iFileAudit
Browser Interface

Version 7.07

As of June 2022

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/ifa/support**

© 2006-2022 Kisco Systems LLC

Table Of Contents

Introduction

This documentation covers the iFileAudit 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 iFileAudit and instructions on using this new browser based interface to the product.

Overview

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

Most iFileAudit functions that were previously available using the standard IBM i green-screen interface are available using the browser based product. Not all functions have yet been implemented, but Kisco is committed to making them all available. We appreciate your feedback on this new capability so that new implementations can be prioritized to customer requirements.

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

Current Limitations

The current implementation of browser interface for iFileAudit does not include support for all features of the iFileAudit product as implemented from a terminal session. The following features are not currently supported:

- Record key maintenance is not currently supported.
- The display journal attributes is not currently supported.
- The journal reset function is not currently supported.
- Printing reports is not currently supported.
- Purging the analysis history files is not currently supported.
- Support is not included for registering multiple files in a single operation.
- Support is not included for activating and deactivating multiple files in a single operation.

All of these features and functions are still available from the original green-screen version of the software.

Note that it is Kisco's intention to support these features from the browser interface in the future. If you find specific features that you would like to see transferred sooner than others, please notify Kisco by email so that your requirements can get prioritized.

Using The Browser Interface

To use the browser interface for iFileAudit, you must first configure the Apache HTTP server on your system and start the server instance for iFileAudit. 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:

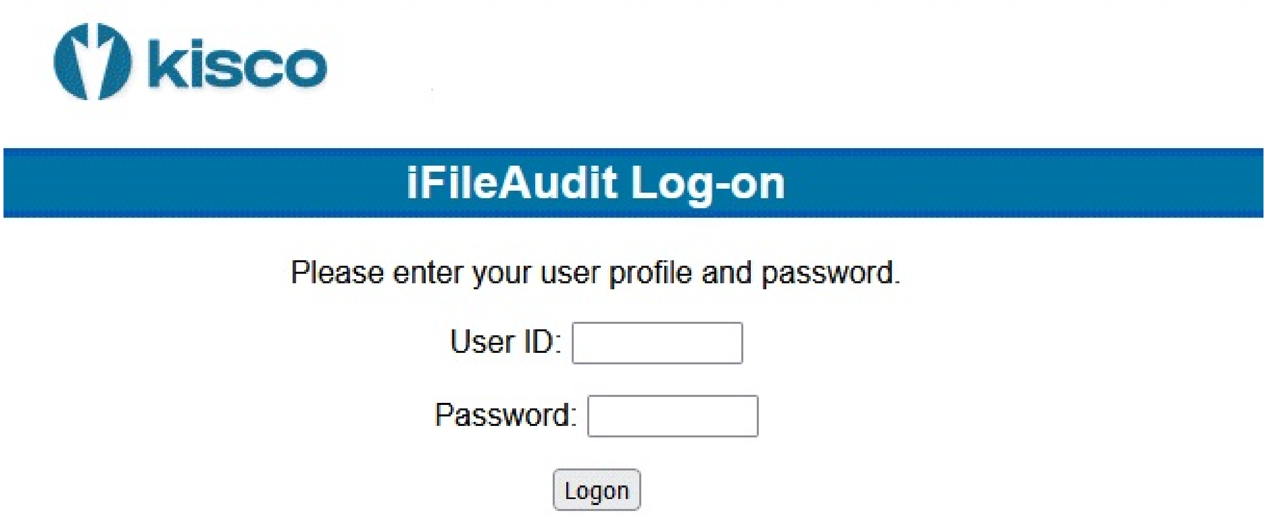
http://yoursystemi.com/ifalogon.htm

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".

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:



iFileAudit Log-on

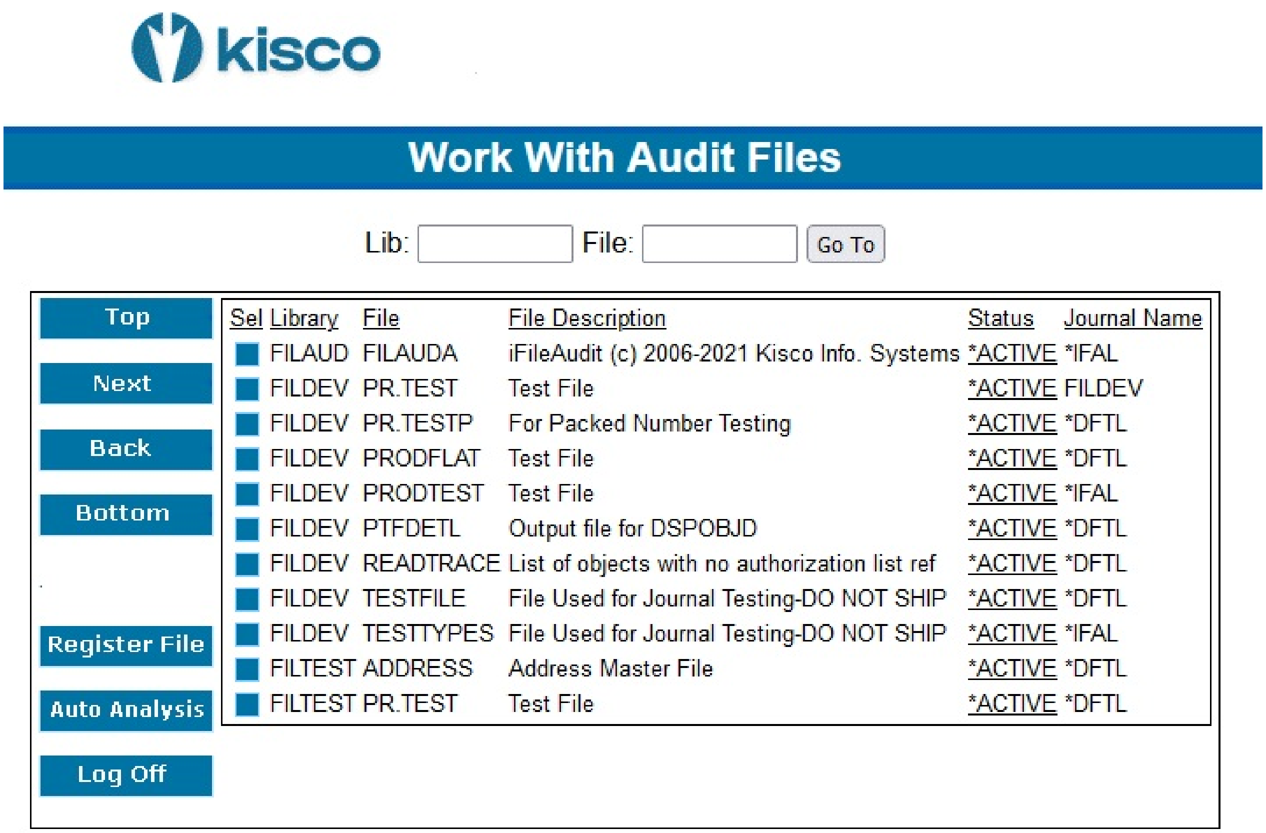
Please enter your user profile and password.

User ID:

Password:

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

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



Sel	Library	File	File Description	Status	Journal Name
■	FILAUD	FILAUDA	iFileAudit (c) 2006-2021 Kisco Info. Systems	*ACTIVE	*IFAL
■	FILDEV	PR.TEST	Test File	*ACTIVE	FILDEV
■	FILDEV	PR.TESTP	For Packed Number Testing	*ACTIVE	*DFTL
■	FILDEV	PRODFLAT	Test File	*ACTIVE	*DFTL
■	FILDEV	PRODTEST	Test File	*ACTIVE	*IFAL
■	FILDEV	PTFDETL	Output file for DSPOBJD	*ACTIVE	*DFTL
■	FILDEV	READTRACE	List of objects with no authorization list ref	*ACTIVE	*DFTL
■	FILDEV	TESTFILE	File Used for Journal Testing-DO NOT SHIP	*ACTIVE	*DFTL
■	FILDEV	TESTTYPES	File Used for Journal Testing-DO NOT SHIP	*ACTIVE	*IFAL
■	FILTEST	ADDRESS	Address Master File	*ACTIVE	*DFTL
■	FILTEST	PR.TEST	Test File	*ACTIVE	*DFTL

After a successful logon, a timer will start every time you select a function. If your session lies dormant for an hour, it will time out and the next time you try to start a process, you will be forced back to the logon page.

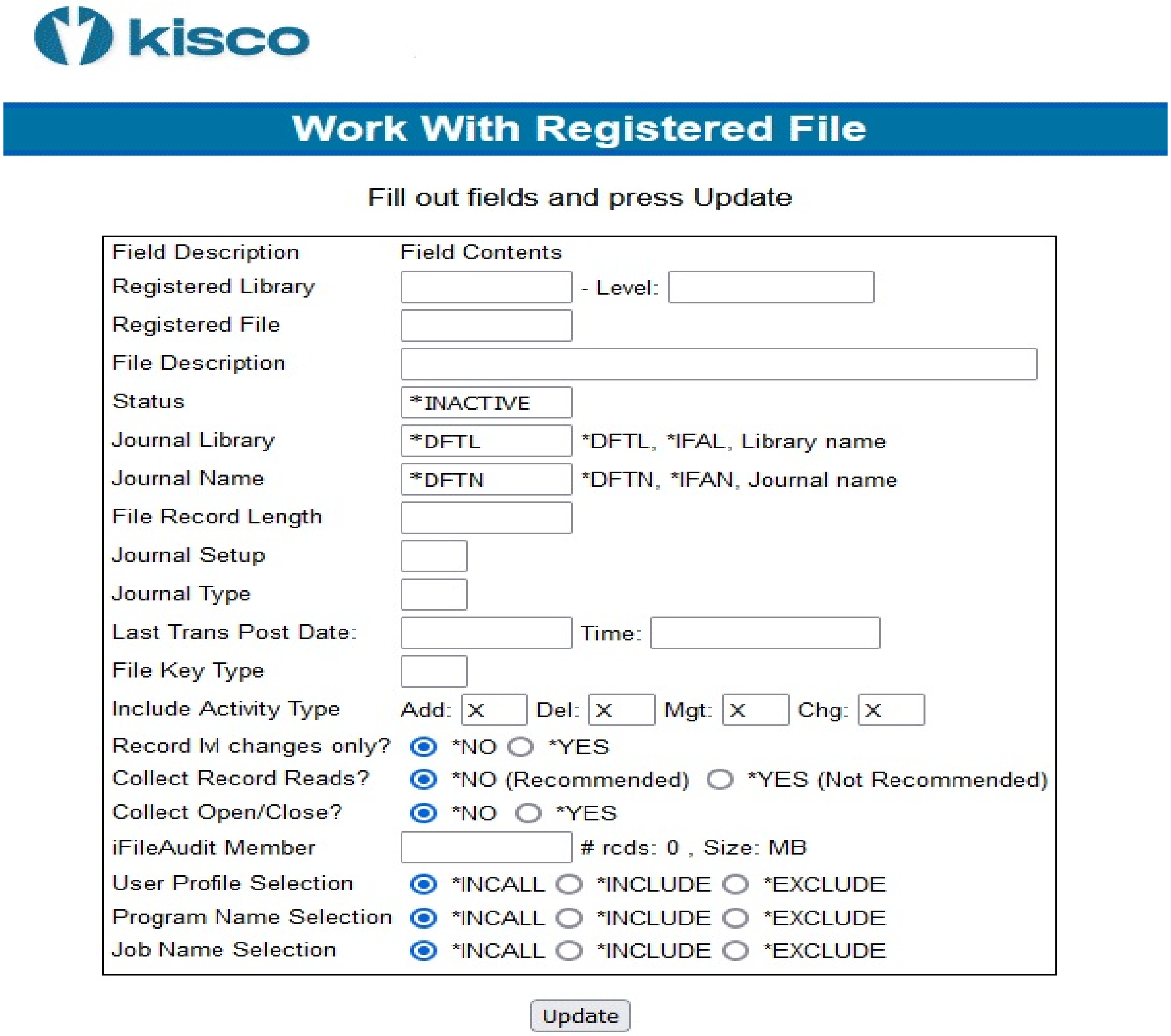
On this display, you will see the start of the list of registered files already set up in iFileAudit on your system. If the list is empty, then no files have yet been registered. The number of lines displayed on each panel can be customized. It defaults to 20 lines as shipped from Kisco Systems. The number of lines is stored in a data area named CONTROL in the application library named FILAUD in positions 111-113 and can be changed by you to meet your specific needs. For most test screens in this documentation, this value has been set to 15 lines.

The buttons along the left margin of the page are for moving through the list of registered files. Top will always take you back to the start of the list of registered files. Next will bring by the next set of files by moving the last file shown from the bottom of the list to the top. Back will scroll up through the list and Bottom will take you to the last set of registered file in the list.

You can also go directly to a specific library and file by entering values in the Lib and File entry fields. If you enter a library name (or partial library name) and leave the file blank, the list will start at the first entry that qualifies. The fields can be entered in either lower case or upper case.

To activate or deactivate a registered file, click on the status display for that file as listed. You will see the status change when the page is refreshed. For a registered file to be tracked by iFileAudit, it must be active.

To register a new file, select the Register File button at the bottom of the page. When you do, the following page will be displayed:



kisco

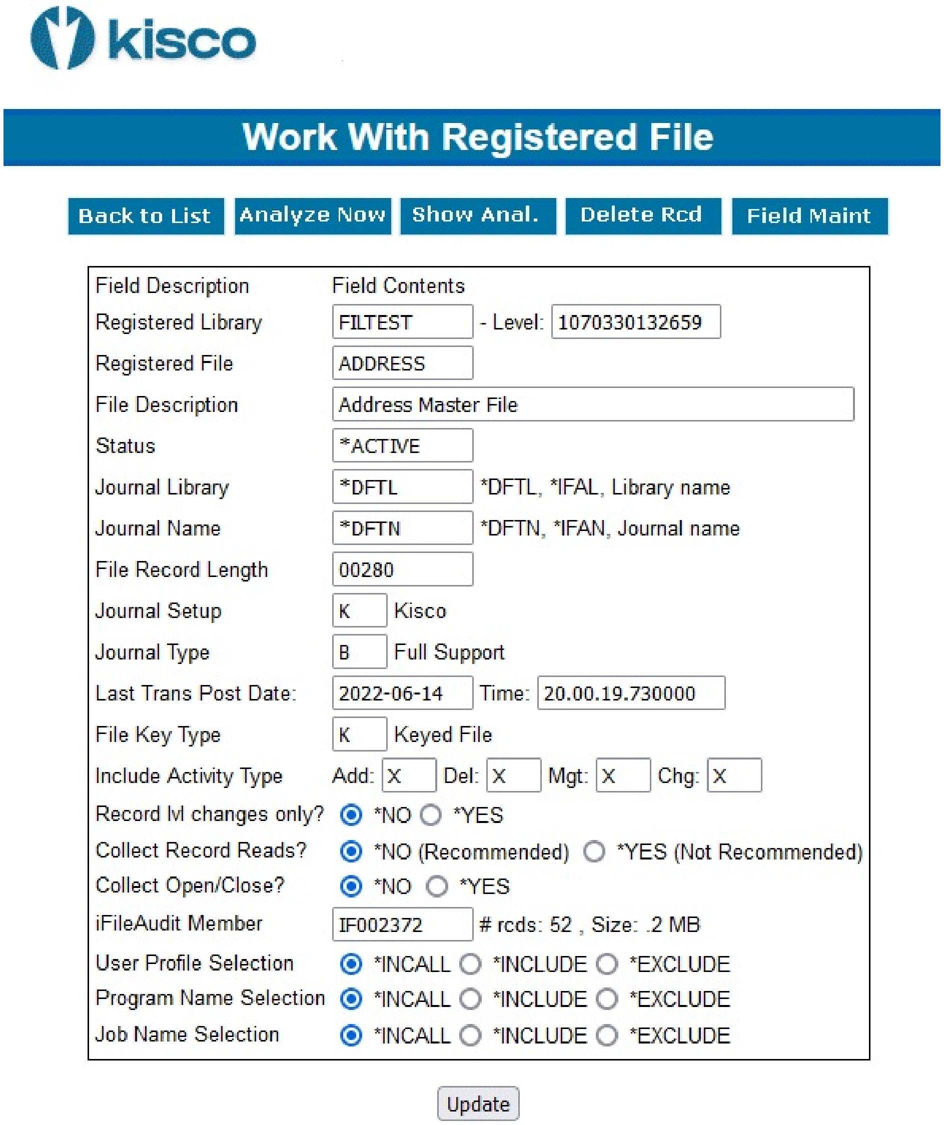
Work With Registered File

Fill out fields and press Update

Field Description	Field Contents
Registered Library	- Level:
Registered File	
File Description	
Status	*INACTIVE
Journal Library	*DFTL *DFTL, *IFAL, Library name
Journal Name	*DFTN *DFTN, *IFAN, Journal name
File Record Length	
Journal Setup	
Journal Type	
Last Trans Post Date:	Time:
File Key Type	
Include Activity Type	Add: X Del: X Mgt: X Chg: X
Record IVI changes only?	● *NO ○ *YES
Collect Record Reads?	● *NO (Recommended) ○ *YES (Not Recommended)
Collect Open/Close?	● *NO ○ *YES
iFileAudit Member	# rcds: 0 , Size: MB
User Profile Selection	● *INCALL ○ *INCLUDE ○ *EXCLUDE
Program Name Selection	● *INCALL ○ *INCLUDE ○ *EXCLUDE
Job Name Selection	● *INCALL ○ *INCLUDE ○ *EXCLUDE

To register the new file, enter the library name and file name. Also, if you want to use a different journal configuration (see the iFileAudit documentation), you can select that information here too. Press the Update button when ready. The page will return to the file list above with the newly registered file listed at the top of the page. The file will come up initially as inactive. You can either work with the registered file to make changes, or just go ahead and activate the file now.

To work with a registered file, select the blue box to the left of the file. When you do, the registration page will be displayed with the information about the file filled in as follows:



Field Description	Field Contents
Registered Library	FILTEST - Level: 1070330132659
Registered File	ADDRESS
File Description	Address Master File
Status	*ACTIVE
Journal Library	*DFTL *DFTL, *IFAL, Library name
Journal Name	*DFTN *DFTN, *IFAN, Journal name
File Record Length	00280
Journal Setup	K Kisco
Journal Type	B Full Support
Last Trans Post Date:	2022-06-14 Time: 20.00.19.730000
File Key Type	K Keyed File
Include Activity Type	Add: X Del: X Mgt: X Chg: X
Record lvl changes only?	● *NO ○ *YES
Collect Record Reads?	● *NO (Recommended) ○ *YES (Not Recommended)
Collect Open/Close?	● *NO ○ *YES
iFileAudit Member	IF002372 # rcds: 52 , Size: .2 MB
User Profile Selection	● *INCALL ○ *INCLUDE ○ *EXCLUDE
Program Name Selection	● *INCALL ○ *INCLUDE ○ *EXCLUDE
Job Name Selection	● *INCALL ○ *INCLUDE ○ *EXCLUDE

From this page, you can change the file description reported by iFileAudit, make changes to the journal settings and manipulate the settings for "Record lvl changes only" and the "User Profile Selection". After making any of these changes, use the Update button at the bottom of the page to post changes.

You can also work with iFileAudit information for this file using the buttons provided at the top of the screen. The specific buttons displayed will depend on the type of file and the way it is registered. The following buttons may be displayed and will do the functions indicated:

Back To List — Takes you back to the file list with the current file shown at the top of the list.

Analyze Now — Will run the iFileAudit file analysis process for this file now.

Show Anal. Will display the current iFileAudit analysis information for this file.

Delete Rcd Will remove this file from the iFileAudit file registration. This can only be done if the file has been changed to inactive status first.

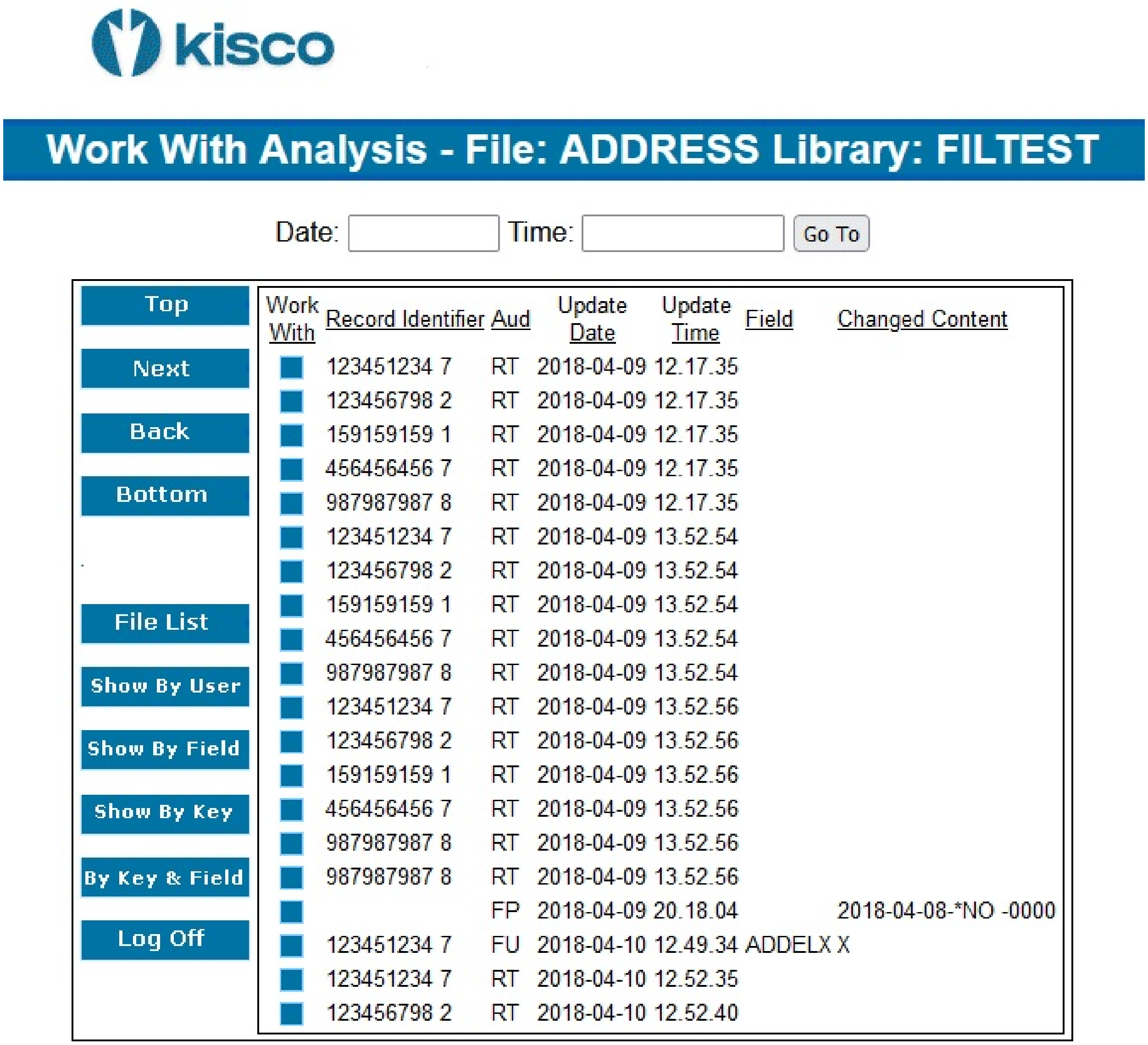
Field Maint Displays a list of fields for the registered file and lets you specify which fields to be included and excluded in the iFileAudit analysis process.

User Maint Displays a list of user profiles associated with the registered file. This only works for files that are set to either *INCLUDE or *EXCLUDE for the user profile selection.

Log Off Ends your browser session with iFileAudit.

Show Analysis

When you select the Show Analysis button when working with a registered file, the following analysis page will be displayed:

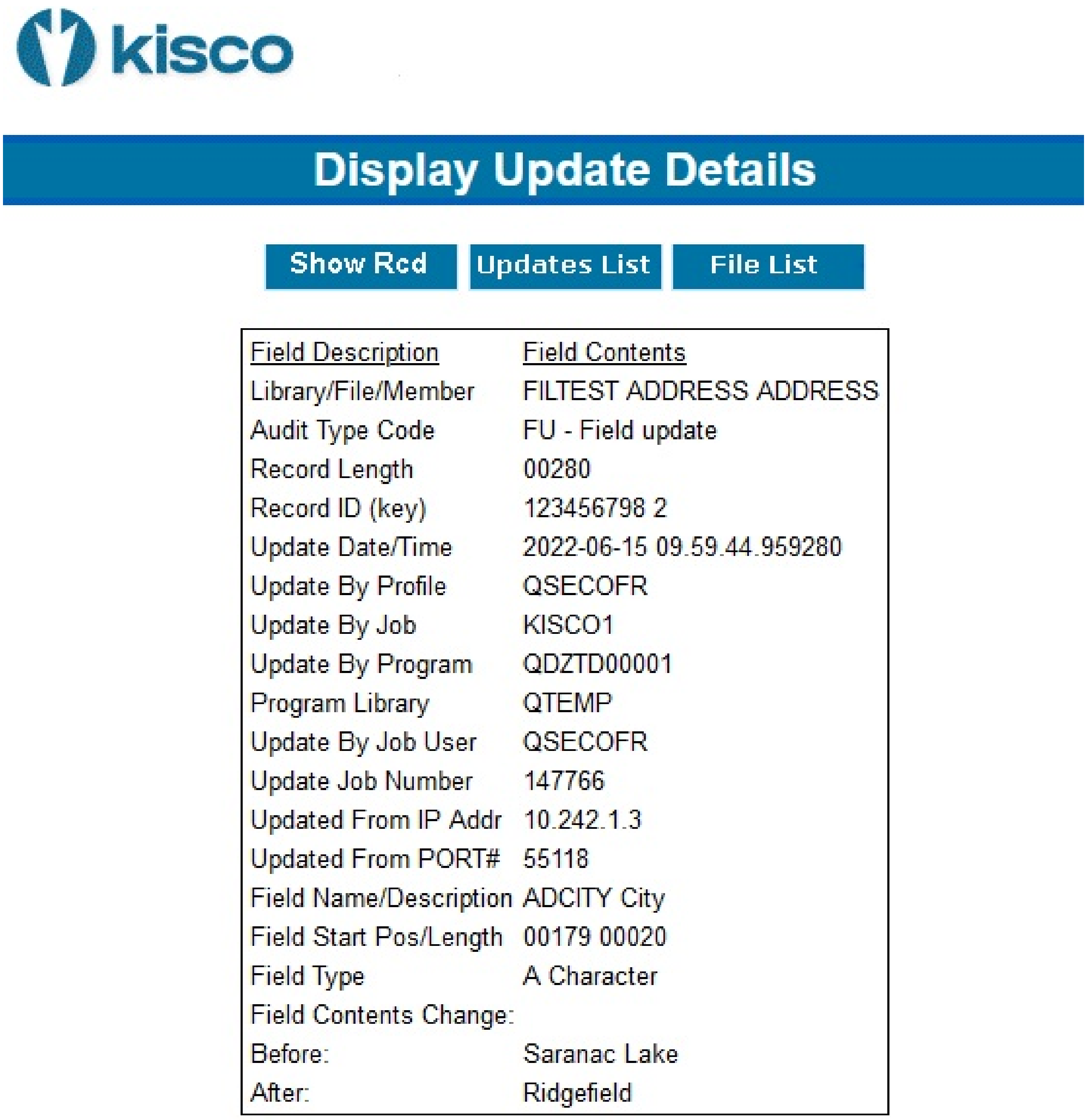


Work With Analysis - File: ADDRESS Library: FILTEST

Work With	Record Identifier	Aud	Update Date	Update Time	Field	Changed Content
■	123451234 7	RT	2018-04-09	12.17.35		
■	123456798 2	RT	2018-04-09	12.17.35		
■	159159159 1	RT	2018-04-09	12.17.35		
■	456456456 7	RT	2018-04-09	12.17.35		
■	987987987 8	RT	2018-04-09	12.17.35		
■	123451234 7	RT	2018-04-09	13.52.54		
■	123456798 2	RT	2018-04-09	13.52.54		
■	159159159 1	RT	2018-04-09	13.52.54		
■	456456456 7	RT	2018-04-09	13.52.54		
■	987987987 8	RT	2018-04-09	13.52.54		
■	123451234 7	RT	2018-04-09	13.52.56		
■	123456798 2	RT	2018-04-09	13.52.56		
■	159159159 1	RT	2018-04-09	13.52.56		
■	456456456 7	RT	2018-04-09	13.52.56		
■	987987987 8	RT	2018-04-09	13.52.56		
■	987987987 8	RT	2018-04-09	13.52.56		
■		FP	2018-04-09	20.18.04		2018-04-08-*NO -0000
■	123451234 7	FU	2018-04-10	12.49.34	ADDELX	X
■	123451234 7	RT	2018-04-10	12.52.35		
■	123456798 2	RT	2018-04-10	12.52.40		

The buttons on the left margin of the page allow you to move around in the file analysis results list. You can also use the Date and Time fields to move the list to a specific point in time. To view the details for any specific field change being reported, just click on the Work With blue box to the left of the line.

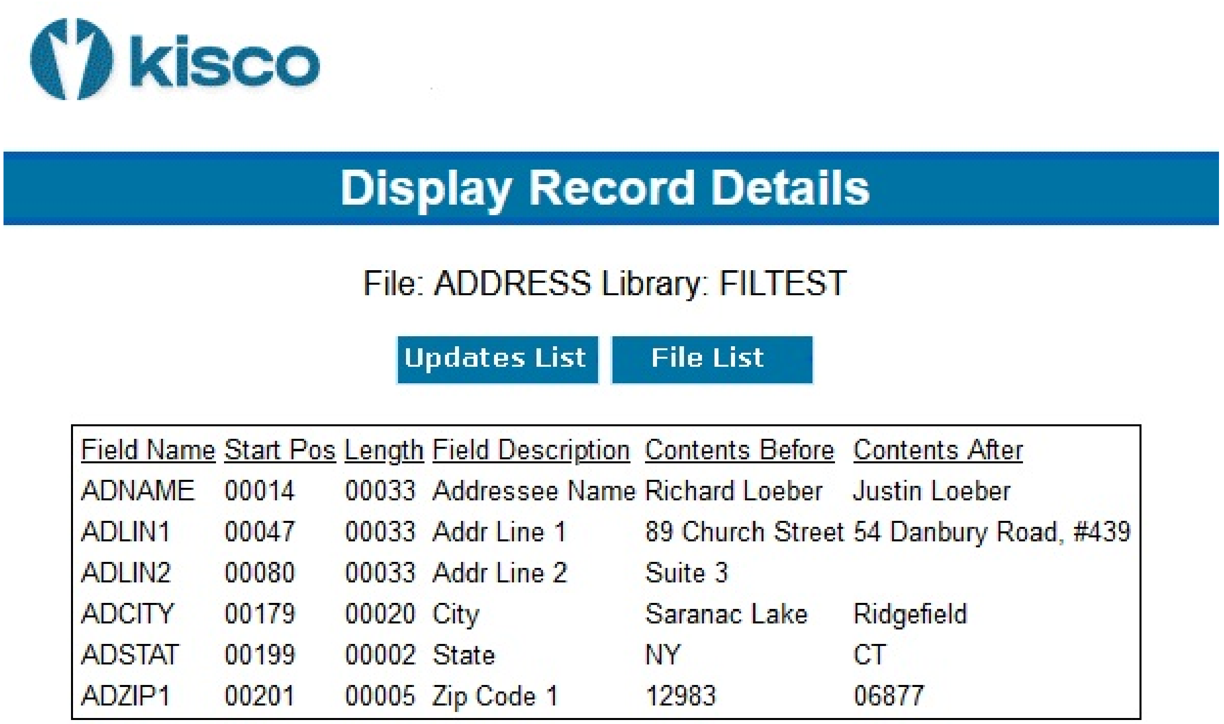
When you select the field update details, the following page will be displayed:



Field Description	Field Contents
Library/File/Member	FILTEST ADDRESS ADDRESS
Audit Type Code	FU - Field update
Record Length	00280
Record ID (key)	123456798 2
Update Date/Time	2022-06-15 09.59.44.959280
Update By Profile	QSECOFR
Update By Job	KISCO1
Update By Program	QDZTD00001
Program Library	QTEMP
Update By Job User	QSECOFR
Update Job Number	147766
Updated From IP Addr	10.242.1.3
Updated From PORT#	55118
Field Name/Description	ADCITY City
Field Start Pos/Length	00179 00020
Field Type	A Character
Field Contents Change:	
Before:	Saranac Lake
After:	Ridgefield

This will show you the details of the specific transaction that was processed and recorded by iFileAudit for the registered file. From here, you can return to the list of file changes that you just came from or you can return to the list of registered files.

From this display, if you want to see all updates that were processed on this record at the same time when this update was processed, use the "Show Rcd" button. When you do, iFileAudit will get all of the related updates together and show them on a panel that looks like the following image:



Display Record Details

File: ADDRESS Library: FILTEST

Field Name	Start Pos	Length	Field Description	Contents Before	Contents After
ADNAME	00014	00033	Addressee Name	Richard Loeber	Justin Loeber
ADLIN1	00047	00033	Addr Line 1	89 Church Street	54 Danbury Road, #439
ADLIN2	00080	00033	Addr Line 2	Suite 3	
ADCITY	00179	00020	City	Saranac Lake	Ridgefield
ADSTAT	00199	00002	State	NY	CT
ADZIP1	00201	00005	Zip Code 1	12983	06877

All the updates shown on this panel were done at the same time as the original update that you selected.

Apache HTTP Server Configuration

For the browser interface for iFileAudit 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 KISCOIFA
Step 3: Edit the configuration file for the new server instance
Step 4: Locate and open the KISCOIFA.txt file supplied by Kisco
Step 5: Cut/Paste the KISCOIFA.txt file contents into the configuration file and apply it
Step 6: Install the server instance files supplied by Kisco
Step 7: Start the new KISCOIFA server instance
Step 8: Finalize object installation setup

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/

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

Step 2: Create a new HTTP server instance named KISCOIFA

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 "KISCOIFA". The server description of "Kisco iFileAudit 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: Edit the configuration file for the new server instance

The above process will leave you with the new KISCOIFA server instance already selected. Scroll down on the left hand list of tasks to the "Tools" section and select the item marked "Edit Configuration File". This will open an edit window with what appears to be a text file displayed by the Web Administration wizard. Leave this open in your browser and move on to the next step.

Step 4: Locate and open the KISCOIFA.txt file supplied by Kisco

In the program materials sent to you from Kisco, you will find a text file named KISCOIFA.txt. Locate this file and open it with NotePad or WordPad on your desktop PC. At this point, you will have the Configuration File for the new server instance open in your browser and the KISCOIFA.txt file open on your desktop.

Step 5: Cut/Paste the KISCOIFA.txt file contents into the configuration file and apply it

Using standard cut and paste methods, copy ALL of the text in the KISCOIFA.txt file over so that it replaces ALL of the text in the Configuration File for the new server instance. When you are done, double check to make sure that all of the Configuration File characters have now been replaced.

Step 6: Install the server instance files supplied by Kisco

Once you have verified that the cut and paste was successful, press the Apply button below the Configuration File in your browser. (You can also close the KISCOIFA.txt file, you will not need it again. Make sure you do not make any changes to this file. If your NotePad or WordPad program asks if you want to save the file, reply “No”.)

Step 7: Start the new KISCOIFA server instance

Start the newly created server instance. You can do this from the Web Administration page or from your command line. If you do this from the command line, issue the following:

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

The server instance will now be active. Go to your browser and enter the following URL:

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

IBM’s standard test page should now be shown. This will indicate that the server is active, but you are not yet ready to use the browser interface features of iFileAudit yet.

Step 8: Finalize object installation setup

At this point, additional objects need to be installed in the IFS plus the required service programs used by your installed version of the OS needs to be set up for use by iFileAudit. You can do all this from your command line by running the following command from the command line:

```
CALL PGM(FILAUD/WWWINSTAL)
```

This process will restore objects to the IFS for use by the newly configured server instance. It will then set those objects with the correct access authority and finally, it will set up the server service programs needed by the HTTP server on your system.

At this point, the browser interface for iFileAudit is now 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 FILAUD as a directory entry
- ADD a URL mapping entry to map "/cgibin/" to FILAUD
- Authorize user access to FILAUD
- Permit CGI programs to be run from FILAUD

If you have other HTTP server instances already running, you may want to configure the iFileAudit 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 iFileAudit will appear as follows:

```
http://yoursystemi.com:8080/ifalogon.htm
```

In this example, the HTTP server instance is running on port number 8080. 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.

As a second level of security, we also recommend that you set up a special user profile for use with the browser interface for iFileAudit access. You should use this profile only for the purpose of loggin in to iFileAudit 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, iSeries Access, etc. If you do not have exit point control software in place, we suggest you take a look at our SafeNet/400 software for your system to guard against this threat.

Configuring Apache for HTTPS Secure Use

iFileAudit supports use of the browser 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 KISCOIFA) 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. Enable SSL for the server instance and register the IFILEAUDIT application.
4. Connect to the Digital Certificate Manager application on your browser.
5. Create a new digital certificate in the *SYSTEM certificate store.
6. Validate the newly created certificate.
7. Assign the new certificate to the IFILEAUDIT application.
8. Start the updated KISCOIFA server instance.
9. 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 web server administration 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
```

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. When the logon is complete, the IBM i5/OS Tasks menu should be displayed. On some releases of the IBM i/OS, you may have to select a link to the “i5/OS Tasks” page following a successful logon process.

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

From the i5/OS Tasks menu, select the "IBM Web Administration for i5/OS" link. This will start the Apache web administration tool. Select the "Manage" tab and then, when it is displayed, select the "HTTP Servers" tab. In the "Server:" selection box, locate and select the KISCOIFA server. **If it is not there, then you need to configure it and test it in a non-secure environment before continuing with this procedure.** This is covered earlier in this documentation. When you have selected the KISCOIFA server, verify that it is showing with a status of "Stopped". If it is showing as active, then you will need to stop it now before continuing.

Before continuing, you will need the text file named KISCOIFA_HTTPS.txt that was shipped with your software. If you received your software on CD, you will find this file on the CD. If you got your software by download, this file is available on the download page for iFileAudit at https://www.kisco.com/ifa/ifadload.html. When you have located this file, open it in a text editor.

In your current browser session, scroll down the lefthand panel until you find the link that shows as "Edit Configuration File" under the "Tools" section at the bottom of the panel. Select this link and your current configuration file will be displayed. If you have customized this at all from the configuration file shipped from Kisco Systems, we recommend that you cut and paste the current configuration statements into a separate text file and save it for possible future use. Once this has been done, you should remove all of the current statements in the configuration file. Then, cut and paste the statements from the KISCOIFA_HTTPS.txt file into the configuration file. When this is done, press the "Apply" button at the bottom of the panel.

Step 3 - Enable SSL for the server instance and register the IFILEAUDIT application

Select the "Security" link from the lefthand panel. In the tab labeled "SSL with Certificate Authentication", select the SSL box and choose the "Enabled" setting. Then, in the box immediately next to the "SSL certificate application name:", key in the value "IFILEAUDIT". We recommend that you do this in all capital letters. Press the "Apply" button to record these changes.

Your server instance is now converted to work with HTTPS. Continue with the next steps.

Step 4 - 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.com:2001

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, like some versions of Internet Explorer, will 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 5 - 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 “IFACERT”.
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 6 - 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 IFACERT 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 7 - Assign the new certificate to the IFILEAUDIT application.

In the left hand panel, select the “Assign certificate” link. Select the IFACERT certificate, then press the “Assign to Applications” button. Locate the IFILEAUDIT 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 8 - Start the updated KISCOIFA server instance.

On a terminal session command line, enter the following command:

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

This will start the server instance that has been converted for use with HTTPS security. 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 9 - 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 KISCOIFA 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 4 above about this issue.