

i2Pass

Bluescape Browser Interface

Version 4

As of August 2023



**Kisco Systems LLC
54 Danbury Road, #439
Ridgefield, CT 06877**

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

© 2023 Kisco Systems LLC

Table Of Contents

Introduction	1
Overview	1
Using The Bluescape Interface	2
Browser Navigation	3
Enrollment Display Panel	4
Initial Admin Display Panel	6
Initial Display Options	7
Notification Address	7
Adding Users	8
Editing Users	10
Changing Initial Program	11
Removing A User	12
Managing Devices	12
Adding Devices	13
Activity Log	14
Activity Log Purge	15
Global Settings	16
Authorized i2Pass Users	21
Apache HTTP Server Configuration	23
Security Considerations	25
Configuring Apache for HTTPS Secure Use	26

Introduction

This documentation covers the Bluescape i2Pass browser interface only. This documentation is intended to provide you with information on how to configure the Apache HTTP server on your IBM i server to run the browser interface for i2Pass and instructions on using this browser based interface to the product.

Instructions for installing and maintaining the software can be found in the i2Pass User's Guide.

Overview

The Bluescape browser interface for i2Pass is a feature that allows you to administer i2Pass using a web browser. This requires that your IBM i OS use the Apache HTTP web server activated and configured to support i2Pass calls.

The Bluescape browser interface allows you to use the features of the browser to simplify and improve efficiency when working with i2Pass. Things like cut/paste, action buttons and browser field content prompts will help your use of i2Pass.

Using The Bluescape Interface

To use the browser interface for i2Pass, you must first configure the Apache HTTP server on your system and start the server instance for i2Pass. Please refer to the separate configuration section of this documentation for instructions on how to set this up.

To get started, just type in the following URL on your browser:

`http://yoursystem.com:8677/i2plogon.htm`

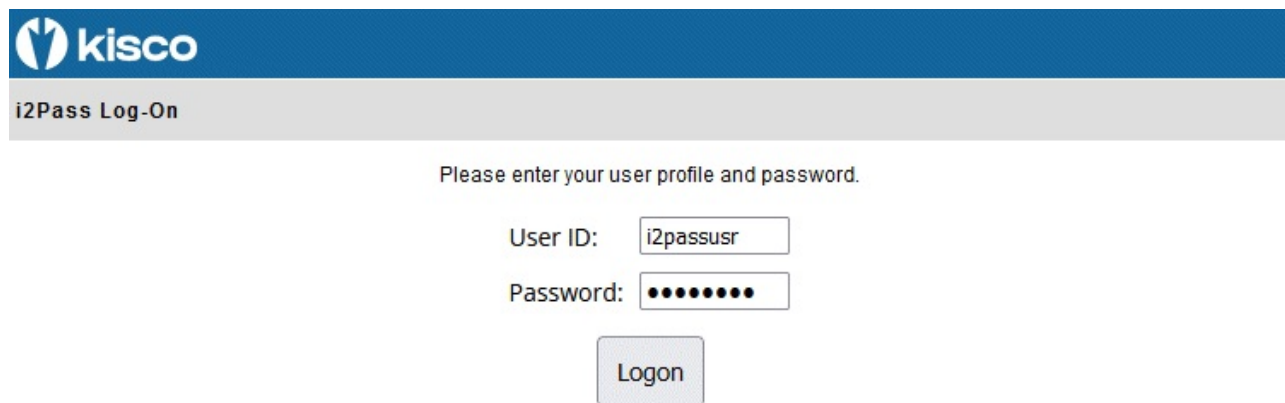
If you have secure HTTPS configuration completed, replace the “http” with “https”.

Replace the “*yoursystemi.com*” with a reference to your IBM I TCP/IP address. You can use either a named address or a numerical address, such as “10.1.1.12”.

If your IBM i system is configured for long passwords, then replace the `i2plogon.htm` with `i2plogon2.htm`.

Important note: The initial recommendation from Kisco Systems is to implement the web interface using the HTTP connection. This connection is not secure and it is recommended that you take precautions as your user profile and password will be passed as open text through your network. See the documentation for setup considerations for an HTTPS secure connection.

When you enter the above URL, the following will be displayed by your browser:



Please enter your user profile and password.

User ID:

Password:

Log on to your system using a user profile that is authorized to use i2Pass.

Browser Navigation

The Bluescape browser interface will always have two navigation bars near the top of each display panel:



On the top blue line, you can always exit your Bluescape session by selecting the arrow icon on the right panel. This will give you a log off confirmation and give you a link to log back on.

The gear icon will let you access the global settings for i2Pass. Please see the separate section of this documentation for information on how to control the settings.

The second gray line will always show a text description of the current display on the left. Then, on the right, optional dark gray action buttons will be displayed. These will change with each function that you access. The above example is taken from the initial display when you first sign on.

At any point during your use of the Bluescape browser interface, you browser's backup function is also available to you. Keep in mind, however, that this will not undo any changes that have been made along the way.

Enrollment Display Panel

When the logon completes, the status of the user profile will be checked. If the profile is enrolled for i2Pass as an end user and they have not yet completed their enrollment process, the following panel will be presented. The enrollment must be completed.

If the user profile is an admin for i2Pass and they are either not enrolled as an end user or that enrollment has been completed, then the Initial Admin Display panel will appear. See the next section of this guide for further instructions.

When a user profile has been enrolled but that enrollment has not yet been completed, the following panel will be shown:

COMPLETE I2PASS ENROLLMENT

User Profile: TESTI2P

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.

<u>Description</u>	<u>Address</u>
Contact Address 1	<input type="text"/>
Contact Address 2	<input type="text"/>
Contact Address 3	<input type="text"/>

You may enter an email address or a text address. When all addresses have been entered, press Send Codes. A single use verification code will be sent for each address entered. Type these values back in on the next panel.

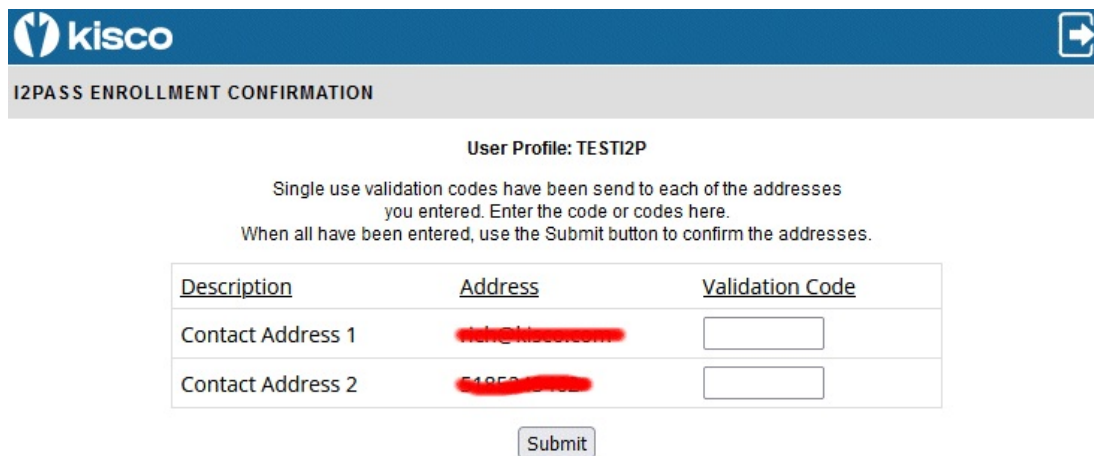
Kisco Connect is installed with the DUO option

With Kisco Connect installed, you can enter a cell phone number and text messages will be sent there.

To complete the enrollment, you can enter up to three contact addresses. The address or addresses will be used to send 2FA codes during an MFA verification process. Any valid email address can be used. If your system has Kisco's Kisco Connect installed, you can optionally enter a cell phone number. If Kisco Connect is installed with the DUO option, then you can specify *DUO as a contact address. When you use *DUO, you can only enter a single contact address.

After you have completed these entry fields, use the Send Codes button. A different 9 digit code will be sent to each contact address you specify. If you specified *DUO, a DUO authentication process will be started. Once that DUO process has been confirmed, your registration process will be considered to be complete. If an email address or cell phone # was used a new entry panel will be shown.

To confirm the MFA codes sent, the following panel will be shown:



kisco

I2PASS ENROLLMENT CONFIRMATION

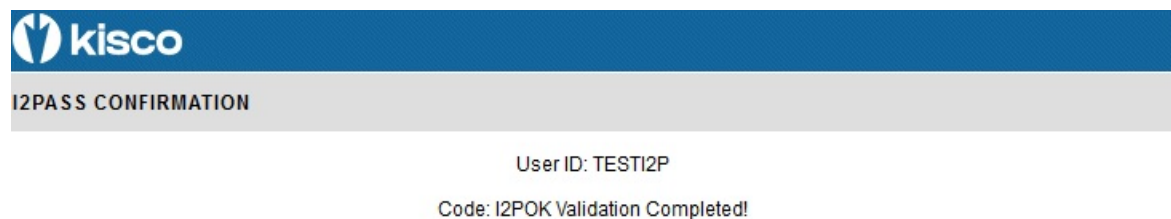
User Profile: TESTI2P

Single use validation codes have been send to each of the addresses you entered. Enter the code or codes here.
When all have been entered, use the Submit button to confirm the addresses.

Description	Address	Validation Code
Contact Address 1	[Redacted]	<input type="text"/>
Contact Address 2	[Redacted]	<input type="text"/>

Submit

Enter the 9 digit code sent to each of the contact addresses and then use the Submit button. The codes will be validated and your enrollment will be completed. The following confirmation will be displayed and you will be logged out of the i2Pass system.



kisco

I2PASS CONFIRMATION

User ID: TESTI2P

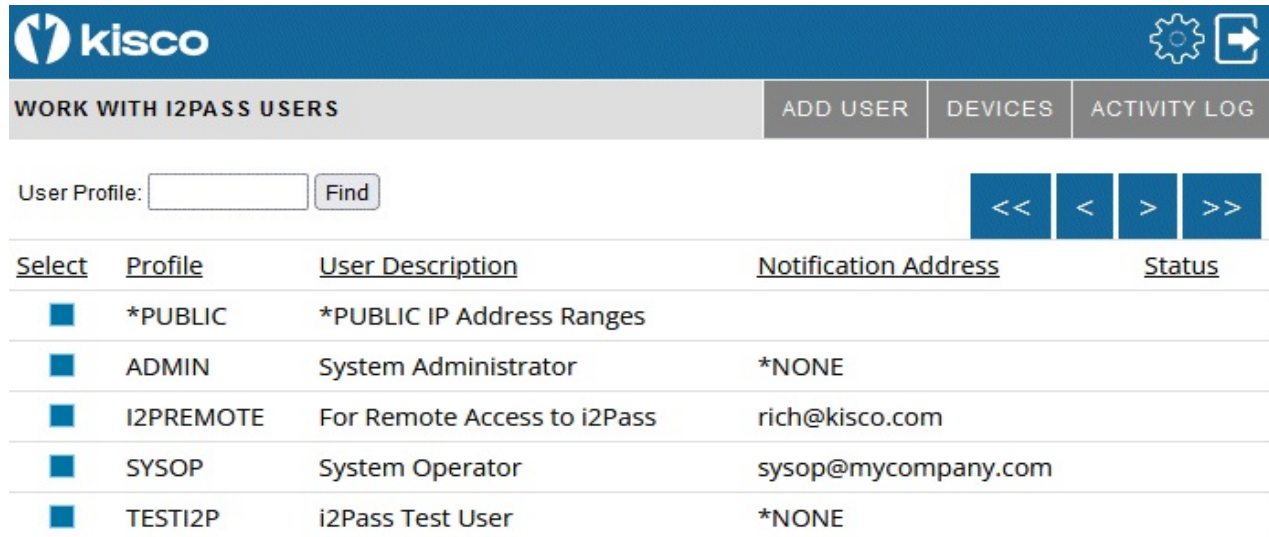
Code: I2POK Validation Completed!

If you are registered in i2Pass as an Admin, you can now sign back in to access the administrative functions available in the Bluescape interface.

If you are not an Admin, your next logon access to your system via an untrusted device will require an MFA process to complete successfully.

Initial Admin Display Panel

When an admin logon is completed, the following starting point display will come up in your browser:



The screenshot shows the Kisco admin interface. At the top is a blue header with the Kisco logo and a settings icon. Below the header is a navigation bar with buttons for "ADD USER", "DEVICES", and "ACTIVITY LOG". The main content area has a "User Profile:" search box with a "Find" button and four blue arrow buttons for navigation: "<<", "<", ">", and ">>". Below this is a table with the following data:

Select	Profile	User Description	Notification Address	Status
<input type="checkbox"/>	*PUBLIC	*PUBLIC IP Address Ranges		
<input type="checkbox"/>	ADMIN	System Administrator	*NONE	
<input type="checkbox"/>	I2PREMOTE	For Remote Access to i2Pass	rich@kisco.com	
<input type="checkbox"/>	SYSOP	System Operator	sysop@mycompany.com	
<input type="checkbox"/>	TESTI2P	i2Pass Test User	*NONE	

Bottom

After a successful logon, a timer will start every time you select a function. If your session lies dormant for longer than the browser timeout setting, it will time out and the next time you try to start a process, you will be forced back to the logon page. The browser timeout value is shipped set to 60 minutes from Kisco, but can be changed using the global settings icon.

The number of detail lines that you see on this screen can be controlled from a value in the global settings. Please see that section of the manual. As shipped from Kisco, this is set to 15 lines per panel.

You can use the blue arrow buttons to scroll through the list of users as follows:

- << Takes you to the first profile on file
- < Scrolls backwards one panel
- > Scrolls forward one panel
- >> Takes you to the last profile on file

To jump directly to a specific profile or a section of users, type that selection in the User Profile box and press the *Find* button.

Each of the dark gray action buttons is described in a separate section in this documentation.

From this display, you can review the details of a user registration, make changes or remove a registered user. Use the blue button under the "Select" column to bring up the user registration details. The user profile *PUBLIC cannot be removed and is used for establishing global IP address ranges.

Initial Display Options

The following options are available along the top of the initial display. Each of the gray buttons will do the following:

- | | |
|--------------|---|
| ADD USER | A new user profile or group of user profiles can be registered. |
| DEVICES | The current status of devices known to i2Pass will be shown along with whether or not they are trusted by i2Pass. |
| ACTIVITY LOG | The i2Pass activity log will be displayed. See the Activity Log section of this user's guide. |

Notification Address

Each registered user includes an entry field for up to three notification addresses. With the base i2Pass software installed, a valid email address may be entered in any of the three fields. The fields must be completed in sequence with the first always used.

If you also have Kisco Connect installed on your system, you can enter a cell number as an all numeric string. Any notifications will be sent as SMS text messages routed through Kisco Connect.

If Kisco Connect is installed with the DUO option activated, then you can use the special value *DUO, but only on the first address with the other two left blank.

Adding Users

To add a new user or group of users, select the ADD USER button on the initial display panel. When you do, the following will be shown:

Description	Setting
User Profile(s)	<input type="text"/> User Profile, GENERIC*, *ALL
Active Users Only?	<input type="radio"/> *NO (All user profiles) <input checked="" type="radio"/> *YES (Only active profiles)
IP Address Checking Active?	<input checked="" type="radio"/> *NO <input type="radio"/> *YES
Enrollment Option:	<input checked="" type="radio"/> *NONE (Enroll for Email/SMS) <input type="radio"/> *DUO (Enroll for DUO)

Kisco Connect available for SMS and DUO

To return to the list of registered users without taking any action, select the GO BACK button.

To add a user or a group of users, fill in the fields as follows:


User Profile(s)	<p>You can enter one of the following values:</p> <p>User profile enter an individual user profile. Just that user will be registered.</p> <p>GENERIC* end a generic profile pattern. All user profiles that match the pattern and are not currently registered will be added to the user registration.</p> <p>*ALL all user profiles that are not already registered will be added.</p>
Active Users Only?	Controls whether all user profiles are to be registered or just active user profiles. A user profile is considered to be active if it has a status of *ENABLED.
IP Address Checking Active?	<p>Determines whether this user's terminal sign-on sessions will be checked against a list of valid IP addresses established for them.</p> <p>Choose one of the following:</p> <p>*NO Terminal sign-on processes will not be checked.</p> <p>*YES Terminal sign-on processes will be check against a list of valid IP addresses for this user.</p>
Enrollment Option	Controls how the user or users will be enrolled. Choose as follows:



- *NONE The users will be enrolled for email and/or SMS notification. For an individual user, this can later be changed to *DUO if desired.
- *DUO The users will be enrolled for *DUO validation control.

At the bottom of this panel, you will see whether or not Kisco Connect is installed on your system. To use the DUO option, Kisco Connect must be installed with the DUO option enabled. To use direct SMS notifications, Kisco Connect must be installed but the DUO option does not need to be enabled.

Editing Users

Once a user is registered, you can edit their registration details by selecting the blue button under the Select column on the initial display. When you do, the following panel will be shown:



WORK WITH I2PASS USERS

INIT PGM
GO BACK

Field Description	Field Contents
User Profile	<input type="text" value="ADMIN"/>
Initial Program/Library	<input type="text" value="*NONE"/> / <input type="text"/>
User Description	<input type="text" value="System Administrator"/>
Notification Addresses	<input type="text" value="*NONE"/> <input type="text"/> <input type="text"/>
Code Format	<input checked="" type="radio"/> 999999999 <input type="radio"/> 999-999-999 <input type="radio"/> 999.999.999 <input type="radio"/> 999/999/999
Daily 5250 Check	<input checked="" type="radio"/> *NO <input type="radio"/> *YES
Failed Signons	0
IP Address Active?	<input checked="" type="radio"/> *NO <input type="radio"/> *YES
List User?	<input checked="" type="radio"/> *NO <input type="radio"/> *YES

Update
[Remove This User](#)

Kisco Connect available for SMS and DUO

Note: When you select the *PUBLIC user profile, only a few of the fields are available and the option to remove the record does not appear.

On this panel, you cannot change the user profile or the initial program fields, but the following are available:

User Description When the user is added, the user profile description is picked up from the current user profile. This can be changed in i2Pass if desired.

Notification Addresses See the previous section in this documentation about Notification Addresses for details.

When a user is first registered, the first of these three addresses will be set to either *NONE or *DUO. If *DUO is used, then it should not be changed and the 2nd and 3rd addresses must be left blank.

If *NONE appears, you can change it to a valid notification address here. If you leave it set to *NONE, then the first time the user signs on to a terminal session, they will be prompted to complete their registration by supplying notification addresses. They can also complete their registration from a browser session by logging in to i2Pass Bluescape.

Code Format

Controls how the 2FA code is presented to this user. Select the option desired. The values that you can choose are:

The code will be presented as a 9 digit number, nnnnnnnnn

The code will be presented as 9 digits separated by the hyphen character, nnn-xxx-xxx

The code will be presented as 9 digits separated by periods, nnn.nnn.nnn

The code will be presented as 9 digits separated by the slash character, nnn/xxx/xxx

Daily 5250 Check

If the Daily 2FA Check in the Global Settings is set to *OPT, this setting will control how daily 2FA checking is done for the registered user. A value of *YES will allow once a day 2FA code processing for this user. *NO will ignore the daily check and always require a 2FA code.

Changing Initial Program

When editing a user registration, you will see the Initial Program and library displayed, but you cannot make any changes. When a user is registered, the initial program associated with the user profile is captured by i2Pass. To make changes to this setting for the user, use the INIT PGM gray button at the top of the edit panel. When you do, the following will come up:

Field Description	Field Contents
Initial Program/Library	*NONE / <input type="text"/>

To change the initial program, enter the program name and the library where it resides on your system. Press the Update button to process the change. The user details will be shown again with the change recorded.

Removing A User

When you edit a registered user profile, you can delete that registration. Use the [Remove This User](#) link at the bottom of the display. You will be asked to confirm your decision and can cancel the removal at that time with no action taken. When you confirm the removal, the registered user profile will be removed from i2Pass and their initial program setting will be restored to their user profile.

Managing Devices

i2Pass can recognize terminal devices as “Trusted” or “Untrusted”. Untrusted devices must use a second authentication factor in order to complete a signon process for an enrolled user profile. To manage how the devices are identified to i2Pass, use the DEVICES gray button at the top of the initial display panel. The following panel will be shown:

Select	Device Name	Device Description	Status
<input type="checkbox"/>	CITX020000	CITX Device 1	Trusted
<input type="checkbox"/>	DSP01	Console	Trusted

When you first install i2Pass, this list will be empty. You can use the navigation features to scroll through this list or use the Find button to position the list at a specific device or segment.

To change either the device description or trust status, use the blue button under the Select column.

Field Description	Field Contents
Device Name	<input type="text" value="CITX020000"/>
Device Description	<input type="text" value="CITX Device 1"/>
Trusted?	<input checked="" type="radio"/> Trusted <input type="radio"/> Untrusted

[Remove This Device](#)

Make the changes that you want and use the Update button to record the change. The full list of

devices will then be shown again. If you want to delete the device from the i2Pass device registrations, you can use the [Remove This Device](#) link and the device will be removed.

Adding Devices

To add a device or devices, use the ADD DEVS gray button at the top of the panel that lists currently defined devices.

The following display will be shown:

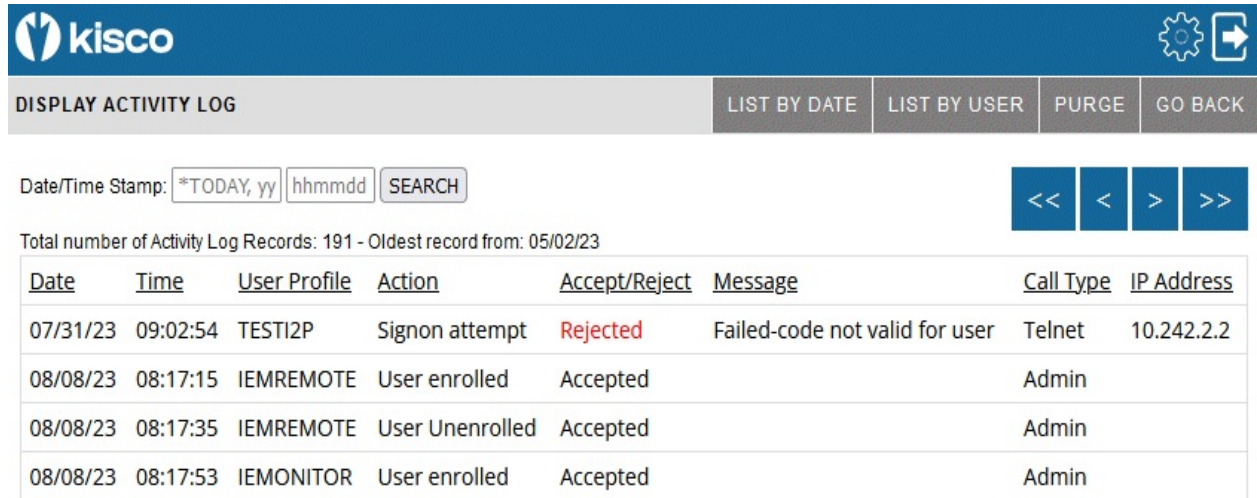
<u>Description</u>	<u>Setting</u>
Device(s)	<input type="text"/> Device Name, GENERIC*, *ALL

Add

You can add an individual device, a group of devices or all devices. When the group or all option is used, only devices that are not already registered to i2Pass will be added. When you select the Add button, the devices specified will be processed and the device list will be shown again with the additions reflected.

Activity Log

From the Initial Display, you can view the i2Pass Activity Log by selecting the ACTIVITY LOG gray button at the top of the panel. The following display will appear:



<u>Date</u>	<u>Time</u>	<u>User Profile</u>	<u>Action</u>	<u>Accept/Reject</u>	<u>Message</u>	<u>Call Type</u>	<u>IP Address</u>
07/31/23	09:02:54	TESTI2P	Signon attempt	Rejected	Failed-code not valid for user	Telnet	10.242.2.2
08/08/23	08:17:15	IEMREMOTE	User enrolled	Accepted		Admin	
08/08/23	08:17:35	IEMREMOTE	User Unenrolled	Accepted		Admin	
08/08/23	08:17:53	IEMONITOR	User enrolled	Accepted		Admin	

You can navigate your way through the Activity Log using several methods. The four blue arrow buttons near the top of the panel will act as follows:

- << Takes you to the oldest records on file
- < Scrolls backwards one panel
- > Scrolls forward one panel
- >> Takes you to the newest records on file

In addition, you can select a specific date and time where you want to start your review. Select the date and time you want to start with. Dates should be entered in yyyyymmdd format. A special value of *TODAY will bring up the most recent activity records. Use the SEARCH button once these values have been set.

From this display, you can generate a printed listing of the log in date sequence or by user profile. When you select those buttons, there will be a short pause that the report will be sent to the default printer defined in the Global Settings.

Activity Log Purge

When you no longer want older records from the Activity Log, you can remove them from the log by selecting the PURGE LOG gray button at the top of the panel. You will be asked to confirm your selection, then the following selection panel will be shown:

KISCO

PURGE LOG GO BACK

Purge Date: yyyyymmdd

Purge Days: 1-999

Run Purge

Enter a date or days, but not both

To run the purge, enter one of the two values shown. Do not enter both.

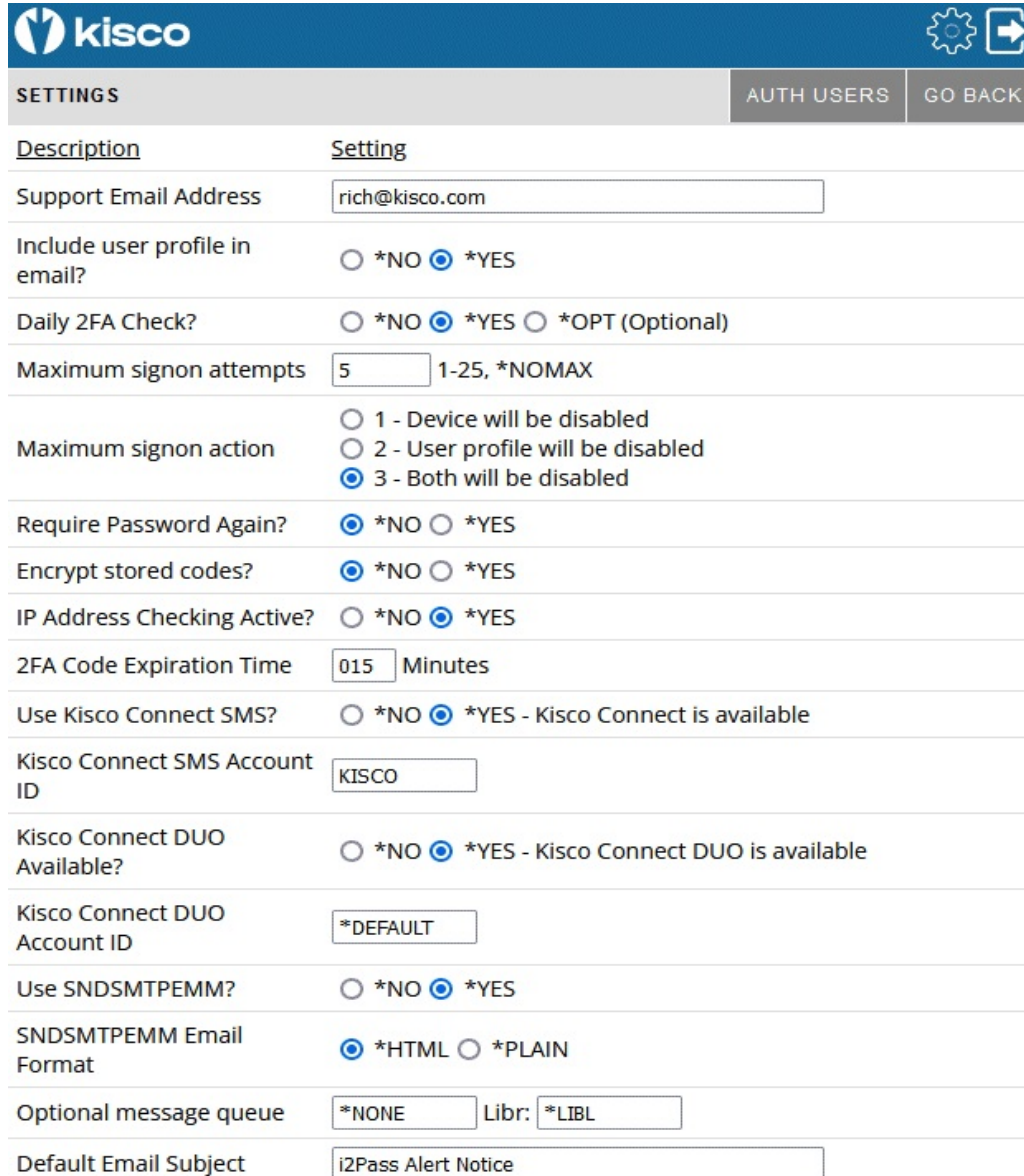
Purge Date: Enter the oldest date that you want to keep on file in format yyyyymmdd

Purge Days: Enter the number of days that you want to keep on file. Older records will be purged.

When you select the Run Purge button, a confirmation panel will be shown before the purge is actually run. The purge may take a while to complete before the next panel is then shown. The results of the purge will appear on the information line at the top of the panel.

Global Settings

Every display panel will give you access to the Settings controls by using the gear icon at the top of the panel. Settings are global settings and controls for i2Pass and help control how it is implemented on your system. The Settings panel appears as follows:



Description	Setting
Support Email Address	<input type="text" value="rich@kisco.com"/>
Include user profile in email?	<input type="radio"/> *NO <input checked="" type="radio"/> *YES
Daily 2FA Check?	<input type="radio"/> *NO <input checked="" type="radio"/> *YES <input type="radio"/> *OPT (Optional)
Maximum signon attempts	<input type="text" value="5"/> 1-25, *NOMAX
Maximum signon action	<input type="radio"/> 1 - Device will be disabled <input type="radio"/> 2 - User profile will be disabled <input checked="" type="radio"/> 3 - Both will be disabled
Require Password Again?	<input checked="" type="radio"/> *NO <input type="radio"/> *YES
Encrypt stored codes?	<input checked="" type="radio"/> *NO <input type="radio"/> *YES
IP Address Checking Active?	<input type="radio"/> *NO <input checked="" type="radio"/> *YES
2FA Code Expiration Time	<input type="text" value="015"/> Minutes
Use Kisco Connect SMS?	<input type="radio"/> *NO <input checked="" type="radio"/> *YES - Kisco Connect is available
Kisco Connect SMS Account ID	<input type="text" value="KISCO"/>
Kisco Connect DUO Available?	<input type="radio"/> *NO <input checked="" type="radio"/> *YES - Kisco Connect DUO is available
Kisco Connect DUO Account ID	<input type="text" value="*DEFAULT"/>
Use SNDSMTPEMM?	<input type="radio"/> *NO <input checked="" type="radio"/> *YES
SNDSMTPEMM Email Format	<input checked="" type="radio"/> *HTML <input type="radio"/> *PLAIN
Optional message queue	<input type="text" value="*NONE"/> Libr: <input type="text" value="*LIBL"/>
Default Email Subject	<input type="text" value="i2Pass Alert Notice"/>

There are more fields on the panel that are not shown here.

Set these parameters 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. (Not used by SNDSMTPEMM)

Include user profile?

Lets you specify that the notification message with 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 failing 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 failing 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 failed 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 The device and 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 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?

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.

Choose one of these options:

*NO Re-entering of the user's password will not be requested. (Default)

*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.

Encrypt stored codes?

Controls whether the 2FA codes stored by i2Pass are encrypted or stored in plain text.

Choose one of these options:

*NO The 2FA codes are stored in plain text. (Default)

*YES The 2FA codes are encrypted.

IP Addr Checking Active?

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.

Choose one of these options:

*NO IP Address checking is not active.

*YES IP Address checking is active for users where the feature is active.

2FA Code Expiration Time

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.

Use kConnect SMS?	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.
kConnect ACCT ID	If you have Kisco Connect installed on your system, this setting specifies the Twilio account definition that you want to use.
kConnect DUO Available?	Controls whether authentication using DUO will be performed using Kisco Connect. For this to be used, the kConnect product must be installed at level 2 or higher. kConnect level 1 does not support DUO authentication.
kConnect DUO ACCT ID	If DUO authentication will be used, the DUO Account ID being used will be entered here. The *DEFAULT value will work if kConnect has been installed and configured and tested for DUO authentication. You may have decided to set up a different account ID in which case enter that account ID here.
Use SNDSMTPEMM?	Controls which email transport mechanism is used by i2Pass to send email from your system. Choose one of the following values: *YES When an email is sent, the IBM i SNDSMTPEMM protocol will be used. Note: This is only valid on system running IBM i OS 7.3 or later. *NO The legacy protocol will be used to send email. This is required on systems running IBM i OS 7.2 or earlier.
SNDSMTPEMM Email Format	Controls how your notification emails are formatted when you are using the SNDSMTPEMM protocol. Choose one of the following values: *HTML The email will be formatted with HTML. Note: This is only valid when “Use SNDSMTPEMM” is set to *YES. *PLAIN The email will be formatted in plain text.
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.

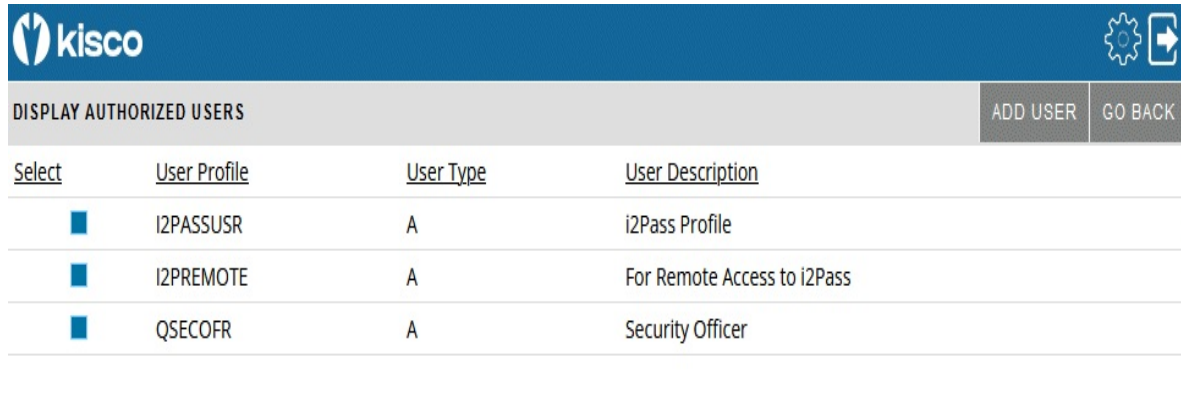
Default Email Subject	This value will be used as the Email Subject when alerts and notification messages are sent. If you are using i2Pass in a multiple partition or multiple server installation, you can use this to differentiate the notification messages so that you know which platform is issuing the message.
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.
Browser Roll Factor	Enter the maximum number of lines that you want to be shown on a multi-line browser panel. Kisco recommends starting this set to 15 but any value from 2 to 50 will be accepted.
Browser Timeout Limit	When you start a Bluescape session, the current time is noted. If no activity happens in the session for the number of minutes entered here, then a new logon will be needed. As shipped from Kisco, this is set to 60 minutes. You can change it to another value up to 999.
Default Printer Device	Some functions in i2Pass generate listings. This setting will control where those listings are printed. You can enter a specific printer name or use the special value *DFT to use the system's default printer device as specified in system value QPRTDEV.

At the base of the Global Settings panel you will see information about the level of the installed i2Pass software, the latest PTF updates, the current IBM i OS level and the serial number and partition number where the software is installed. This information may be useful to Kisco Systems technical support team.

Authorized i2Pass Users

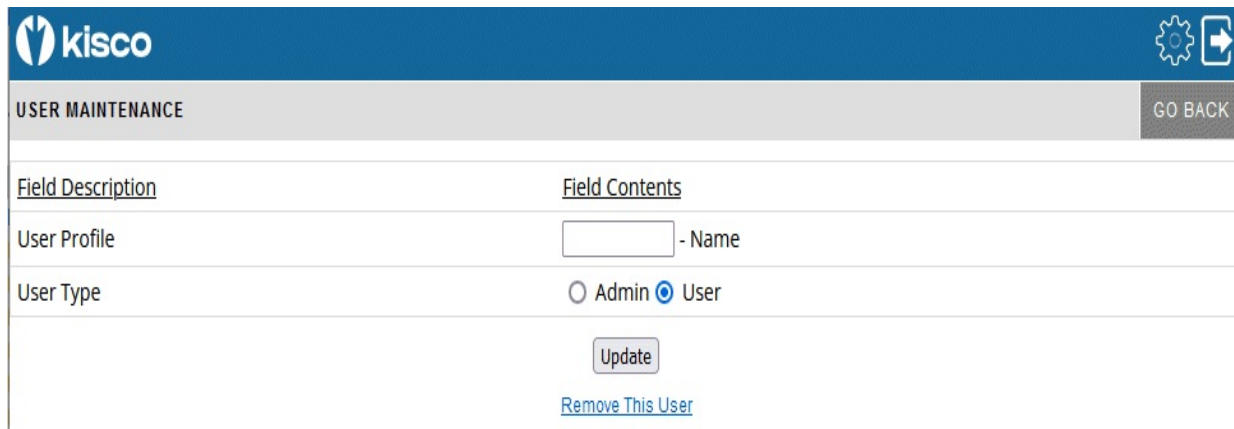
At the top of the General Settings panel there is a gray button labeled AUTH USERS. This lets you control who can administer i2Pass. You must be an authorized administrator for i2Pass before you can access this function. As shipped from Kisco Systems, the QSECOFR user profile is already authorized.

When you select this button, the following will be shown:



Select	User Profile	User Type	User Description
<input type="checkbox"/>	I2PASSUSR	A	i2Pass Profile
<input type="checkbox"/>	I2PREMOTE	A	For Remote Access to i2Pass
<input type="checkbox"/>	QSECOFR	A	Security Officer

This is a list of the currently authorized user profiles. You can maintain an existing user by selecting the blue button on the left side of the panel or you can add a new user by selecting the ADD USER gray box at the top. When you do, the following will be shown:



Field Description	Field Contents
User Profile	<input type="text"/> - Name
User Type	<input type="radio"/> Admin <input checked="" type="radio"/> User
<input type="button" value="Update"/>	
Remove This User	

Complete the entry as follows:

User Profile Enter a valid user profile.

User Type Select the type of user that you are registering.

Admin An admin user can use all functions and features of the i2Pass software product.

User For the Bluescape web browser interface for i2Pass administration, a User type can only look at settings and active tasks, they cannot change them, set up new monitors or start and stop monitors.

The Update button will add or update the entry being processed. If you want to remove a currently registered user, use the [Remove This User](#) link.

Apache HTTP Server Configuration

For the Bluescape interface for i2Pass to work, you will have to configure and activate a server instance for the Apache HTTP server on your IBM i.

The following checklist will have to be done to complete the configuration. The details will follow for each step.

- Step 1: Start the Apache Administrative server tool on your IBM i.
- Step 2: Create a new HTTP server instance named I2PASS
- Step 3: Install the HTTP Server objects for i2Pass
- Step 4: Start the new I2Pass server instance
- Step 5: Update End User Table

Step 1: Start the Apache Administrative server tool on your IBM i.

To configure an Apache server instance, you must first start the Administration server instance for Apache. You can do this from a command line on your IBM i with the following command:

```
STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
```

The server may take a while to initialize, so wait a few minutes before starting up the configuration wizard in your browser. When you are ready, point your browser to the following web address:

```
http://yoursystemi.com:2001/HTTPadmin
```

The system will prompt you for a user profile and password. Once that has been supplied, a page of IBM i Tasks will be displayed. Select the “IBM Web Administration for IBM i” option. This will take you to the Web Administration wizard that comes with your OS.

Step 2: Create a new HTTP server instance named I2PASS

After you sign on and get to the Web Administration page, navigate to the “Manage” tab and then the “HTTP Servers” tab below that. Under the “Common Tasks and Wizards”, select “Create HTTP Server”. For server name, you MUST specify the value “I2PASS”. The server description of “Kisco i2Pass Server” can also be used. Click on Next for all of the following displays taking all of the default options presented until you reach the “Create HTTP Server” panel with a “Finish” button at the bottom. Press the Finish button to complete creating the new server instance.

Step 3: Install the HTTP Server objects for i2Pass

On a terminal session where you are signed on as a security officer, go to the INSTALL menu in library I2PLIB by entering the following command:

```
GO I2PLIB/INSTALL
```

Run option #12 (Install HTTP Server Instance Objects) from this menu. This will install the HTTP server objects needed by i2Pass.

Step 4: Start the new I2PASS server instance

On a terminal session where you are signed on as a security officer, go to the MASTER menu in library I2PLIB by entering the following command:

```
GO I2PLIB/MASTER
```

To start the newly created server instance, run option #8. After the server has been started and running for about 30 seconds, run the following command from the command line:

```
WRKACTJOB JOB(I2PASS)
```

You should see at least 4 jobs running with the job name I2PASS. This will indicate that the server is running correctly.

Go to your browser and enter the following URL:

```
http://yoursystemi.com:8677
```

A test page should now be shown. This will indicate that the server is active.

Step 5: Update End User Table

To be able to logon to the Bluescape interface, a user profile must be enrolled in i2Pass as an Administrator. Run option #11 on the INSTALL menu and make sure that the user profile or profiles that you want to use for Bluescape are enrolled with Admin type code A for full access.

At this point, the Bluescape interface for i2Pass is available for use on your system.

If you want to configure your own server instance or use a different instance that is already active on your system, you can do so provided that the following are taken into account:

- Add I2PLIB as a directory entry
- ADD a URL mapping entry to map “/cgibin/” to I2PLIB
- Authorize user access to I2PLIB
- Permit CGI programs to be run from I2PLIB

If you have other HTTP server instances already running, you may want to configure the i2Pass instance so that it works from a different port number. If that is the case, then the access URL that you use to start the browser interface for i2Pass will appear as follows:

```
http://yoursystemi.com:8081/ifalogon.htm
```

In this example, the HTTP server instance is running on port number 8081. Only the starting URL needs to be changed, the other URLs within the product will pick up the correct port number from this initial use.

Security Considerations

For instructions on how to configure the Apache server for a secure HTTPS connection, please review the following section of this documentation.

If you decide to implement the Apache server without HTTPS security, then user is cautioned that the logon process used will pass a valid user profile and password through your network in open clear text. As a result, Kisco specifically recommends that you only use this feature in a secure network environment where all activity takes place behind a firewall or a strong network router using internal IP addresses only (using a VPN).

As a second level of security, we also recommend that you set up a special user profile for use with the Bluescape interface for i2Pass access. You should use this profile only for the purpose of logging in to i2Pass through your browser. When you set the profile up, it must be a security officer class, but to limit its function in the event that the profile and password are compromised, we recommend that you include the following additional specification when the profile is created:

INLMNU(*SIGNOFF)	This will force a logoff if someone tries to log on through a normal terminal session using this profile.
------------------	---

Also, if you have exit point control software in place, you should set this profile up to deny all network access to your system. This will prevent the profile from being used by FTP, ODBC, IBM i Access, etc. If you do not have exit point control software in place, we suggest you take a look at our SafeNet/i software for your system to guard against this threat.

Configuring Apache for HTTPS Secure Use

i2Pass supports use of the Bluescape interface over a secure HTTPS browser connection. We recommend that when you first set up and configure the browser interface on your system, that you use the previous non-secure configuration to get started. This will simplify the setup routine. The following documentation assumes that you already have a working configuration using plain HTTP browser connections to your IBM i server.

HTTPS Configuration Overview

The following sequence of events must be completed to convert your working HTTP server instance (named IEVENTMON) from a plain HTTP server configuration to a secure HTTPS server configuration.

1. Start the *ADMIN server instance on your IBM i and log in.
 2. Update your current HTTP server instance configuration to support HTTPS.
 3. Connect to the Digital Certificate Manager application on your browser.
 4. Create a new digital certificate in the *SYSTEM certificate store.
 5. Validate the newly created certificate.
 6. Assign the new certificate to the I2PASS application.
 7. Start the updated I2PASS server instance.
 8. Verify that the configuration is working correctly.
-

Step 1 - Start the *ADMIN server instance on your IBM i and log in.

From the command line on your system, enter the following command:

```
STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
```

This will start the IBM Web Administration for i tool on your system. This startup process can take a minute or two to complete. After waiting, go to your web browser and enter the following address in the address box of your browser:

```
http://yoursystemi.com:2001/HTTPadmin
```

You will be prompted for a logon process. **You must sign on as a security officer** with full authority to your system, such as QSECOFR.

Step 2 - Update your current HTTP server instance configuration to support HTTPS.

1. Select the “HTTP Servers” tab.
2. Use the Servers window and select the I2PASS server.
3. Make sure that the server instance is showing with the status of “Stopped”. If not you MUST stop it before you continue with this procedure.
4. In the left hand panel, select the “Security” option.
5. When the security display shows, enable SSL and on the following line, enter “I2PASS” in the Server Application ID.
6. Press the “Apply” button at the bottom of the display.
7. In the left hand panel, select the “General Server Configuration” option.
8. On the next display, locate the “Server IP addresses and ports to listen on” section.
9. Add port number 443 for this server instance.
10. If port number 80 is shown, it must be removed.
11. Press the “Apply” button at the bottom of the display.

At this point, the HTTP server instance has been updated. Do not try to start it again until the following additional steps have been completed.

Step 3 - Connect to the Digital Certificate Manager application on your browser.

In your browser, re-enter the base address for the i5/OS Tasks:

`http://yoursystemi:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0`

This will bring you back to the main menu. Select the link for the “Digital Certificate Manager”.

Note: The following process will self-issue a digital certificate for use with your HTTPS server instance. When used from your browser, this will give you a warning because your server is not a registered certificate issuer, but the process will work correctly as long as you bypass the warning. On some browsers, such as Firefox, you will be allowed to accept the certificate the first time you use it and it will not be questioned again. Other browsers may question your use every time. Regardless, you will know where the certificate came from and you will be able to trust it by virtue of that knowledge.

Step 4 - Create a new digital certificate in the *SYSTEM certificate store.

Select the button in the top left corner of your browser that reads “Select a Certificate Store”. On the next panel, select the *SYSTEM store and press the “Continue” button. (If the *SYSTEM store does not exist, you will need to first create it using the “Create New Certificate Store” link.) Your system will prompt you for the password for the *SYSTEM certificate store. If you don’t know the password, you can use the reset function to assign a new password. When you are finished, the *SYSTEM certificate store will be open and available.

Now, select the “Create Certificate” link from the left-hand panel. On the next panel, select the option for “Server or client certificate” and press the “Continue” button. Next, select the option for “Local Certificate Authority” and press “Continue” again. Now the certificate form is displayed. Fill out the required fields as follows:

Certificate label	Enter the value “I2PASS”.
Common name	Enter a unique name. Kisco recommends that you use the system name for your system (or partition) as shown from the DSPNETA command display.
Organization name	Enter the name of your company or organization.
State or province	Enter the name of the state or province where you are located.
Country or region	Enter an abbreviation for your country.

Select the “Continue” button at the bottom of the page and your certificate will be created.

Step 5 - Validate the newly created certificate.

In the left hand panel, select the “Manage certificates” link. Next, select the “Validate certificate” link. Choose the “Server or client” option and press the “Continue” button. Select the I2PASS that you just created, then press the “Validate” button at the bottom of the page. If everything with the certificate is OK, a message will be displayed confirming that the certificate is valid.

Step 6 - Assign the new certificate to the I2PASS application.

In the left hand panel, select the “Assign certificate” link. Select the I2PASS certificate, then press the “Assign to Applications” button. Locate the I2PASS application in the list displayed and place a check mark next to it. Press the “Continue” button. A message will be displayed confirming that the certificate is now assigned to the application.

Step 7 - Start the updated I2PASS server instance.

On the MASTER menu in library I2PLIB, start the HTTP server instance using option #8.

This will start the server instance that has been converted for use with HTTPS security along with the I2PASS subsystem. Use option following command to check if the server starts correctly.

```
WRKACTJOB JOB(I2PASS)
```

When active, it will have at least 4 jobs active. If the server instance fails to start, make sure there is not another server instance active using the secure port number 443. Only one application at a time can be active using this port. If you need more than one active, you will have to change the server instance to use a different port number.

Step 8 - Verify that the configuration is working correctly.

Once the server instance has been started, enter the following web address into your browser's address box:

```
https://yoursystemi.com
```

A test page from the I2PASS server instance should be displayed. As stated earlier, a warning message about the certificate in use may be issued by your browser. Please note the comments associated with Step 3 above about this issue.

Note: Switching to https will change the port number use for access. The default port number for https access will now be active so there is no need to specify port number 8080 as you did with plain http access unless an alternate port is required for your installation.