

iFileAudit

Web-Enablement

Version 3

As of July 2009



Kisco Information Systems
89 Church Street
Saranac Lake, New York 12983

Phone: (518) 897-5002
FAX: (518) 897-5003
E-mail: Sales@Kisco.com
WWW: <http://www.kisco.com>
Customer Support: <http://www.kisco.com/webreport/support>

© 2006-2009 Kisco Information Systems

Table Of Contents

Introduction	1
Overview	1
Current Limitations	2
Using The Browser Interface	3
Show Analysis	8
Apache HTTP Server Configuration	10
Security Considerations	12

Introduction

This documentation covers the iFileAudit web-enabled interface only. This documentation is intended to provide you with information on how to configure the Apache HTTP server on your System i server to run web-enabled iFileAudit and instructions on using this new browser based interface to the product.

Overview

Web-enabled iFileAudit is a new feature that allows you to administer iFileAudit using a web browser interface. This requires that your System i use the Apache HTTP web server active and configured to support iFileAudit calls. To activate web-enabled iFileAudit, you must install the iFileAudit Release 3 plus any applicable additional PTFs that have been released by Kisco Information Systems.

Most iFileAudit functions that were previously available using the standard System 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 new browser based 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 (like those available in FireFox) will help your use of iFileAudit.

Current Limitations

The current implementation of web-enabled 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 web-enabled 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.

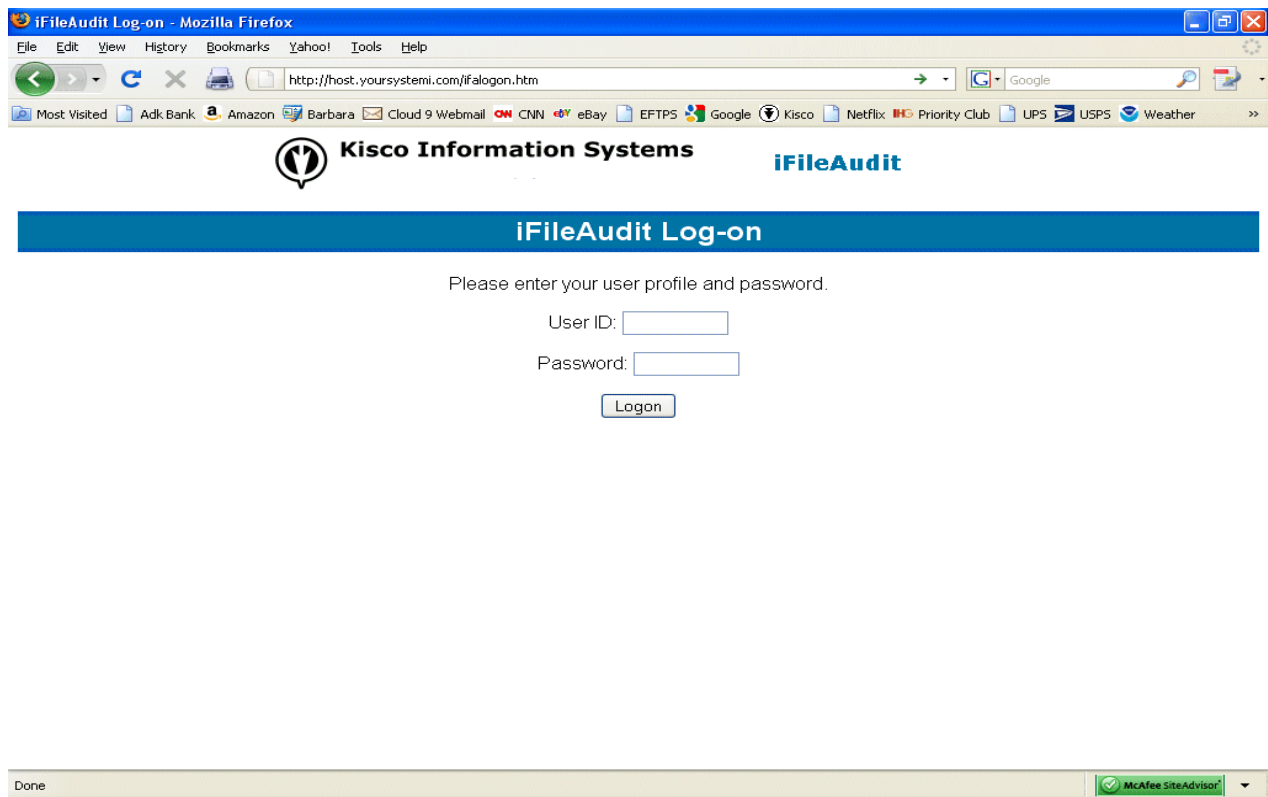
To get started, just type in the following URL on your browser:

`http://yoursystemi.com/ifalagon.htm`

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

Important note: The current version documentation does not include documentation on how to configure the Apache HTTP server for maximum security. When using the current version, it will be important to remember that user profiles and passwords will be passed through your network “in the clear”. You should not implement the iFileAudit web-enabled version unless your network is secure from the Internet. You can see more about this topic in the configuration section of this documentation.

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



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:

Lib: File:

	<u>Sel Library</u>	<u>File</u>	<u>File Description</u>	<u>Status</u>	<u>Journal Name</u>
<input type="button" value="Top"/>	FILDEV	PR.TEST	Test File	*ACTIVE	*DFTL
<input type="button" value="Next"/>	FILDEV	PRODTEST	Test File	*ACTIVE	FILDEV
<input type="button" value="Back"/>	FILDEV	PRODTEST1	Test File	*ACTIVE	FILDEV
<input type="button" value="Bottom"/>	FILDEV	TESTTYPES	File Used for Journal Testing-DO NOT SHIP	*ACTIVE	FILDEV
<input type="button" value="Register File"/>	FILTEST	ADDRESS	Investor Address Master (Distribution System)	*ACTIVE	*IFAL
<input type="button" value="Auto Analysis"/>	PCSECDTA	ALERTS	Safenet/400 Copyright 1997-2008 MP Assoc.,Inc.	*ACTIVE	PCSECDTA
<input type="button" value="Log Off"/>	PCSECDTA	CMDUSR	SafeNet/400 (c)1997-2006. All Rights Reserved	*ACTIVE	PCSECDTA
	PCSECDTA	DESCR	SafeNet/400 (c)1997-2006. All Rights Reserved	*ACTIVE	PCSECDTA
	PCSECDTA	FTPUSR	SafeNet/400 (c)1997-2006. All Rights Reserved	*ACTIVE	PCSECDTA
	PCSECDTA	PCACCESS	SafeNet/400 (c)1997-2006. All Rights Reserved	*ACTIVE	PCSECDTA
	PCSECDTA	PCACCESU	SafeNet/400 (c)1997-2006. All Rights Reserved	*ACTIVE	PCSECDTA
	PCSECDTA	PCACCLNG	SafeNet/400 (c)1997-2006. All Rights Reserved	*ACTIVE	PCSECDTA
	PCSECDTA	TCPIPS	SafeNet/400 (c)1997-2006. All Rights Reserved	*ACTIVE	PCSECDTA
	PCSECDTA	TRAPOD	SafeNet/400 (c)1997-2006. All Rights Reserved	*ACTIVE	*DFTL
	PCSECDTA	WRKREGPF	SafeNet/400 (c)1997-2006. All Rights Reserved	*ACTIVE	PCSECDTA
	QS36F	ADDRESS	Investor Address Master (Distribution System)	*ACTIVE	QS36F
	QS36F	COMPANY	Company Database	*ACTIVE	QS36F
	QS36F	INVESTR	Investor Master (Distribution System)	*ACTIVE	QS36F

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 Information 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 entry 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:

The screenshot shows a web browser window titled "iFileAudit File Registration - Mozilla Firefox". The address bar shows the URL: `http://yoursystemi.com/cgi-bin/dspfilcu?USRPRF=WV8M58G3VZ&SELFIL=*CREATE&SELLIB=*CREATE`. The browser's bookmark bar includes links to Adk Bank, Amazon, Barbara, Cloud 9 Webmail, CMN, eBay, EFTPS, Google, Kisco, Netflix, Priority Club, UPS, USPS, and Weather. The main content area has a blue header "Work With Registered File" and a sub-header "Fill out fields and press Update". Below this is a form with the following fields:

Field Description	Field Contents
Registered Library	<input type="text"/>
Registered File	<input type="text"/>
File Description	<input type="text"/>
Status	<input type="button" value="*INACTIVE"/>
Journal Library	<input type="text" value="*DFTL"/> *DFTL, *IFAL, Library name
Journal Name	<input type="text" value="*DFTN"/> *DFTN, *IFAN, Journal name
File Record Length	<input type="text"/>
Journal Setup	<input type="text"/>
Journal Type	<input type="text"/>
Last Trans Post Date	<input type="text"/>
Last Trans Post Time	<input type="text"/>
File Key Type	<input type="text"/>
Record w/ changes only?	<input checked="" type="radio"/> *NO <input type="radio"/> *YES
iFileAudit Member	<input type="text"/>
File level ID	<input type="text"/>
User Profile Selection	<input checked="" type="radio"/> *INCALL <input type="radio"/> *INCLUDE <input type="radio"/> *EXCLUDE

At the bottom of the form is an "Update" button. The browser's status bar at the bottom shows "Done" and "McAfee SiteAdvisor".

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	QS36F
Registered File	COMPANY
File Description	Company Database
Status	*ACTIVE
Journal Library	QS36F *DFTL, *IFAL, Library name
Journal Name	COMPANY *DFTN, *IFAN, Journal name
File Record Length	00375
Journal Setup	K Kisco
Journal Type	B Full Support
Last Trans Post Date	2009-06-29
Last Trans Post Time	20.00.17.300000
File Key Type	K Keyed File
Record lvl changes only?	<input checked="" type="radio"/> *NO <input type="radio"/> *YES
iFileAudit Member	IF000235
File level ID	0881120113405
User Profile Selection	<input checked="" type="radio"/> *INCALL <input type="radio"/> *INCLUDE <input type="radio"/> *EXCLUDE

Update

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:

The screenshot shows the iFileAudit application interface. At the top, the browser title is "iFileAudit Work With Analysis - Mozilla Firefox". The address bar shows the URL: http://yoursystemi.com/cgi-bin/dspfilcz?USRPRF=VV8M58G3VZ&SELFIL=*DSPF&SELLIB=*DSPF. The page header includes the Kisco Information Systems logo and the iFileAudit logo. Below the header is a blue banner with the text "Work With Analysis - File: WRKREGPF Library: PCSECDTA".

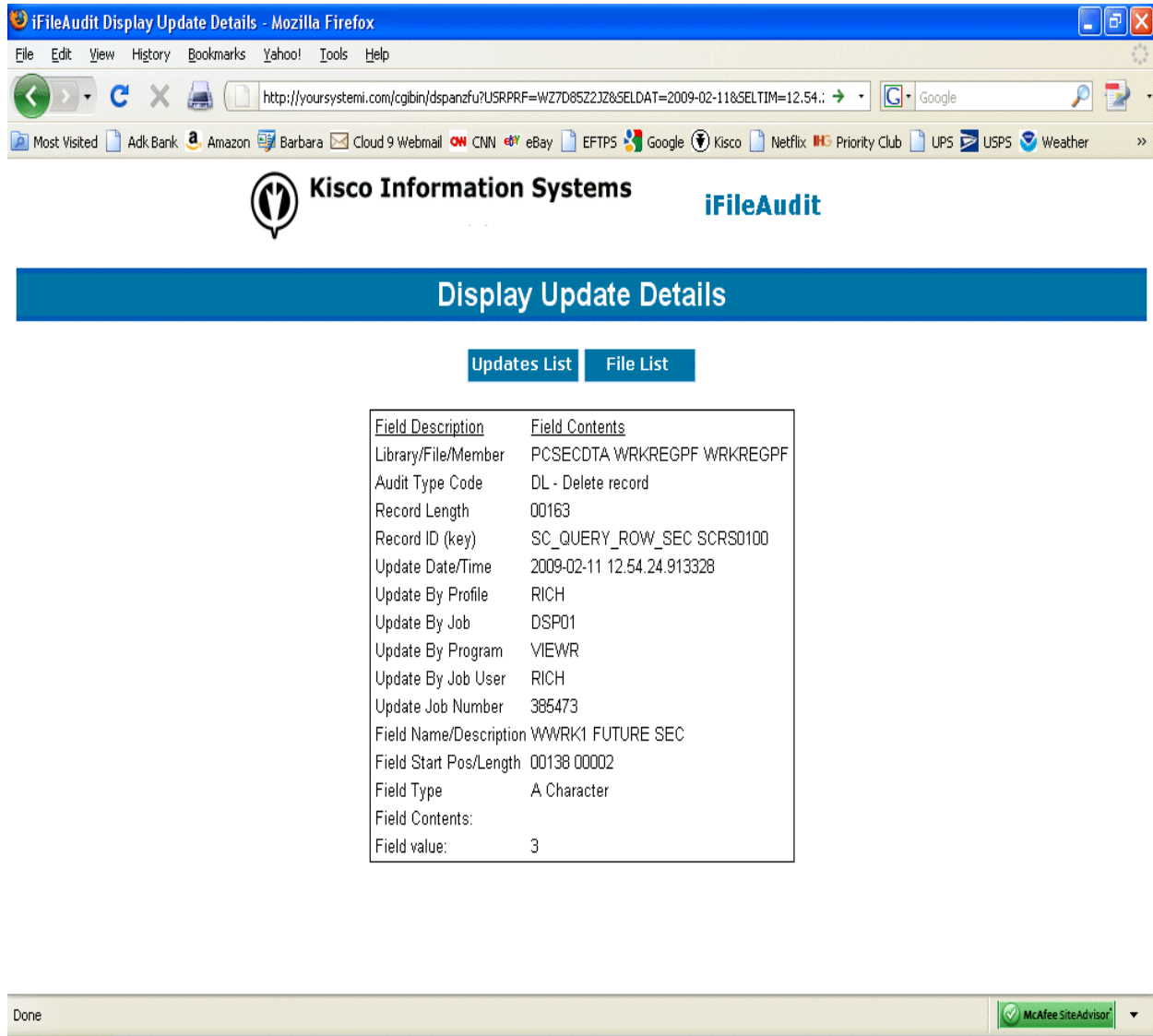
Below the banner is a filter section with "Date: [] Time: [] Go To" buttons. The main content is a table with the following columns: "Work With", "Record Identifier", "Aud", "Update Date", "Update Time", "Field", and "Changed Content". The table contains 20 rows of data, each starting with a blue square icon in the "Work With" column.

Work With	Record Identifier	Aud	Update Date	Update Time	Field	Changed Content
■	SC_QUERY_ROW_SEC SCRS	DL	2009-02-11	12.54.24		
■	SC_QUERY_ROW_SEC SCRS	DL	2009-02-11	12.54.24	WEXITP	SC_QUERY_ROW_SEC
■	SC_QUERY_ROW_SEC SCRS	DL	2009-02-11	12.54.24	WFORMT	SCRS0100
■	SC_QUERY_ROW_SEC SCRS	DL	2009-02-11	12.54.24	WSTATS	1
■	SC_QUERY_ROW_SEC SCRS	DL	2009-02-11	12.54.24	WMSGTX	ShowCase row securit
■	SC_QUERY_ROW_SEC SCRS	DL	2009-02-11	12.54.24	WEXPGN	PCCL01C
■	SC_QUERY_ROW_SEC SCRS	DL	2009-02-11	12.54.24	WEXPGL	PCSECLIB
■	SC_QUERY_ROW_SEC SCRS	DL	2009-02-11	12.54.24	WSRVID	*SHOWCASE
■	SC_QUERY_ROW_SEC SCRS	DL	2009-02-11	12.54.24	WLOGLV	A
■	SC_QUERY_ROW_SEC SCRS	DL	2009-02-11	12.54.24	WWRK1	3
■	SC_QUERY_ROW_SEC SCRS	DL	2009-02-11	12.54.24	WSTOD	N
■	QIBM_QSY_DLT_PROFILEDLTP	FU	2009-02-11	12.56.12	WEXPGN	
■	QIBM_QSY_DLT_PROFILEDLTP	FU	2009-02-11	12.56.12	WEXPGL	
■	QIBM_QTMX_SVR_LOGON TCPL	FU	2009-02-11	12.56.12	WEXPGN	PCCL04D
■	QIBM_QSY_DLT_PROFILEDLTP	FU	2009-02-11	12.56.13	WEXPGN	PCCL01A
■	QIBM_QSY_DLT_PROFILEDLTP	FU	2009-02-11	12.56.13	WEXPGL	PCSECLIB
■	*DDM *DDM	FA	2009-02-11	12.57.26	WEXITP	*DDM
■	*DDM *DDM	FA	2009-02-11	12.57.26	WFORMT	*DDM
■	*DDM *DDM	FA	2009-02-11	12.57.26	WSTATS	4

The bottom of the page shows a "Done" status bar and a "McAfee SiteAdvisor" icon.

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:



The screenshot shows a Mozilla Firefox browser window displaying the 'iFileAudit Display Update Details' page. The browser's address bar shows the URL: `http://yoursystemi.com/cgi-bin/dspanzfu?USRPRF=WZ7D85Z2JZ&SELDAT=2009-02-11&SELTIM=12.54.:`. The page features the Kisco Information Systems logo and the iFileAudit branding. Below the branding is a blue header with the text 'Display Update Details'. Underneath the header are two tabs: 'Updates List' (selected) and 'File List'. The main content area displays a table of field update details.

Field Description	Field Contents
Library/File/Member	PCSECDTA WRKREGPF WRKREGPF
Audit Type Code	DL - Delete record
Record Length	00163
Record ID (key)	SC_QUERY_ROW_SEC SCRS0100
Update Date/Time	2009-02-11 12.54.24.913328
Update By Profile	RICH
Update By Job	DSP01
Update By Program	VIEWR
Update By Job User	RICH
Update Job Number	385473
Field Name/Description	WWRK1 FUTURE SEC
Field Start Pos/Length	00138 00002
Field Type	A Character
Field Contents:	
Field value:	3

At the bottom of the browser window, the status bar shows 'Done' and a McAfee SiteAdvisor icon.

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.

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 System 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 System 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 System 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 System 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 web-enabled 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, web-enabled 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 web-enabled 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

The current version of web-enabled iFileAudit does not include configuration support for the Apache server in secure mode. The 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 web-enabled iFileAudit access. You should use this profile only for the purpose of logging 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.