

i2Pass

Two Factor Authentication for the IBM i

Version 3.03

As of December 2022



**Kisco Systems LLC
54 Danbury Road, #429
Ridgefield, CT 06877**

Phone: (518) 897-5002
E-mail: Sales@kisco.com
E-mail support: Support@kisco.com
WWW: <http://www.kisco.com/i2p>
Customer Support: <http://www.kisco.com/i2p/support>

© 2015-2022 Kisco Systems LLC

Table Of Contents

Introduction	<u>1</u>
Overview	<u>1</u>
What's New In Release 3.03?	<u>4</u>
What Was New In Release 3?	<u>4</u>
What Was New In Release 2?	<u>4</u>
IBM i Security Loophole	<u>5</u>
Installation and Security	<u>6</u>
Uninstall Procedure	<u>6</u>
Kisco Software Support	<u>6</u>
World Wide Web Support	<u>7</u>
The Master Menu	<u>8</u>
Work With Enrolled User Profiles	<u>10</u>
First Signon Process	<u>14</u>
Update Initial Program	<u>16</u>
Work With i2Pass Device Information	<u>17</u>
Alternate Signon Screen	<u>18</u>
Installing the Alternate Signon Screen	<u>19</u>
List Codes for User Profile	<u>20</u>
Display i2Pass Log Information	<u>20</u>
Purge i2Pass Log Information	<u>21</u>
IP Address Controls for Terminal Sessions	<u>21</u>
Custom Application Security	<u>24</u>
PASGENA API	<u>24</u>
PASCHKA API	<u>25</u>
Installation and Configuration	<u>26</u>
Installation from Media	<u>26</u>
Installation from Internet	<u>27</u>
Configuration Considerations	<u>28</u>
The Install Menu	<u>29</u>
Display installation status	<u>31</u>
Change installation status	<u>33</u>
Permanent installation	<u>34</u>
Print additional documentation	<u>34</u>
Enroll Active User Profiles	<u>34</u>
Process Kisco PTF Package	<u>35</u>
Update I2Pass Device Information	<u>35</u>
Update i2Pass Settings	<u>36</u>
Send Test Email Message	<u>40</u>
Work With Admins	<u>40</u>

Introduction

i2Pass provides extra security protection for IBM i (Power i, iSeries, AS/400) applications. It works with 5250 terminal session connections or with your own applications.

Your passwords may be compromised when using Telnet and other products over the Internet. “Hackers” and “snoopers” can pick up your user profiles and passwords and then use them to access your IBM i especially if your terminal session are not encrypted.

i2Pass gives you this protection by implementing a two factor authentication requirement for specific signon devices and users. This additional password, a randomly generated nine digit number, can only be used once. After it has been used, it can never be used again for a specific user profile, the additional password is permanently retired. This method allows you to access your system from a remote location for a legitimate purpose, but when someone tries to use that same authentication code over again, they are denied access. There is an option to require your user to enter their password a second time along with the second authentication number for full validation at final signon.

You can register your users along with their notification address. When a signon is in process, the second authentication code is automatically sent to the user and then requested to complete the signon process. When a code is sent, it must be used within a user defined window of time. After the time limit lapses, it will expire and cannot be used.

i2Pass can also be set up to trust known terminal device names. Then, if a user signs on from a trusted device, the 2FA process is bypassed. A trusted device name might be for local device that resides inside your network and is behind your firewall protection.

The two factor authentication can also be used from within your own applications. APIs (Application Program Interface) allow you to call our routines to generate the second authentication factor and send it to your user along with subsequent validation of the combination of user and secondary code.

i2Pass can be used to pre-generate a set of two factor authentication codes and produce them on a printed report. These can then be used to establish a remote connection. As each code is used, it is retired. Additional codes can be generated as needed and new listings of pre-generated codes can be made. If a user profile is defined to use a list of passwords, they cannot use the secondary code provided dynamically at signon time.

Overview

When first installed, the only user profile that will be able to administer i2Pass is QSECOFR. To authorize additional user profiles, sign on as QSECOFR (or any other (*SECOFR or *SECADM profile) and use option 11 on the INSTALL menu to authorize additional profiles.

When you first install i2Pass, no changes are made to your system. You must configure i2Pass to your specific requirements before it will start protecting your remote access sessions. This configuration process lets you identify the device profiles for “at risk” terminal devices and also lets you enroll those users where you want the user profile verified since they are connecting to your system via an exposed connection. No authentication codes are generated when a user is enrolled. Part of the configuration process includes verifying that the email transmission used by

i2Pass works on your system. ***This must be verified before you start implementation.***

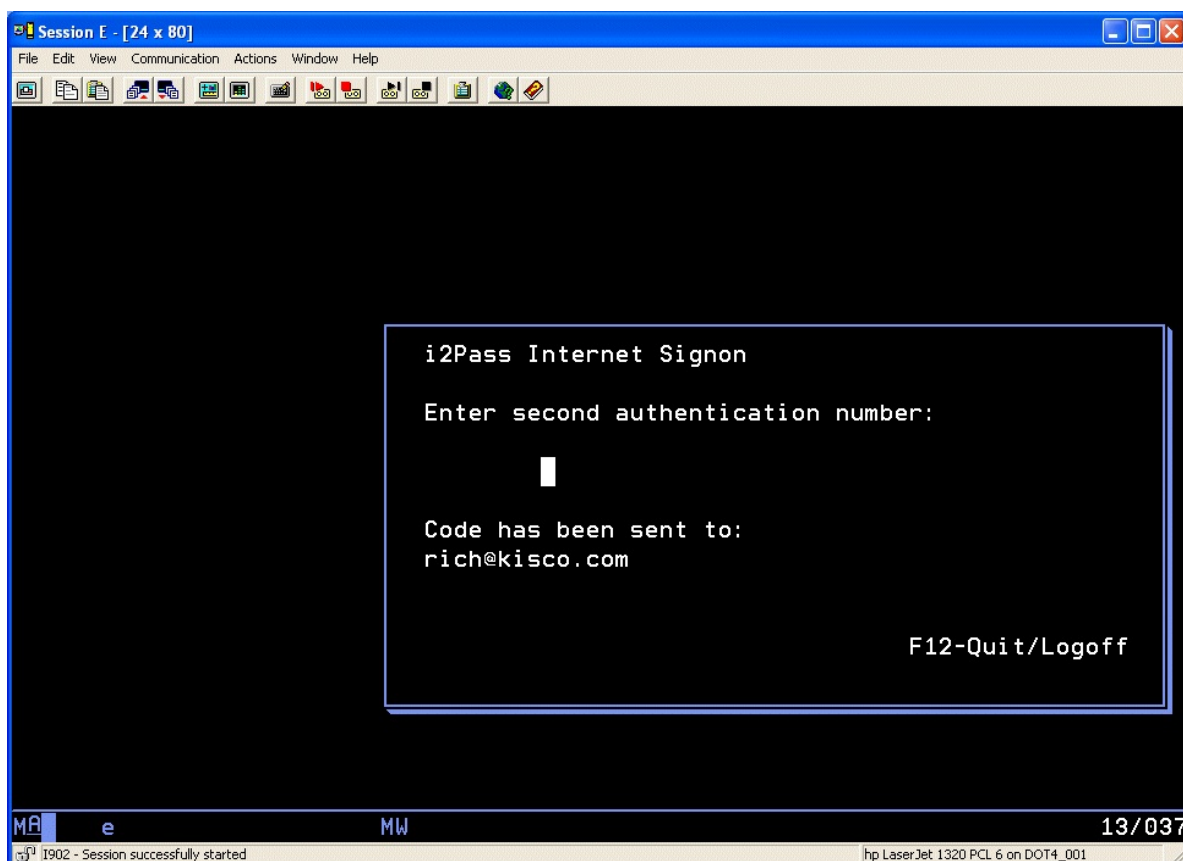
Note: All terminal devices with names that start with QPADEV* are considered to be at risk devices.

Before you start using i2Pass, we recommend that you test your email configuration to make sure that the email transport mechanism works correctly. Use option #10 on the INSTALL menu for this purpose. See the section in this manual for a description.

Once the configuration is done, you can start protecting your system using i2Pass. When a new user is registered without their email address, then the first time they sign on they will be prompted to enter their notification address (or addresses) where they want the 2FA codes sent. A validation process will follow to confirm that the notification address works. Once that is done, then they will be signed off and the next signon attempt will follow the normal 2FA signon process.

When a user profile is registered with a notification address, we recommend that you send a test notification to the user and verify that it has been received.

When a user that is registered and current in the software logs in from a device that has been identified as “foreign” (un trusted), the following screen will be displayed after their user profile and password have been entered and validated by the IBM i OS:



For users using the pre-issued codes from listings, as passwords are used up, users will have to generate new passwords. When someone accesses your system with an incorrect 2FA code or with a 2FA code that has already been used, the failure action specified on the I2PSET command (option 9 on the INSTALL menu) is taken and an alert notice is issued.

A log of all system activity, access acceptances and access rejections is also kept by i2Pass. You can periodically review this information on-line or produce reports for later review.

What's New In Release 3.03?

Release 3.03 of i2Pass adds integration with Kisco's new Kisco Connect software for easier and more reliable messaging via text (SMS) to your cell phones. When you have Kisco Connect installed and active on your system, you can send all text notifications and alerts using that method rather than the less reliable method of email-to-text that has been available up to this point.

Also new for Release 3.03, two new global variables have been added to the I2PSET options (menu option #9 on the INSTALL menu). One option will optionally let you log activity information to a message queue in addition to the normal logging in i2Pass. This message queue can then be used by you to integrate with other SIEM software on your system. Another global variable has been added to let you control how long a new 2FA code is valid for. Prior to this change, the timeout was hard coded to 15 minutes. Now you can specify a range from 1 to 60 minutes.

What Was New In Release 3?

Release 3 of i2Pass adds a self-activation feature as part of the user registration. When enrolling new users, the administrator no longer needs to know every email address. If a user is registered with the email address set to *NONE, then the first time they sign on after registration to i2Pass, they will be prompted for the email address (or addresses) that they want to use and complete a validation process.

Also new for Release 3, the specific email addresses are now split up into three different fields. This eliminates the previously confusing method of stacking multiple email addresses in a single field.

What Was New In Release 2?

Release 2 of i2Pass included an optional feature that lets you control who can establish a 5250 terminal session with your system based on their IP address. When first installed or immediately following an upgrade, this feature is not active. When activated, however, you can control which IP addresses are allowed 5250 terminal access to your system. This can be activated on a user-by-user basis. See the "[IP Address Controls for Terminal Sessions](#)" section of this user's guide for instructions.

Also new with Release 2, the source IP address of each 5250 terminal session is captured and reported in the Activity Log. This information can be displayed and/or listed using option #9 on the MASTER menu. Please note that only logon processes that occur following an upgrade to release 2 from an earlier release will include this information.

IBM i Security Loophole

i2Pass closes a security loophole in the IBM i OS that could be used to bypass entry of the second authorization code during an i2Pass signon process from a 5250 terminal session. As of release level 1.12 of i2Pass, this is no longer possible.

To make this work there are two settings changes that are made when i2Pass is installed.

First, the *MENU object named ASSIST in the QSYS system library has been changed so that user profile I2PASSUSR has *EXCLUDE authority for the object. If your IBM i OS is upgraded, this change will have to be done following the OS upgrade. The correct command to accomplish this is:

```
GRTOBJAUT OBJ(QSYS/ASSIST) OBJTYPE(*MENU) USER(I2PASSUSR)
AUT(*EXCLUDE)
```

Second, the I2PASSUSR user profile has to have the *ALLOBJ special authority REMOVED. We have also removed *SECADM as an additional security consideration. Installation of i2Pass as a new product will configure this user profile correctly and installation of the PTF IEPTF112 also resets the user profile. The correct set of special authorities for this user profile should be as follows:

```
*IOSYSCFG
*JOBCTL
*SAVSYS
*SPLCTL
```

Installation and Security

Specific installation instructions are covered in the section of this manual titled "Installation and Configuration". To install your product on trial, follow those instructions. i2Pass can be installed from distribution media supplied by Kisco Systems or from a download file from the Internet. The initial installation will allow i2Pass to run on your system for a period of at least thirty days. At the end of the trial period, the software will no longer function.

When you decide to keep i2Pass you must send your payment to Kisco Systems. At that time, Kisco must know the full serial number for your system and the partition number where the software is being used. If you are not sure of your serial number, go to the INSTALL menu in library I2PLIB and run option #2. Send Kisco a screen shot of the information displayed.

When Kisco receives your payment, serial number and partition information, they will issue a password to you. This password, when applied, will certify your copy of i2Pass and will permanently activate the software on your system. The password and certification instructions will be provided in writing by Email.

Uninstall Procedure

If you decide that you do not want to keep i2Pass after your free trial period, you can take the following steps to safely remove the software from your system:

1. Go to the MASTER menu in library I2PLIB and run option #1.
2. Delete any registered user profiles that show up here.
3. Exit the MASTER menu.
4. Delete the library named I2PLIB.

At this point, the software will be safely removed from your system.

Kisco Software Support

Kisco Systems provides unlimited software support during your first year of ownership. This includes the time during your free trial. Following the first year of ownership, there is a modest fee structure to maintain support for your software.

The Kisco support policy program works as follows:

1. First year support will be FREE! This includes unlimited telephone support, unlimited E-mail support, free release updates and free license transfers.
2. After the first year, an annual charge will apply for support and software maintenance.
3. Support covered by this annual fee includes:
 - a. Unlimited telephone support (518-897-5002)
 - b. Unlimited E-mail support (Support@kisco.com)
 - c. Defect analysis and correction

- d. Free updates to correct known defects
- e. Free license transfers
- f. Free use of our Customer Support Website information

At the end of your first year of ownership, you will receive a quote from us for your next year's maintenance charge. Please respond to this quote and a renewal invoice will be supplied.

World Wide Web Support

You can use the World Wide Web to reach us and to obtain software support information. Just set your web browser to our URL at:

<https://www.kisco.com>

Support information specifically for i2Pass can be found at URL:

<https://www.kisco.com/i2p>

At our Website, you will find:

- Product information about all Kisco software products for the IBM i market.
- Customer support information including:
 - ▶ Latest release level information for all products
 - ▶ Technical bulletins
 - ▶ Descriptions for recent enhancements to products
 - ▶ E-mail contact information for getting in touch with us
- Information about consulting services available from Kisco Systems.
- and more

We invite you to visit our Website, use the contact features to let us know what you think. We're always looking for ways to better serve you, our customer.

The Master Menu

The main menu used by i2Pass is called MASTER and is found in the library I2PLIB. There are several ways to display the menu. You can issue the following GO command from any terminal command line:

```
GO I2PLIB/MASTER
```

This method does not require that the library name be added to your library list. You can also add the library to your library list and display the menu with an easier format. To add the library to your library list, enter the following two commands:

```
ADDLIB I2PLIB
GO MASTER
```

The main i2Pass menu appears as follows:

```

C - 2:5250 Display
File Edit View Communication Actions Window Help
MASTER
QSECOFR
i2Pass Master Menu
1 Work With Enrolled User Profiles WRKPASUSER
2 Work With i2Pass Device Information WRKPASDEVS
3 List Codes for User Profile LSTPASWRDS
6 Display i2Pass Log Information DSPPASLOG
7 Purge i2Pass Log Information PRGPASLOG
10 Install Menu
(c) 2015-2022 Kisco Systems LLC
Selection or command
==>
  
```

Each menu option handles the following functions. Each function is described in more detail later in this manual:

- | | |
|----------------------------------------|-------------------------------------------------------------------------|
| 1. Work With Enrolled User Profiles | Displays a list of the enrolled users and allows you to work with them. |
| 2. Work With i2Pass Device Information | Displays a list of the known display devices on your |

system and their status registration with i2Pass.

3. List Codes for User Profile

Lets you generate a printed list of 2FA codes for a user that is set up as a List User.

6. Display i2Pass Log Information

Displays or lists the activity log and lets users view activity details.

7. Purge i2Pass Log Information

Lets you purge the log activity file.

10. Install Menu

Displays the Install control menu.

The following section of the manual will describe each menu option and its use.

Work With Enrolled User Profiles

Choosing menu option #1, or keying the command WRKPASUSER, will bring up the following display:

```

D - 5250 Display
File Edit View Communication Actions Window Help
i2Pass User File Maintenance PASSUS

Type options, press Enter.
  2=Change  4=Delete  5=Display  6=Send Test Note  7=Create codes
             8=IP Addr  9=List codes

User
Opt Profile  User Description  Notification Address
- *PUBLIC    *PUBLIC IP Address Ranges
- ADMIN      System Administrator  8005551212
- PATTYB     Pat                pattyb@mycompany.com
- RLOEBER    Rich Loeber        5185243462
- SYSOP      System Operator    sysop@mycompany.com

F3=Exit  F5=Refresh  F6=Create  F9=List Users

Bottom

Mâ D 03/006 10.2.2.3:23

```

Pressing the F9 function key from this display will generate a listing of the user profiles enrolled in i2Pass. The report will be sent to your session output queue.

From this display, you can enroll new users, display information about current users, generate new codes for existing users, test email addresses and generate code listings for list users.

Note: The entry above for the user profile ADMIN is a cell number for texting purposes. You can only specify cell numbers like this when Kisco Connect is also installed on your system.

To enroll a new user, use the F6 function key. When you do, the following display will show:

```

D - 5250 Display
File Edit View Communication Actions Window Help
ADD                                i2Pass User File Maintenance                                PASSUS

Type information, press Enter.
User Profile . . . _____ F4=Select
Init Program . . .
Init Pgm Lib . . .
User Description .
Notification 1 . . *NONE
Notification 2 . .
Notification 3 . .
Code Format . . . 0 0 - . /
Daily 5250 Check . *NO *NO/*YES
Failed signons . . 0
IP Address Active? *NO
List User? . . . . N Y / N

F12=Cancel
F3=Exit F7=Init Pgm F8=IP Adrrs F9=Fail Reset F4=Prompt

M A D 06/021
10.2.2.3:23

```

Enter the user profile in the first field. If you are not sure, use the F4 selection function to display a list of profiles on your system and you can select one from the list.

When you have entered the user profile, skip down to the Email Address field. If your user will be working from printed listings of two factor authentication codes, leave the email address set to the default value of *NONE and make sure that the List User? at the bottom is set to "Y". If the user will be receiving their authentication codes dynamically via email or text, then you can enter their notification address here or leave it set to *NONE. When you leave it set to *NONE, the first time the user logs on after being registered, they will be prompted for their notification address (or addresses) and taken through a validation process.

After a user has been registered, the list of user profiles enrolled in i2Pass will be displayed again. To send a test email message, you can use option 6 next to the user just registered and a test email will be sent. You should confirm with the user that the test is received to validate the email address if it was entered during registration.

After entering the email address, fill in the following setting as indicated:

Code Format	Controls how the 2FA code is presented to this user. The values that you can choose are:
-------------	------------------------------------------------------------------------------------------

During user registration, if the user profile has an initial program other than *NONE associated with it, that value in the user profile is updated and the current initial program information is stored in i2Pass. During a normal signon process, the initial program called by the IBM OS will be in i2Pass. When the logon has been validated by i2Pass, then their original initial program will be called.

Additional options that you can use from the list of user profiles enrolled are:

- 2 Change - will let you make changes to a user's email address
- 4 Delete - lets you remove a user profile that has been enrolled.
- 5 Display - displays the details of the enrollment for the user
- 6 Send a test notification message to the user's address
- 7 Create codes - if the user is a List User, this generates new codes for the user profile. These are authentication codes that can be listed and then used by the user since this user is not registered with an email contact address.
- 8 Maintain the list of IP Address ranges allowed for the user profile.
- 9 List codes - for List Users, a listing of the user's generated codes is created.

First Signon Process

When a user is enrolled with the email address set to *NONE and they are not specified as a List User, then the first time they sign on after they have been enrolled, they will see the following display on their terminal:

```

D - 5250 Display
File Edit View Communication Actions Window Help
RLOEBER i2Pass User Registration 12/07/22

Your user profile has been registered in the i2Pass two-factor logon control
system on this computer. To complete the registration, please provide one or
more contact addresses for 2FA codes to be issued during future logon attempts.

Contact Addr 1: _____
Contact Addr 2: _____
Contact Addr 3: _____

You may enter an email address or a text address. See the following web page
for information on how to specify a text address:

https://www.kisco.com/i2p/support/texting.htm

When all addresses have been entered, press ENTER. A single use verification
code will be sent. Type them back in on the next screen panel.

Kisco Connect is installed here

F12=Cancel/Logoff

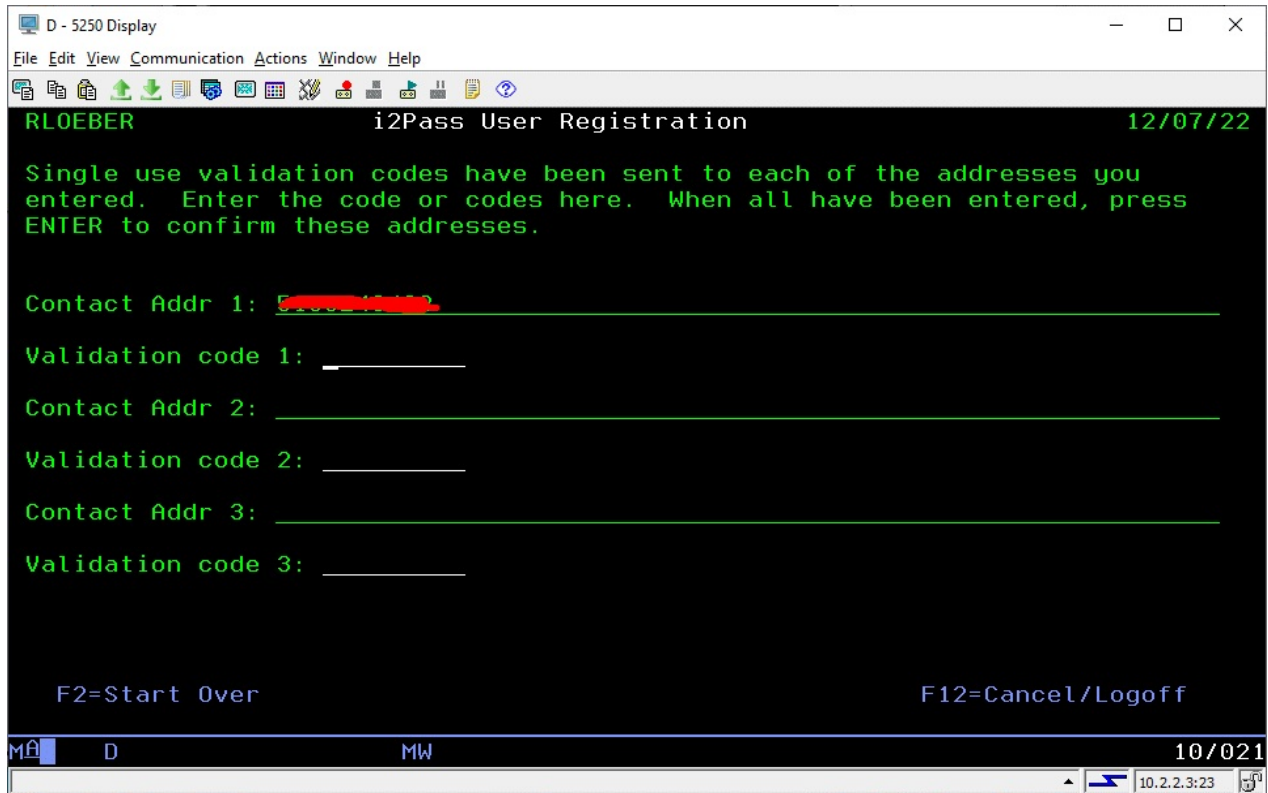
M&A D MW 08/018
10.2.2.3:23

```

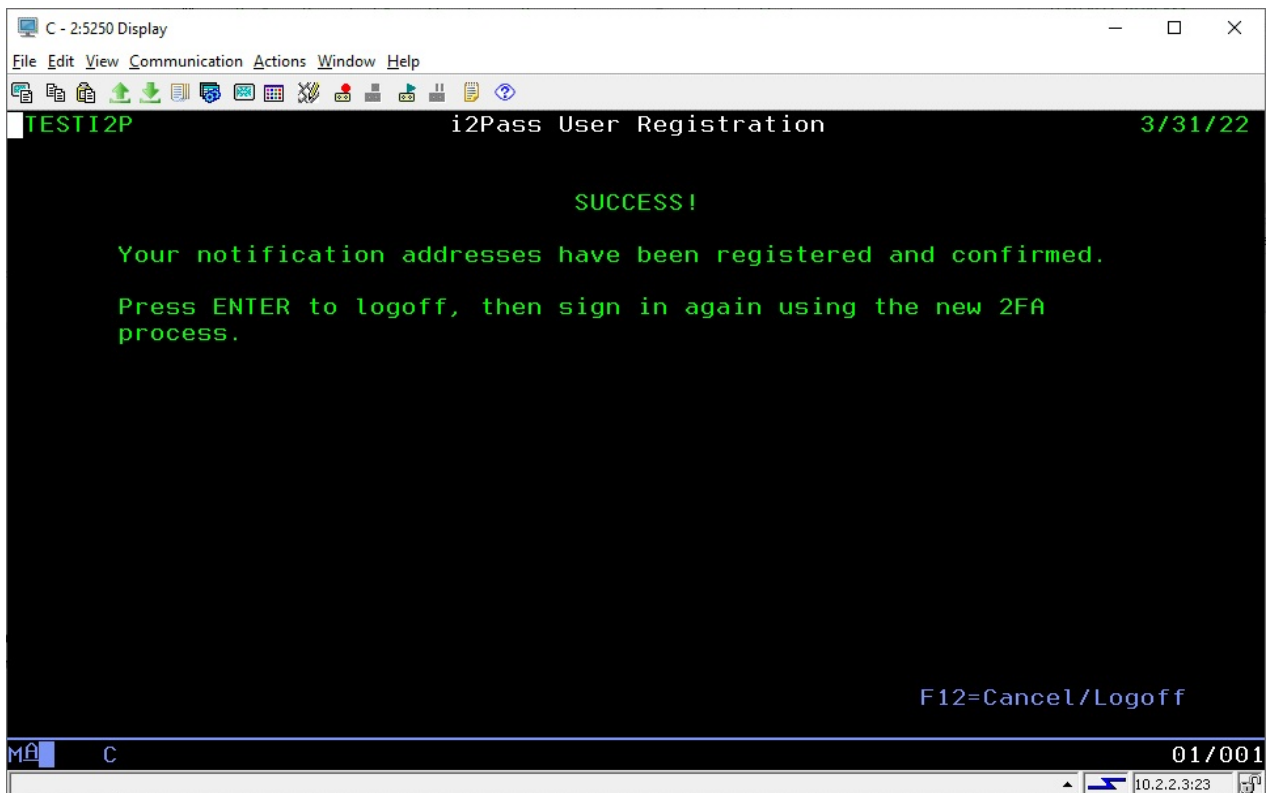
To complete their registration, the user will need to enter a valid email address in the Contact Address 1 field. If they want to receive notifications at additional addresses, those can be entered in the additional fields. When they are done entering all addresses that they want to use, press the ENTER key.

When the ENTER key is pressed, i2Pass will generate a unique 9 digit number code for each address entered and send a notification to each address.

The user should wait until all responses have been received, then enter the codes underneath each address:



When all of the codes have been entered, they will be validated and a confirmation display will appear:



When the user presses the ENTER key, they will be signed off. To gain access to the system, they should now do a normal signon and the 2FA process will operate normally.

Update Initial Program

When a user profile is registered to i2Pass, the current Initial Program (and Library) is transferred from the user profile in the IBM i OS to a database file in i2Pass. You can change the Initial Program and Library for a user after it has been registered in i2Pass.

When you have a user profile registered, run option 1 on the MASTER menu and place a 2 (Change) next to it. The next screen will show you how that user is registered, including the Initial Program and Library. To make a change to the Initial Program and Library, press the F7 function key. This will make these fields available for update.

Note, to remove an Initial Program and Library setting, change the Initial Program to *NONE and blank out the Library field.

The next time the user in question accesses your system through i2Pass, the new Initial Program setting will take effect.

Work With i2Pass Device Information

i2Pass can be configured to recognize specific terminal devices as “foreign”. Foreign devices must use a second authentication factor in order to complete a signon process for an enrolled user profile. That code can either be provided dynamically via email at the time of the signon or can be selected from a listing of pre-generated authentication codes.

i2Pass considers all device names that start with QPADEVxxxx as foreign device names.

i2Pass includes an option on the INSTALL menu for registering all terminal device names automatically. Please see the documentation for the INSTALL menu for details on how to run this option.

To maintain the list of terminal devices, run option #2 on the MASTER menu. The following will be displayed:

The screenshot shows a terminal window titled "Session E - [24 x 80]" with a menu bar (File, Edit, View, Communication, Actions, Window, Help) and a toolbar. The main content area is titled "i2Pass Device File Maintenance" and "PASSDE". It displays a list of devices with their descriptions and types. The list is as follows:

Opt Code	Device Description	Device Type
—	ALLIANCE1 Alliance connection	
—	ALLIANCE2 Alliance connection	
—	ALLIANCE3 Alliance connection	
—	ALLIANCE4 Alliance connection	
—	ALLIANCE5 Alliance connection	
—	ALLIANCE6 Alliance connection	
—	ALLIANCE7 Alliance connection	
—	BLOCK111	F Foreign
—	BLOCK123	F Foreign
—	BLOCK999	F Foreign
—	CGIDEV2 Testing	F Foreign
—	DSP01	
—	GARNET	

At the bottom of the list, it says "More...". Below the list, there are function key shortcuts: F3=Exit, F5=Refresh, and F6=Create. The terminal window also shows a status bar at the bottom with "MA e" on the left, "03/006" on the right, and "hp LaserJet 1320 PCL 6 on DOT4_001" at the bottom right.

From this list, you can flag any device as a foreign terminal device. Place a 2 next to the device description and change the device type to F. When a user profile that has been enrolled in i2Pass attempts to sign on from a foreign device, a second authentication code will be required after the user id’s regular password has been authenticated by the IBM OS.

Note: Kisco recommends that you NOT implement i2Pass on the device that is used as your

system console.

From this list, you can also remove devices using option 4 or create new device entries using the F6 option.

Alternate Signon Screen

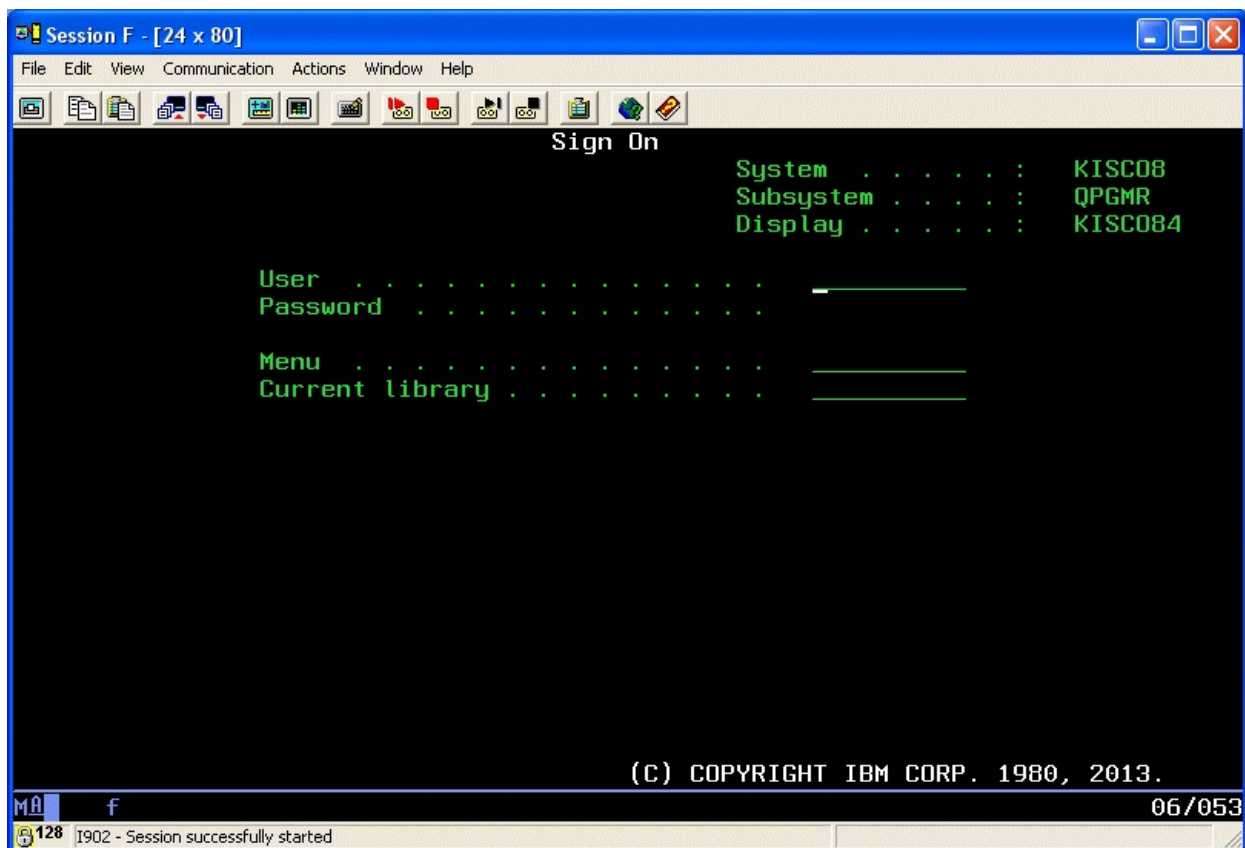
A savvy user on your system could be enrolled in i2Pass and then, by a trick done during the logon process, bypass the i2Pass requirement for a 2FA code validation.

If you are familiar with the IBM i 5250 signon screen, it typically includes the following lines for most IBM i systems:

```
User . . . . . _____
Password . . . . . _____
Program/procedure . . . . . _____
Menu . . . . . _____
Current library . . . . . _____
```

An educated user could sign on using their normal user profile and password and then, in the "Program/procedure" field, type in the value 'QCMD' with the result that i2Pass processing is bypassed and the user gains direct access to your system with a command line being displayed.

To correct for this, it is a simple matter to replace the standard signon screen with a custom screen that removes the "Program/procedure" field from being available for use. When this change is made, the familiar signon screen will look like this:



If your system already has a customized signon screen, stop reading now and contact your system administrator to arrange for the "Program/procedure" field to be removed.

If, however, you are still using the standard signon screen that came with your system, we have now provided an alternate to it packaged with i2Pass. The signon screen is named QDSIGNON (if you are using long passwords, the screen is named QDSIGNON2) and is located in the system QSYS library. We have these two *FILE objects now included in the I2PLIB application library for i2Pass. The source code for both of these screens is also now included in a source file named QDDSSRC, also in the I2PLIB library. The screens have been tested for IBM i OS level 6.1, 7.2 and 7.3 and we anticipate that they will also work with other active IBM i OS release levels.

Installing the Alternate Signon Screen

***** WARNING *** WARNING *** WARNING *** WARNING *** WARNING *****

Changing the signon screen specification can result in your users, including you, not being able to log on to your system effectively locking you out of your system. Implementation of this should be fully tested at a time when there are no active users on your system.

You should not make this change if you are still just evaluating i2Pass. If you later decide not to purchase i2Pass and remove our library from your system, you could create a situation where your users are locked out of the system.

The signon screen specification is stored in the subsystem description for any interactive subsystem on your system. For most systems, this is the QINTER subsystem. Some systems may also use the QPGMR subsystem for interactive work.

DO NOT IMPLEMENT THE ALTERNATE SIGNON SCREEN FOR THE QCTL SUBSYSTEM, this will guarantee that your system console will always be available.

To implement the alternate signon screen, do the following steps which will include the recommended testing process. This example will use the QINTER subsystem, but it can be followed for any interactive subsystem that you need to change.

1. Sign on to your system console as QSECOFR. Verify that this terminal session is running in the QCTL subsystem.
2. Check and make sure that no users are signed on using the interactive subsystem that you want to change.
3. End the subsystem to be changed.
4. Run the following command:

```
CHGSBSD SBSD(QINTER) SGNDSPF(I2PLIB/QDSIGNON)
```

If your system is configured for long passwords (system value QPWDLVL value of 2 or 3), then use the following command instead:

```
CHGSBSD SBSD(QINTER) SGNDSPF(I2PLIB/QDSIGNON2)
```

5. Start the subsystem back up using the STRSBS command.
6. Start a terminal session. Confirm by observation that the new logon screen is active. Then, perform a log on and make sure that you get to the logon destination that you would normally see.
7. If step #6 completes normally, then you can resume normal processing.
8. If step #6 reveals any problem, the recovery is as follows:
 - a. From the system console, end the subsystem again.
 - b. Run the following command to restore the system signon screen that was previously in use:


```
CHGSBSD SBSD(QINTER) SGNDSPF(QSYS/QDSIGNON)
```
 - c. Restart the subsystem and check to make sure that the signon process is now working correctly again.

If you have any questions about this process, feel free to contact us at Kisco Systems with your questions or concerns.

List Codes for User Profile

Option #3 on the MASTER menu will let you generate a listing of pre-generated codes for a user profile. This will prompt the LSTPASWRDS command and will ask for the user profile to be listed. An option on the prompt will let you also list passwords that have already been used for the profile. This option is only available for users that are registered as List Users.

Display i2Pass Log Information

i2Pass logs all activity to a log file. You can display or print this information by selecting option #6 from the menu or by using the DSPPASLOG command. You are initially prompted for which entries you want displayed. The options are:

- | | |
|----------|-----------------------------------------------------------------------------------|
| *TODAY | The initial display will show entries from the current date. This is the default. |
| *PRVDAY | The initial display will show entries from the previous day. |
| YYYYMMDD | Entries from the specific date will be shown. |

Details will be shown for events.

From this display, there are two function keys that you can use to create a listing of the log information. F6 will create a listing of the information in sequence by date and time. The F8 key will create the listing in sequence by user, date and time.

Purge i2Pass Log Information

As you use i2Pass, the log file will begin to get quite large. A purge function is provided to let you remove records from the log file. To purge the log file, choose menu option #10 or use the PRGPASLOG command. When you start the purge, it will ask you for a specific purge date in the format YYYYMMDD or a second parameter can be used to indicate the number of days to keep activity on file. One or the other parameter must be used.

Note: Once records are removed from the log file, they are no longer available for display or reporting purposes. Be sure to run any reports you may want to keep before you run a purge of the log file.

IP Address Controls for Terminal Sessions

i2Pass includes an optional feature that will let you establish access controls for 5250 terminal sessions by the IP address that the session is coming from. This feature can be activated for individual user profiles to specify a range of IP addresses that the user is allowed to connect to your system from. There is also a feature that lets you establish a range of IP addresses that can apply to all users who have IP address checking activated.

When first installed, this feature is turned off on a global basis. You should consider running your system for a little while with the featured turned off so that you can collect the IP addresses currently being used. This information will appear in the i2Pass Log (option #6 on the MASTER menu) once users have been enrolled and start using i2Pass.

To turn the feature on and start using it, you will have to update the setting that activates the feature using option #9 on the INSTALL menu. Check the parameter setting that shows as follows:

```
IP Addr Checking Active? . . . . > *NO
```

Change this value to *YES. Once this change has been made, then any user that is registered to i2Pass with the IP Address checking feature active will be subject to this test before a terminal session can be established. Note that this test is done before any 2FA activity takes place.

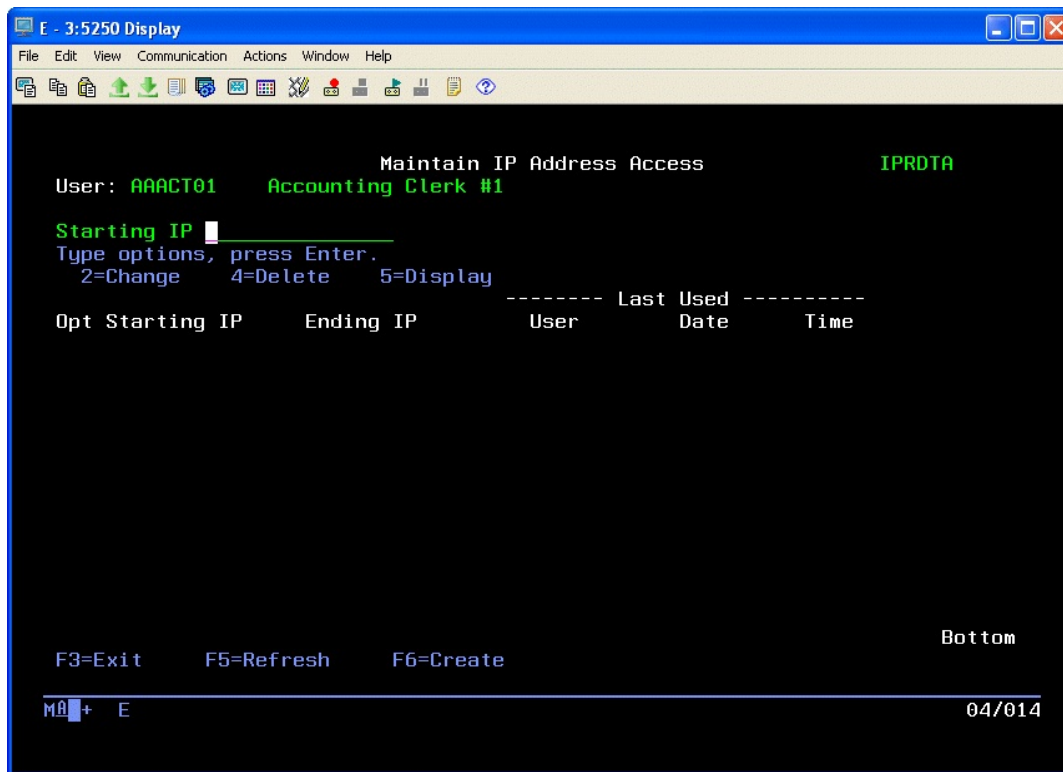
To restrict a user to a specific IP address or a range of IP addresses, start menu option #1 on the MASTER menu. Locate the user in question and place a 2 next to their registration listing to update the settings for the user profile. When the detail screen is displayed, find the setting marked as follows:

```
IP Address Active? *NO
```

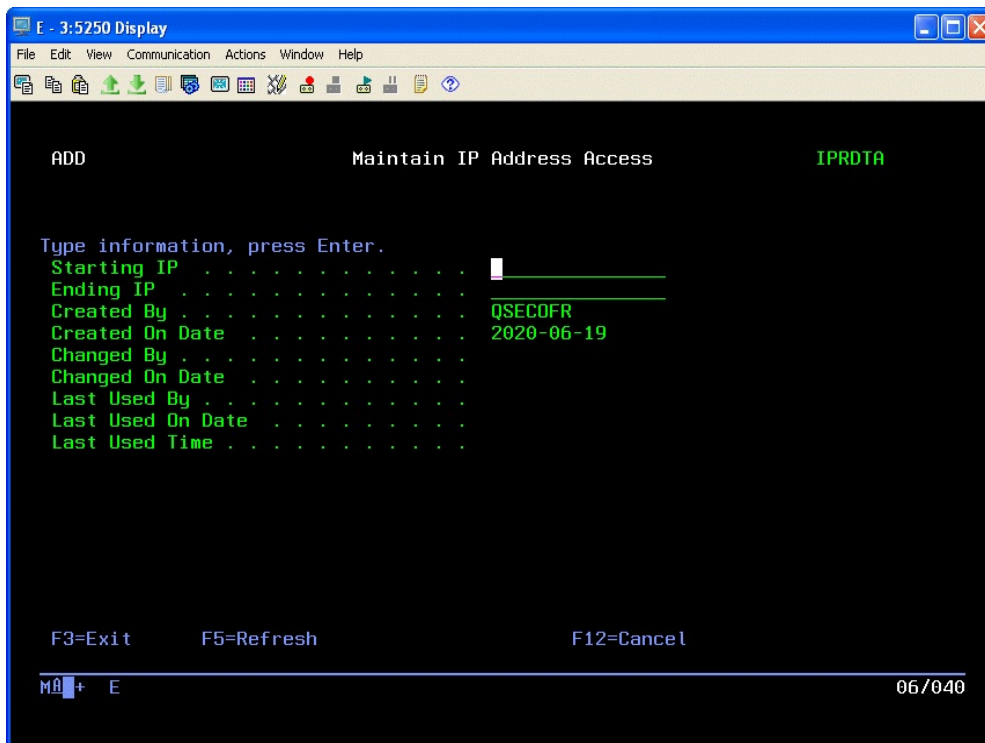
Change the setting to *YES.

After this change has been recorded, you will need to define an IP address or range of IP addresses that the user can use to access your system.

Locate the user in the list of registered users and place an 8 next to their user profile. The following display will appear:



To add an IP address range, press the F6 key and the following screen will be displayed:



Enter a range of IP addresses in the form of nnn.nnn.nnn.nnn. For example, you could define a range of 10.1.1.1 to 10.1.1.25. If you want to define a single specific IP address, put the same IP address for both the starting and ending IP address. Press ENTER to record the IP address range. If you will need additional IP address ranges, you can enter them now.

The “Last Used By” and “Last Used On Date/Time” refer to the last time that this IP Address range record was used to allow a user sign-on process.

In your list of registered users, you will see an entry for a profile named *PUBLIC. This is not an actual user profile and the entry cannot be updated, but you can place an 8 next to it to authorize IP addresses. When you do, these IP address ranges will be used for all users who have the IP address checking feature activated. Using this method, you can specify one range of IP addresses for all users and then only specify unique addresses for individual user profiles.

Custom Application Security

i2Pass lets you use two factor authentication functions from within your own application programs. This will allow you to implement single-use, self-expiring authentication controls in your own applications.

This feature is implemented through the use two APIs included with i2Pass.

PASGENA Generates a single two factor authentication code and sends a notification to the registered user and sets a return code

PASCHKA Validates the user profile and two factor authentication code provided and sets a return code with results

You can call these two APIs from within your own programs. Details on each API follow.

PASGENA API

The PASGENA API can be used to issue a single use two factor authentication code and return the code to the calling program. The API has three parameters as follows

Parameter	Type	Length	Description
User Profile	Input	10	This is the user profile for which you want to generate the authentication code. The user must be registered to i2Pass with a valid email address provided.
Code	Output	9	This is the nine digit two factor authentication code generated from the call to the API
Return Code	Output	2	This is a two digit code that reports the results of the call to the API. Values returned are as follows: 00 - Code generated and sent 01 - User not enrolled in i2Pass 02 - No notification address on file for user 03 - User profile not valid on this system

When the return code is 00, a valid code has been generated and sent as email. The code will expire based on the global setting in I2PSET. The PASGENA API is stored in the I2PLIB library.

PASCHKA API

The PASCHKA API can be used to validate a two factor authentication code for a specific user profile. It will issue a return code with the results of the authentication. There are four parameters used with this API as follows:

Parameter	Type	Length	Description
User Profile	Input	10	Provide the user profile for which the authentication code will be validated.
Code	Input	9	Provide the two factor authentication code you want to validate for the given user profile.
Call Type	Input	1	Must be coded with the value 'A' - indicates an API use of the validation process.
Return Code	Output	2	This is a two digit code that reports the results of the call to the API. Values returned are as follows: 00 - Code is OK and its use has been logged 01 - User/code not found 02 - User/code already used 03 - Code is expired

If the code returned is 00, then the combination of the user profile and the code provided were valid. The API will retired the code so that it cannot be used again and the validation process will be logged in the activity log.

Installation and Configuration

Before any i2Pass functions will work, the initial install procedure must be run. i2Pass can be installed from media received with a shipment from Kisco Systems or from a download file obtained from the Internet. If you received a direct shipment from Kisco, use the *Installation from Media* instructions. If you downloaded a file from the Internet, use the *Installation from Internet* instructions. Both follow.

Installation from Download

To install from download, a URL at the Kisco website will be provided with detailed instructions. This will be available from the following website for i2Pass:

<https://www.kisco.com/i2p/i2pdload.html>

Follow the instructions from the Download page. We recommend that you print these instructions and use them as a check list for best results. The software download from the website is a standard ISO CD image file.

Configuration Considerations

Once the software has been installed, additional configuration considerations should be taken into account as follows:

1. The current display devices for your system must be identified to i2Pass so that correct context can be determined. Additional information for this is in the user's guide, including a tool for initializing device information on the INSTALL menu in the following section.
2. User profiles will also have to be enrolled in i2Pass. Only those user profiles that will actually use Telnet signon should be enrolled. If all of your users will be using Telnet, there is another tool on the INSTALL menu to enroll all users at once. Users who may need to be validated from the APIs provided must also be enrolled.
3. i2Pass issues security alert notification messages to up to 5 user profiles. The default user profile QSECOFR is initially assumed by the software. An option on the INSTALL menu will let you add more user profiles to the list. You can also register email addresses for notifications.
4. Base i2Pass relies on email for notification of codes generated and for activity violation attempts. **Before you use the software**, you should go to the INSTALL menu and run option #10 to send a test email to a valid email address. If the email gets delivered, great, you can proceed with your implementation. If the email does not get delivered, you will have to see why it is failing. This can frequently be determined by checking the joblog from the session where the test message has been sent (DSPJOBLOG).

If you have trouble with this, first check the suggestions at the following address at our website:

<https://www.kisco.com/i2p/emailconfig.html>

If you still need help with this, contact Kisco support staff.

5. If you want to use native SMS (Short Message Service, also known as texting), you can install Kisco Connect from Kisco Systems. i2Pass will integrate seamlessly with Kisco Connect and you can use cell phone numbers in place of email addresses.

The Install Menu

When you select item 10 from the main menu, the installation menu is displayed as follows:

```

D - 5250 Display
File Edit View Communication Actions Window Help
INSTALL                               INSTALL Menu

Select one of the following:

  1. Run initial install procedure
  2. Display installation status
  3. Change installation status
  4. Print documentation
  5. Display i2Pass Version Information
  6. Enroll Active Users in i2Pass           ENRALLUSRS
  7. Process Kisco PTF Package
  8. Update i2Pass Device Information from System   GENPASDEVS
  9. Update i2Pass Settings                   I2PSET
 10. Send Test Message
 11. Work With Admins                       WRKI2PUSR

 20. To Main Menu

                                (c) 2015-2022 Kisco Systems LLC

===> _
  
```

Menu items perform the following functions. Each function is discussed in greater detail later in this document:

- | | |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Run initial install procedure - | Do not use this option unless directed to do so by Kisco Support staff. This option is automatically run during normal install processing. |
| 2. Display installation status - | Displays a screen showing the current installation status for the software. |
| 3. Change installation status - | Displays the current software installation status and allows for changes to be made. |
| 4. Print documentation - | Prints this documentation manual to the default print device. |
| 5. Display i2Pass Version Information | Displays the current version and PTF information about your installed version of i2Pass. |

6. Enroll Active Users in i2Pass Lets you enroll an individual user profile, a set of GENERIC* user profiles or all user profiles on your system.
7. Process Kisco PTF package - Allows you to process a corrective PTF package received from Kisco for program fixes.
8. Update I2Pass Device Information from System Automatically analyzes the device information for your system and creates the initial file for all known display devices.
9. Update i2Pass Settings Sets and updates values used by i2Pass.
10. Send Test Message Sends a test message to any notification address. For email addresses, this must be done immediately following installation to make sure that your email transmission process works correctly with your current system configuration.
11. Work With Admins Lets you define the user profiles that can administer the i2Pass software product.
20. To Main Menu - Will display the i2Pass main menu.

Display installation status

At any time, you can check the current installation status of your copy of i2Pass by selecting this menu option. You must be signed on with security authority of QSECOFR or equivalent. The following screen will be displayed:

```

C - 2:5250 Display
File Edit View Communication Actions Window Help
Software Security

Installation for      I2PLIB      Developer ID code  KISCO
Machine serial number 785D4C0    Current Library    I2PLIB
                    Sec.serial number 785D4C0
                    Sec.install date. 220310
Machine run date.... 220330      Sec.expire date.. 999999
                    Sec user count... 9999 002

Security Status PERMANENTLY INSTALLED...Z-003

Please enter:                PTF: IPPTF203

Type of install .....
Install password .....
New expire date.....
User count.....

T for trial, or P for permanent
Blank for trial, or permanent password
Blank for trial, or 999999 for permanent
0025 for trial or authorized count for
permanent installation

Cm3,7-Return to menu      HELP      ENTER-process installation

M C 16/031
10.2.2.3:23

```

The message at the center of the screen indicates your current installation status. You should also check the Sec.expire date for an expired trial period. i2Pass may still show as installed on a trial basis but, if the trial is expired, it will no longer function.

The following are the possible status messages that can appear on this display:

<u>Message</u>	<u>Explanation</u>
Z-001 NOT INSTALLED	Trial installation not started
Z-002 TRIAL EXPIRED	Trial period has ended
Z-003 PERMANENTLY INSTALLED	Software is permanently installed
Z-004 INSTALLED ON TRIAL	Software is installed on trial
Z-005 PASSWORD NOT ACCEPTED	Password keyed is not valid
Z-006 WRONG LIBRARY	Programs must run from our library
Z-007 PLEASE RUN TRIAL INSTALL	Must have trial install before perm.
Z-008 INVALID INSTALL REQUEST	Must be P or T

Z-009 INVALID SECURITY (REC#6)	Call Kisco
Z-010 INVALID SECURITY (NO ZZ)	Call Kisco
Z-011 INVALID SECURITY (HASH.)	Call Kisco

Change installation status

To make changes to your installation status, use this menu option. The changes processed can include both a trial period extension and permanent installation. You must be signed on with QSECOFR security authority or equivalent. When you select this option, the following screen is displayed:

```

C - 2:5250 Display
File Edit View Communication Actions Window Help
Software Security

Installation for      I2PLIB      Developer ID code  KISCO
Machine serial number 785D4C0    Current Library    I2PLIB
Sec.serial number     785D4C0
Sec.install date     220310
Machine run date.... 220330      Sec.expire date..  999999
Sec user count...    9999 002

Security Status PERMANENTLY INSTALLED...Z-003

Please enter:                PTF: IPPTF203

Type of install .....  [ ]  T for trial, or P for permanent
Install password .....  [ ]  Blank for trial, or permanent password
New expire date.....  [ ]  Blank for trial, or 999999 for permanent
User count.....  [ ]  0025 for trial or authorized count for
                           permanent installation

Cm3,7-Return to menu      HELP      ENTER-process installation

MÁ C 16/031
10.2.2.3:23

```

Trial extension

To extend a trial period, contact Kisco Systems and request an extension. We will provide you with an extension password and new expiration date. On the above screen, enter the following:

Type of install	Enter 'T' for trial
Install password	Enter all six digits of the extension password provided, including any leading zeros
New expire date	Enter the new expiration date in the format YYMMDD (ie: Jan 12, 1998 would be 980112)
User count	Enter the user count that your copy of i2Pass will be authorized for.

When the parameter fields have been completed, press enter to reactivate your software.

Permanent installation

To permanently install your software package, use the permanent password provided by Kisco Systems following receipt of payment. On the above screen, enter the following:

Type of install	Enter 'P' for permanent
Install password	Enter all six digits of the extension password provided, including any leading zeros
New expire date	Enter all 9's (ie: 999999)
User count	Enter the user count that your copy of i2Pass will be authorized for.

When the parameter fields have been completed, press enter. Your software is now permanently installed.

Print additional documentation

At any time, you can reproduce the additional documentation by using this menu option. A full copy of the additional documentation topics will be printed.

Enroll Active User Profiles

You can use this option to enroll all user profiles in i2Pass. This is only recommended for those shops where all or most users will be using the Telnet connection.

Note: This option will enroll the user profiles, but will not record an email address for each user. The first time a user signs on after they have been registered without an email address, they will be prompted for an email address (or addresses) and taken through a validation process.

Process Kisco PTF Package

i2Pass supports distribution of program updates remotely via the Internet. When programs in i2Pass are updated or program fixes are required, Kisco Systems can send the updates directly to you via the Internet. If needed, we will send E-mail to you with an attached PC file. This file, when loaded into a folder on your system, can be used to post program updates and changes to your copy of i2Pass.

To install a PTF received by email, go to the following link at our website:

<https://www.kisco.com/i2p/support/i2pptfupd.html>

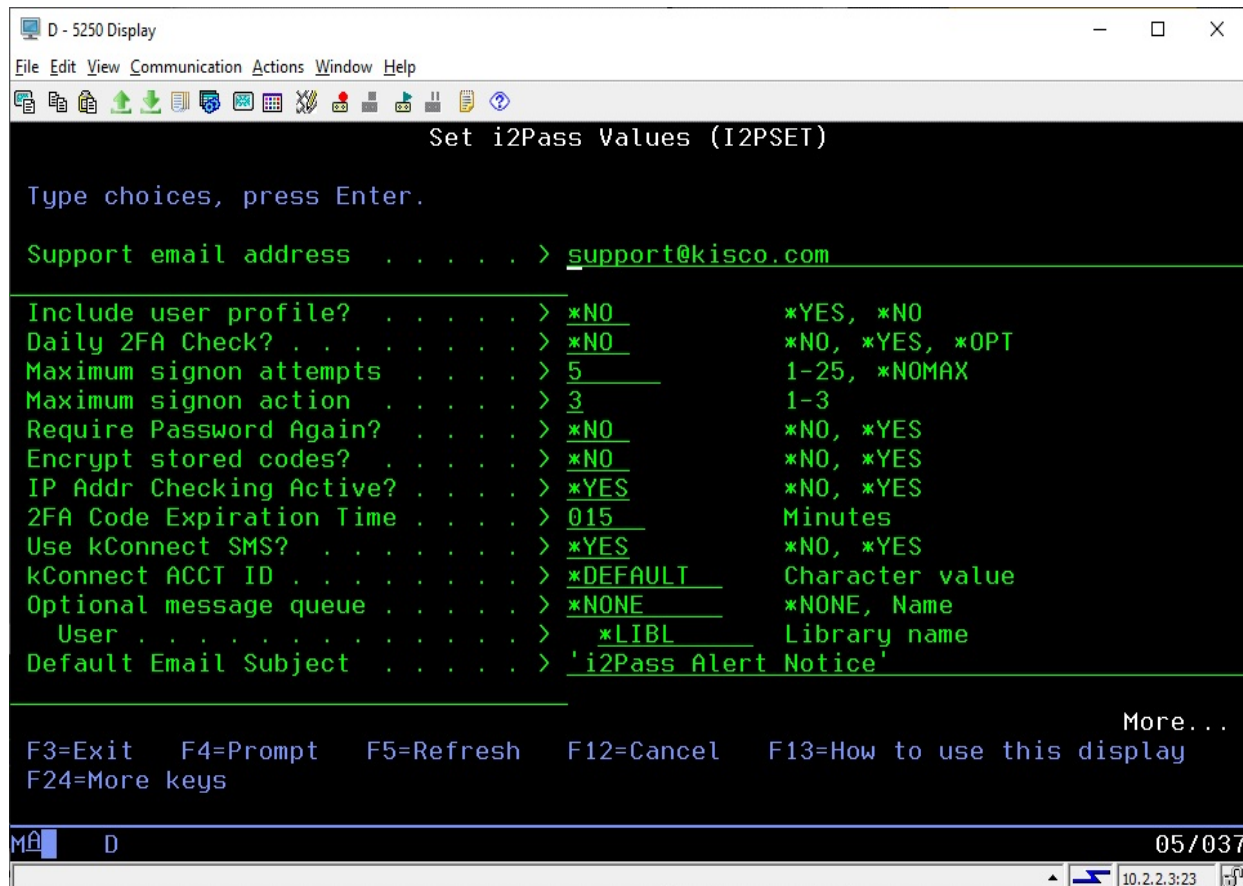
Update I2Pass Device Information

i2Pass determines signon context based on a list of terminal devices maintained within i2Pass. After initially loading the software, you can run this option from the INSTALL menu to populate the list with all known terminal devices. Once the list has been initialized, you can use the menu options to review and maintain the list.

You can also run this option at any time after the initial use. Any new terminal devices will be added to the table while existing device records will be left as they currently appear.

Update i2Pass Settings

Option #9 on the INSTALL menu lets you maintain certain global settings for i2Pass. When you start this option, the following will be shown:



```

D - 5250 Display
File Edit View Communication Actions Window Help
Set i2Pass Values (I2PSET)

Type choices, press Enter.

Support email address . . . . . > support@kisco.com
-----
Include user profile? . . . . . > *NO          *YES, *NO
Daily 2FA Check? . . . . . > *NO          *NO, *YES, *OPT
Maximum signon attempts . . . . . > 5           1-25, *NOMAX
Maximum signon action . . . . . > 3           1-3
Require Password Again? . . . . . > *NO          *NO, *YES
Encrypt stored codes? . . . . . > *NO          *NO, *YES
IP Addr Checking Active? . . . . . > *YES         *NO, *YES
2FA Code Expiration Time . . . . . > 015         Minutes
Use kConnect SMS? . . . . . > *YES         *NO, *YES
kConnect ACCT ID . . . . . > *DEFAULT     Character value
Optional message queue . . . . . > *NONE        *NONE, Name
User . . . . . > *LIBL        Library name
Default Email Subject . . . . . > 'i2Pass Alert Notice'
-----
More . . .
F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys

Mâ D 05/037
10.2.2.3:23
  
```

Enter the values as follows:

Support email address

Enter a valid email address. This will be used by i2Pass as the sender's email for all notification email messages.

Include user profile?

Lets you specify that the notification email message that contains the second authentication factor exclude the user profile in the message text. Some customers may prefer to not include both the user profile and the authentication factor in the same message.

Choose one of these options:

*YES The user profile will be included with the authentication code email message.

*NO The authentication code will be sent without the user profile in the message.

Daily 2FA Check?

This is a global specification on how you want to control repeated 5250 signon processes for a user profile using the same terminal address.

Choose one of these options:

- *NO Each time a user signs on with a 5250 terminal, a 2FA code will be sent.
- *YES The first time a user signs on with a 5250 terminal each day, a 2FA code will be sent. Subsequent signons from the same terminal session will not require a 2FA code.
- *OPT Checking for once a day signon privileges will be determined at the user registration level.

Maximum signon attempts

This is the number of signon attempts that will be allowed before an action is taken on the system to stop logon processing.

Choose one of these options:

- *NOMAX Indicates that an unlimited number of attempts will be allowed and no action will be taken by the system.
- 1-25 Indicates that the number of attempts will be allowed before an action is taken. This defaults to 3 when initially installed.

Maximum signon action

The action you want to take when the sign on attempt limit has been exceeded.

Choose one of these options:

- 1 The device will be disabled.
- 2 The user profile will be disabled.
- 3 Both the device and the user profile will be disabled.

Note: This function (the previous 2 settings) mirrors the IBM i OS special values of QMAXSIGN and QMAXSGNACN. Kisco recommends that you seriously consider implementing this new control. Someone attempting to gain access to your system with a known user profile and password, could potentially gain access via a brute force Telnet attack. Implementing this feature can serve to stop this kind of attack before any serious damage.

Require Password Again?	<p>Indicates whether you want a user to re-enter their password when the 2FA code is verified. This will cause the user to enter their password twice during 5250 signon processing, but may be a requirement for certain security settings that require that the password and the 2FA code be validated concurrently.</p> <p>Choose one of these options:</p> <p>*NO Re-entering of the user's password will not be requested. (Default)</p> <p>*YES When the user signs on with a 5250 terminal, in addition to the 2FA code they will also be required to re-enter their password a second time along with the 2FA code.</p>
Encrypt stored codes?	<p>Controls whether the 2FA codes stored by i2Pass are encrypted or stored in plain text.</p> <p>Choose one of these options:</p> <p>*NO The 2FA codes are stored in plain text. (Default)</p> <p>*YES The 2FA codes are encrypted.</p>
IP Addr Checking Active?	<p>Controls whether the IP address checking controls are active or inactive. Deactivating the IP address checking will turn this feature off for all user profiles registered with i2Pass, regardless of how each individual user is configured.</p> <p>Choose one of these options:</p> <p>*NO - IP Address checking is not active.</p> <p>*YES - IP Address checking is active for users where the feature is active.</p>
2FA Code Expiration Time	<p>Controls the number of minutes that an i2Pass 2FA code will be allowed to be used. Initially defaults to 15 minutes. This can be set to any value in a range of 1 to 60 minutes.</p>
Use kConnect SMS?	<p>If you have Kisco Connect installed on your system, set this value to *YES to allow you to use cell phone numbers for notifications and alerts. If Kisco Connect is not installed, this must be set to *NO.</p>

kConnect ACCT ID	If you have Kisco Connect installed on your system, this setting specifies the Twilio account definition that you want to use.
Optional message queue	Lets you optionally direct that the log entries also be posted to a message queue. When set to *NONE, the option is turned off. If you specify a valid message queue, then log entries will also be posted to the message queue.
Default Email Subject	This value will be used as the Email Subject when alerts and notification messages are sent. If you are using i2Pass in a multiple partition or multiple server installation, you can use this to differentiate the notification messages so that you know which platform is issuing the message.

Additional settings can be accessed when you roll up to show the following values:

Notify users	Enter up to 5 user profiles where you want notification messages sent when i2Pass issues a code rejection.
Email notifications	Enter up for 5 email addresses where you want notification messages send when i2Pass issues a code rejection. If no email addresses are going to be used, enter the special value *NONE in the first field.
SMS notifications	Enter up for 5 SMS addresses where you want notification messages sent when i2Pass issues a code rejection. If no SMS addresses are going to be used, enter the special value *NONE in the first field.

Send Test Message

This option will prompt you for a notification address. When you complete the address and press ENTER, a test message will be sent to the address provided. If it fails to go through, run the DSPJOBLOG command from the command line to check for error codes posted. Contact Kisco if you need help with your system configuration at this point. If you have Kisco Connect installed and activated in i2Pass, you can also test text addresses using this option.

Work With Admins

This option lets you control which user profiles can be used to administer the i2Pass software on your system. When you start option 11 on the INSTALL menu or use the WRKI2PUSR command from the I2PLIB library, the following display will show:

```

Session F - [24 x 80]
File Edit View Communication Actions Window Help
Maintain End-User Table          USRMTP

Type options, press Enter.
  2=Change    4=Delete    5=Display
  User       User
Opt Profile  Type
- I2PASSUSR  A  i2Pass System Profile-DO NOT DELETE
- QSECOFR    A  Security Officer

F3=Exit      F5=Refresh   F6=Create

Bottom

MA f 03/007
128 I902 - Session successfully started

```

As shipped from Kisco, the two user profiles shown above are always included. You cannot delete either of these.

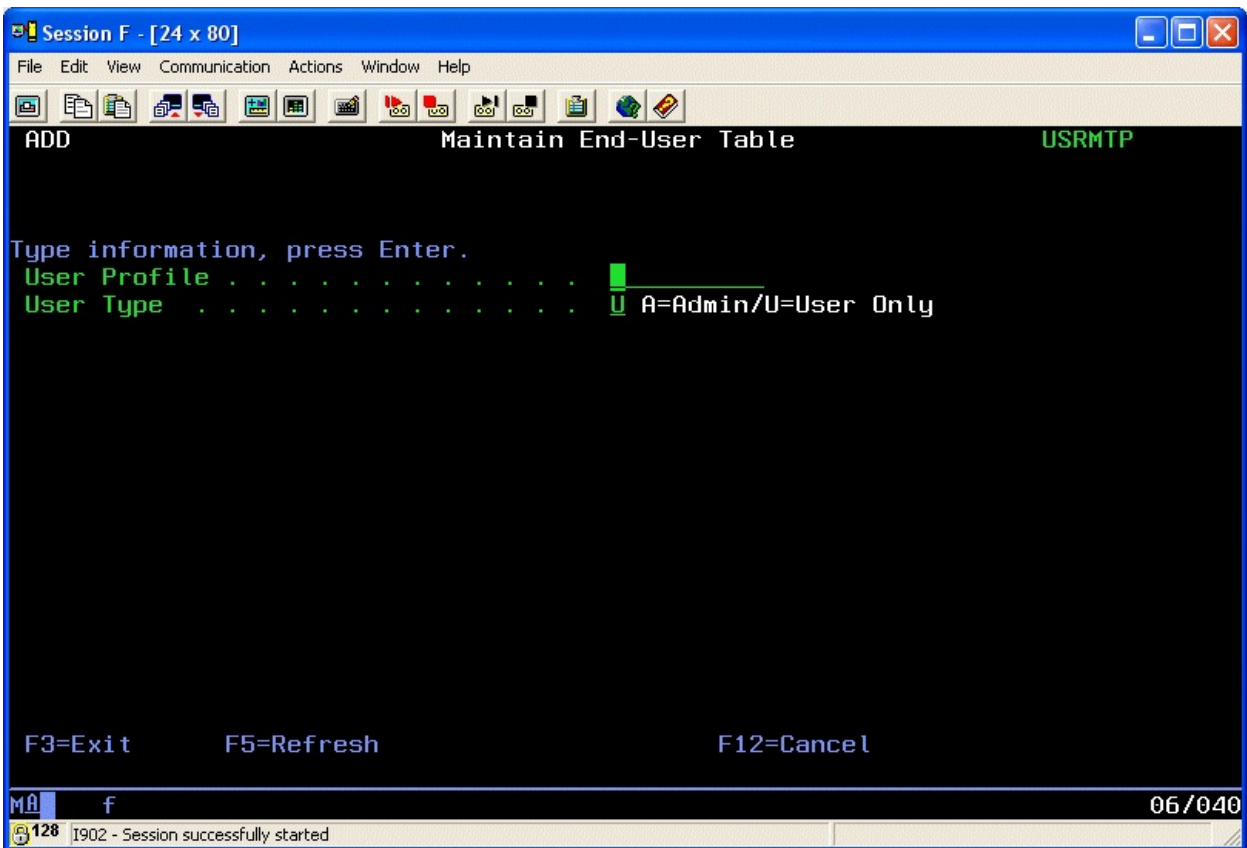
i2Pass provides for two different levels of admin profiles as follows:

Type A - Full administrative privileges

Type U - Limited privileges

The type U administrator can enroll user profiles, but they cannot run any of the purge functions, remove user profile enrollments or work with admins using option 11 on the INSTALL menu.

To add a new admin to this list, use the F6 function key. The following add screen will be displayed:



Enter the user profile that you want to add and assign the type of admin code you want to use and press ENTER. The user will be added to the list of profiles allowed to administer i2Pass.