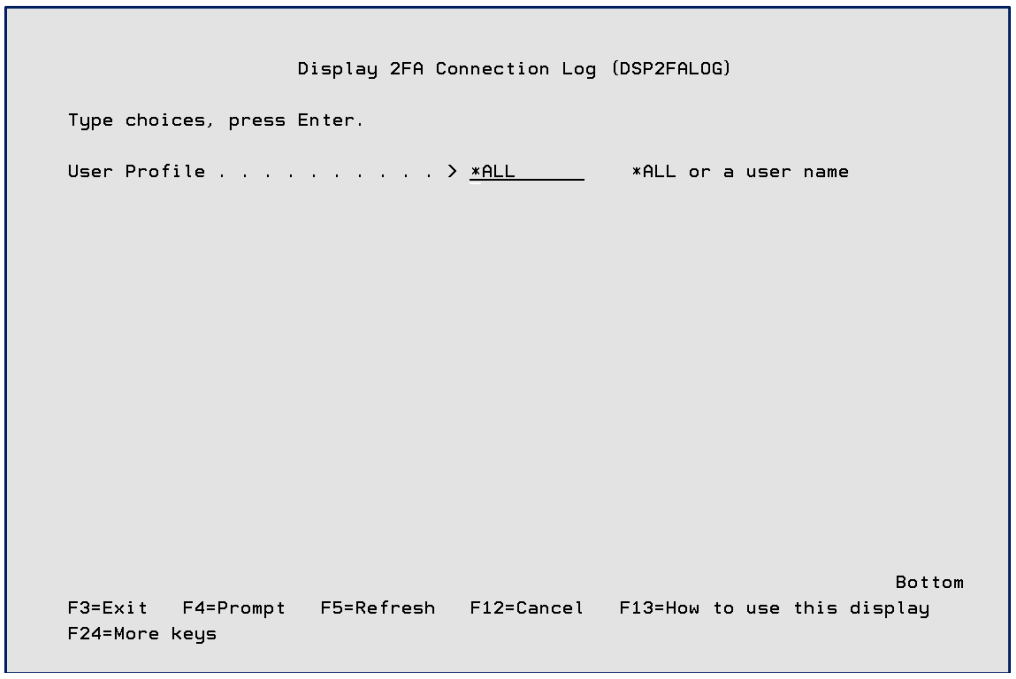
Menu Option 5 – Work with 2-Factor User Overrides



Use this screen to override user defaults. You can:

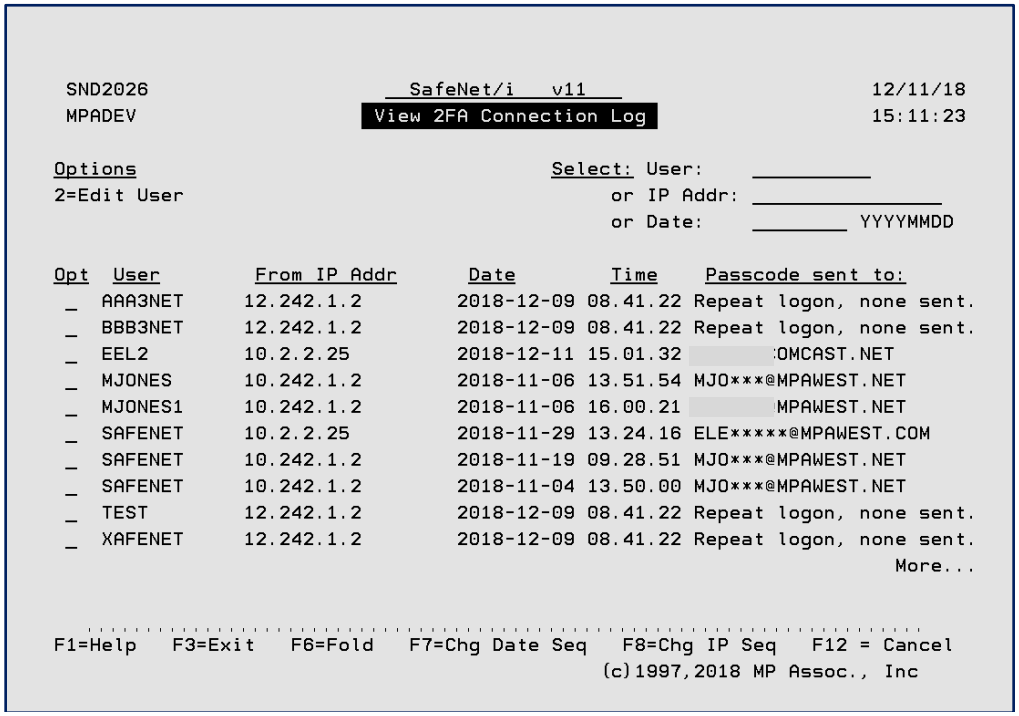
- Specify that a user ALWAYS needs to use 2FA regardless of the network.
- Override self-enrollment ability to limit access to user maintenance when a user signs on.
- Also override any logging values for the user.

Menu Option 6 – Display 2-Factor Audit Log

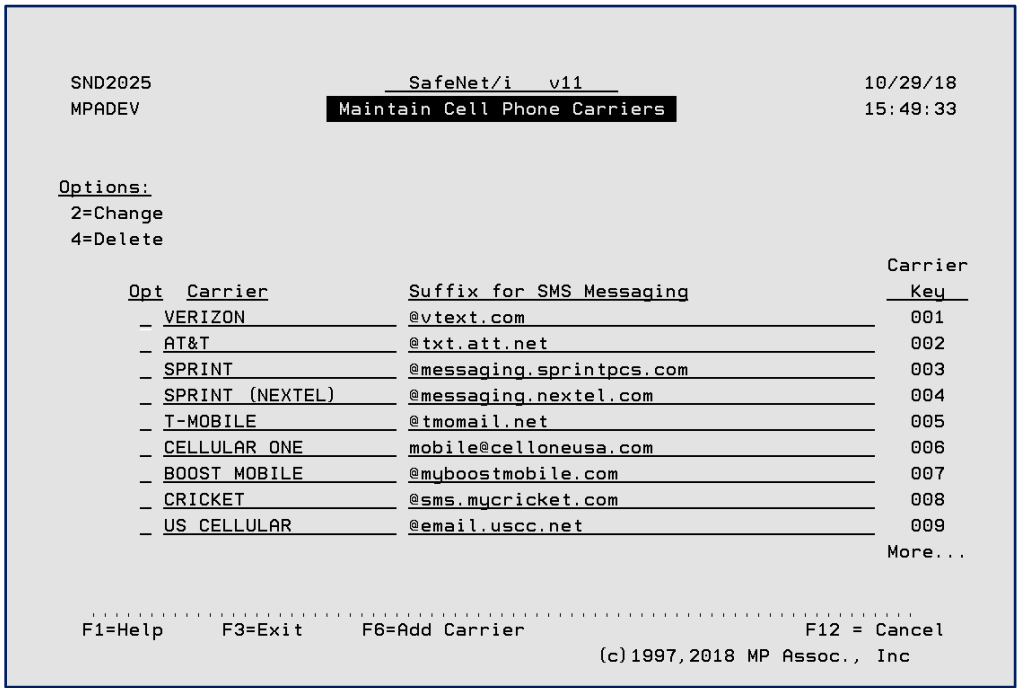


You can view an individual user or all log entries.

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

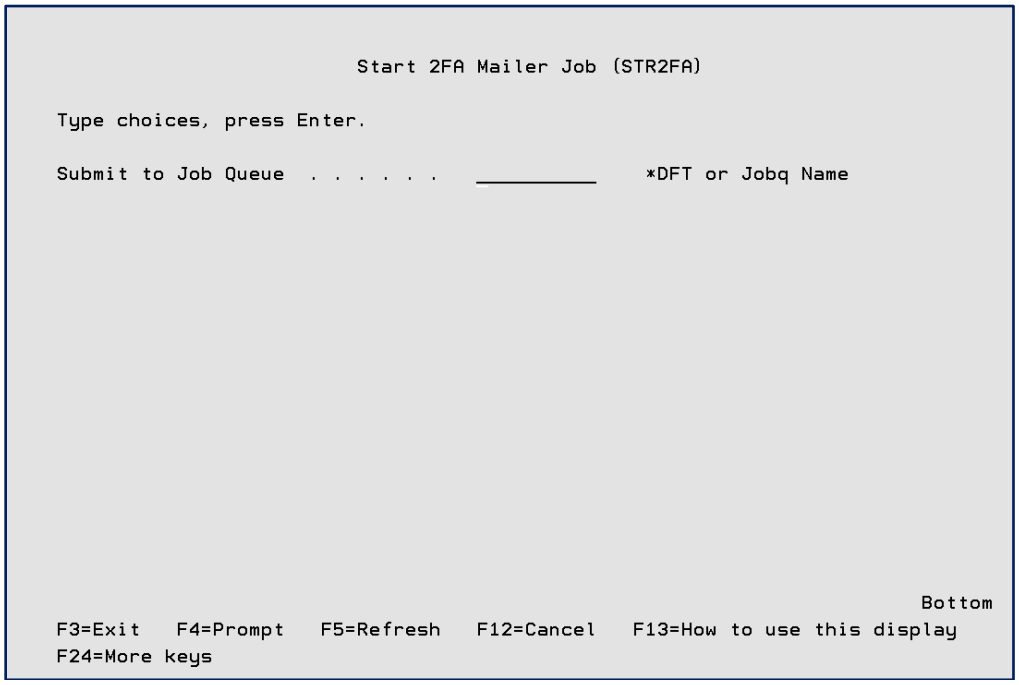


Menu Option 8 - Work with Cell Carrier SMS Addresses



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

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

© Copyright 2018 MP Associates of Westchester, Inc.

2FA Problem Determination

- The user is not being prompted for 2FA passcode when they signon.
  a. Is 2FA active on your system? – use command CHG2FAENV to check.
  b. Is the SN2FASNDR job that sends the passcodes 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. Do you allow repeat connections and are the connections within the allowed timeframe? – See command CHG2FAENV.

- 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.

© Copyright 2018 MP Associates of Westchester, Inc.

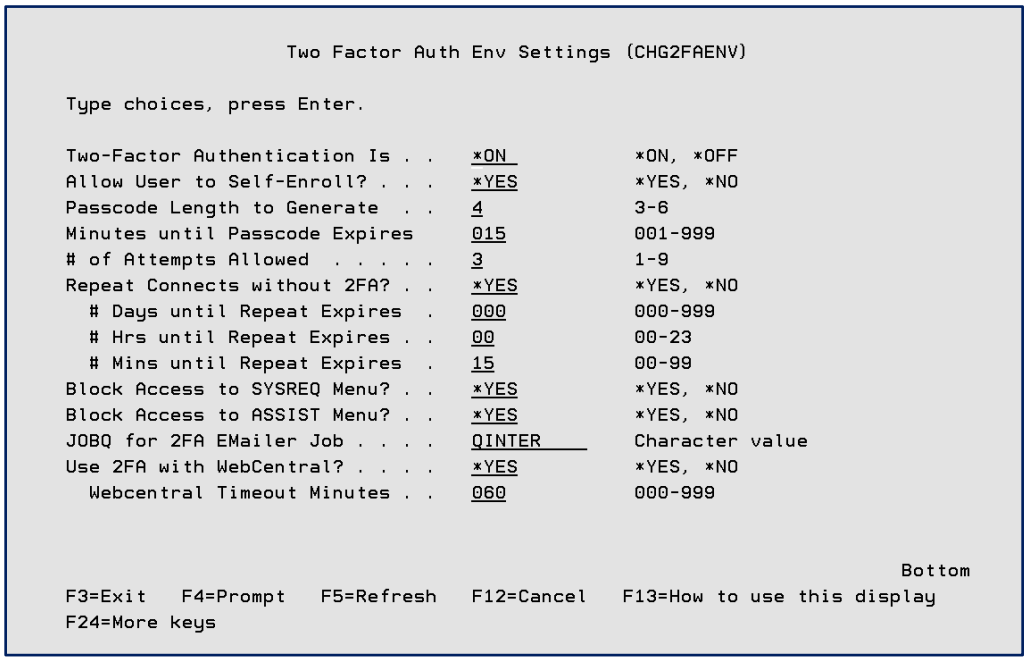
Chapter 3 - Two-Factor Authentication for SafeNet/i Web-Central

1. Enable Two-Factor Authentication for Web-Central

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

   OR

   Use command **CHG2FAENV WEBCENTRAL(*YES)**



```
                    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  .   15          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
  Webcentral Timeout Minutes . .   060         000-999


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

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

3. Restart Web-Central if active, or just start Web-Central
   - ENDTCPSVR SERVER(*HTTP) HTTPSVR(WEBCENTRAL)
   - STRTCPSVR SERVER(*HTTP) HTTPSVR(WEBCENTRAL)

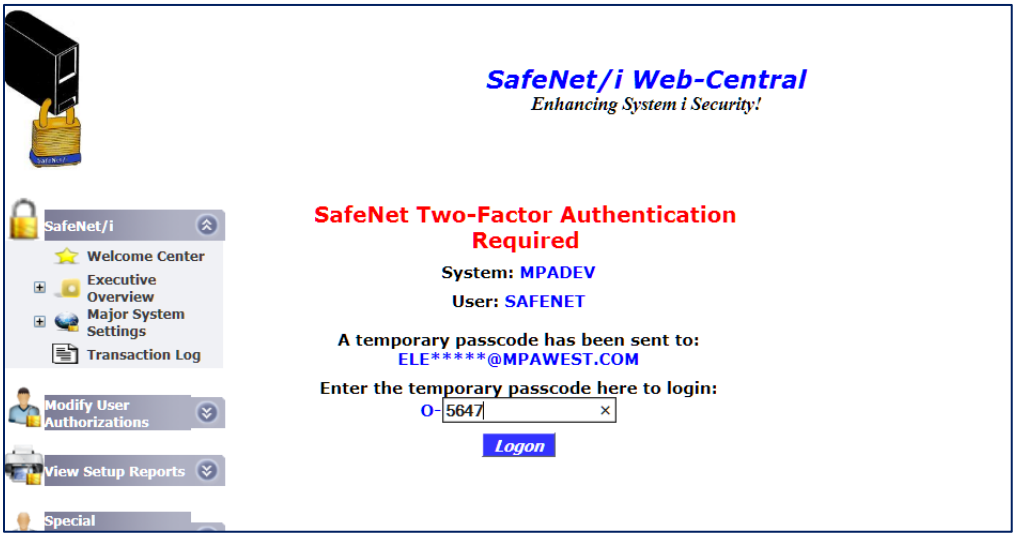
4. Sign on to Web-Central with a user that has 2FA contact info already entered. If the user does NOT have 2FA contact info, they will be unable to sign on.

© Copyright 2018 MP Associates of Westchester, Inc.

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

Multi-Address selection prompt:

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



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

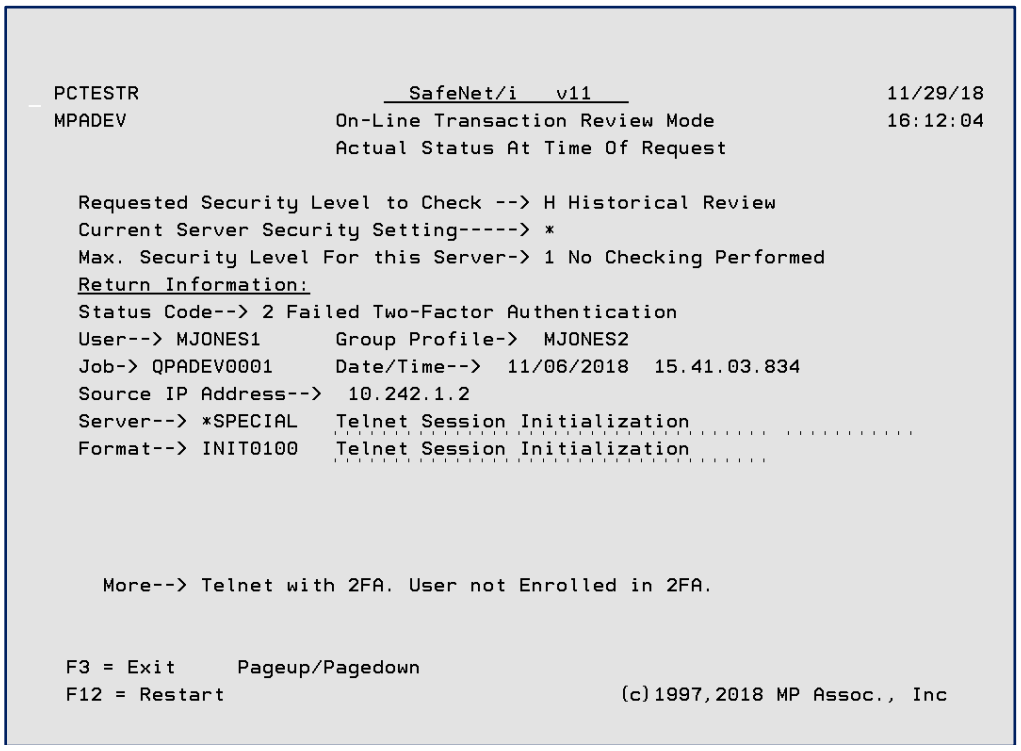
© Copyright 2018 MP Associates of Westchester, Inc.

Chapter 4 - 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



© Copyright 2018 MP Associates of Westchester, Inc.