

# **iFileAudit**

## **Bluescape Browser Interface**

**Version 8**

**As of September 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 .....                            | <a href="#">1</a>  |
| Overview .....                                | <a href="#">1</a>  |
| Using The Bluescape Interface .....           | <a href="#">2</a>  |
| Browser Navigation .....                      | <a href="#">3</a>  |
| Initial Display Panel .....                   | <a href="#">4</a>  |
| File Registration Exceptions .....            | <a href="#">5</a>  |
| File Registration .....                       | <a href="#">6</a>  |
| Optional Links .....                          | <a href="#">8</a>  |
| Show Analysis .....                           | <a href="#">9</a>  |
| Field Selection .....                         | <a href="#">13</a> |
| Reports .....                                 | <a href="#">14</a> |
| Export .....                                  | <a href="#">15</a> |
| Purge .....                                   | <a href="#">16</a> |
| Auto Analysis .....                           | <a href="#">17</a> |
| Settings .....                                | <a href="#">18</a> |
| Apache HTTP Server Configuration .....        | <a href="#">22</a> |
| Security Considerations .....                 | <a href="#">24</a> |
| Configuring Apache for HTTPS Secure Use ..... | <a href="#">25</a> |

## Introduction

This documentation covers the Bluescape 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 browser based interface to the product.

## Overview

The Bluescape 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.

The Bluescape 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.

## Using The Bluescape 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:8080/ifalogon.htm>

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

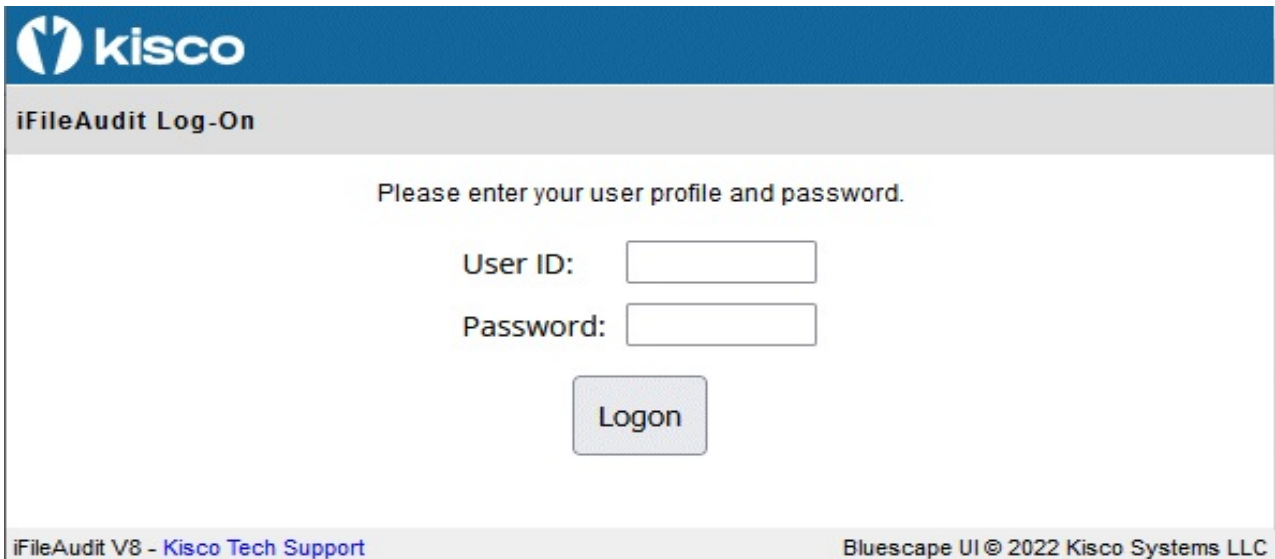
If your system is configured for password level 2 or 3 (check system value QPWDLVL), then you should use the following URL in your browser:

<http://yoursystemi.com:8080/ifalogon2.htm>

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:



**kisco**

**iFileAudit Log-On**

Please enter your user profile and password.

User ID:

Password:

Logon

iFileAudit V8 - Kisco Tech Support Bluescape UI © 2022 Kisco Systems LLC

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

## 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 iFileAudit. 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.

## Initial Display Panel

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

| <u>Sel</u> | <u>Library</u> | <u>File</u> | <u>File Description</u>                        | <u>Status</u>  | <u>Journal Name</u> |
|------------|----------------|-------------|--|----------------|---------------------|
| ■          | FILAUD         | FILAUDA     | iFileAudit (c) 2006-2021 Kisco Info. Systems   | <u>*ACTIVE</u> | <u>*IFAN</u>        |
| ■          | FILDEV         | PR.TESTP    | For Packed Number Testing                      | <u>*ACTIVE</u> | <u>*DFTN</u>        |
| ■          | FILDEV         | PRODFLAT    | Test File                                      | <u>*ACTIVE</u> | <u>*DFTN</u>        |
| ■          | FILDEV         | PRODTEST    | Test File                                      | <u>*ACTIVE</u> | <u>*DFTN</u>        |
| ■          | FILDEV         | PTFDETL     | Output file for DSPOBJD                        | <u>*ACTIVE</u> | <u>PTFDETL</u>      |
| ■          | FILDEV         | READTRACE   | List of objects with no authorization list ref | <u>*ACTIVE</u> | <u>*DFTN</u>        |
| ■          | FILDEV         | TESTFILE    | File Used for Journal Testing-DO NOT SHIP      | <u>*ACTIVE</u> | <u>*DFTN</u>        |

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.

The number of detail lines that you see on this screen can be controlled from a value in the settings. Please see that section of the manual. As shipped from Kisco, this is set to 20 lines per panel.

To navigate this panel, you can enter a specific library and file and use the search button. The list will then be repositioned at the start of that section. If you leave the file name blank, the list will start with all files in the library entered. You can use the blue arrow buttons to scroll through your list of files. The << button will always bring you back to the top and the >> button will always take you to the end. The < and > buttons will scroll one set back or forward as needed.

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

From this display, you can change the status of a file registration from active to inactive or back to active from inactive. To do so, just click on the \*ACTIVE or \*INACTIVE link and the status will be changed. You can also check to see the status of the current journal in use for the file tracking by clicking on the Journal Name associated with the file. This will generate a journal status report that will then be displayed in your browser session in a new tab.

To view the file registration details, click on the blue button to the left of the file. A detailed registration panel will be displayed. This is documented along with registration for a new file in a separate section of this documentation.

### File Registration Exceptions

If there are any problems with the registration of a file, the status column will show in a color other than black. These can be interpreted as follows:

- |        |  |
|--------|--|
| Yellow | indicates that the file journaling is not currently active. This is normal when the status shows as *INACTIVE. If an *ACTIVE status shows in yellow, click on it and it should correct itself by reactivating the journal. |
| Red    | indicates that there is a problem with the journal associated with this file. Check with Kisco tech support for assistance if you see this condition.  |
| Pink   | indicates that the file has an active journal but it is a different journal than the one specified with the file was registered with iFileAudit. iFileAudit will not work correctly until this situation is corrected.     |

## File Registration

When you use the REGISTER FILE button or when you click the blue button next to a file that is already registered, the following panel will be displayed:




| <u>Field Description</u> | <u>Field Contents</u>   |
|--------------------------|---|
| Registered Library       | <input type="text"/>  |
| Registered File          | <input type="text"/>  |
| File Description         | <input type="text"/>  |
| Status                   | <input type="text" value="*INACTIVE"/>  |
| Journal Library          | <input type="text" value="*IFAL"/> *IFAL, *DFTL, Library name   |
| Journal Name             | <input type="text" value="*IFAN"/> *IFAN, *DFTN, Journal name   |
| Include Activity Type    | Add: <input type="checkbox"/> X Del: <input type="checkbox"/> X Mgt: <input type="checkbox"/> X Chg: <input type="checkbox"/> X |
| Record lvl changes only? | <input checked="" type="radio"/> *NO <input type="radio"/> *YES   |
| Collect Record Reads?    | <input checked="" type="radio"/> *NO (Recommended) <input type="radio"/> *YES   |
| Collect Open/Close?      | <input checked="" type="radio"/> *NO <input type="radio"/> *YES   |
| User Profile Selection   | <input checked="" type="radio"/> *INCALL <input type="radio"/> *INCLUDE <input type="radio"/> *EXCLUDE                          |
| Program Name Selection   | <input checked="" type="radio"/> *INCALL <input type="radio"/> *INCLUDE <input type="radio"/> *EXCLUDE                          |
| Job Name Selection       | <input checked="" type="radio"/> *INCALL <input type="radio"/> *INCLUDE <input type="radio"/> *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.

If you decide that you don't want to register a new file once you get to this point, use the dark gray GO BACK button at the top to return to the list of files already registered.



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

|       |   |
|--|---|
| WORK WITH REGISTERED FILE <input type="button" value="ANALYZE"/> <input type="button" value="SHOW"/> <input type="button" value="REMOVE"/> <input type="button" value="FIELDS"/> <input type="button" value="PURGE"/> <input type="button" value="GO BACK"/> |   |
| Field Description  | Field Contents  |
| Registered Library   | <input type="text" value="FILDEV"/> - Level: <input type="text" value="1040609082047"/>   |
| Registered File  | <input type="text" value="TESTFILE"/>   |
| File Description   | <input type="text" value="File Used for Journal Testing-DO NOT SHIP"/>  |
| Status   | <input type="text" value="*ACTIVE"/>  |
| Journal Library  | <input type="text" value="*DFTL"/> *IFAL, *DFTL, Library name   |
| Journal Name   | <input type="text" value="*DFTN"/> *IFAN, *DFTN, Journal name   |
| File Record Length   | <input type="text" value="00247"/>  |
| Journal Setup  | <input type="text" value="K"/> Kisco  |
| Journal Type   | <input type="text" value="B"/> Full Support   |
| Last Trans Post Date:  | <input type="text" value="2022-09-26"/> Time: <input type="text" value="20.00.14.080000"/>  |
| File Key Type  | <input type="text" value="K"/> Keyed File   |
| Include Activity Type  | Add: <input type="text" value="X"/> Del: <input type="text" value="X"/> Mgt: <input type="text" value="X"/> Chg: <input type="text" value="X"/> |
| Record lvl changes only?   | <input checked="" type="radio"/> *NO <input type="radio"/> *YES   |
| Collect Record Reads?  | <input checked="" type="radio"/> *NO (Recommended) <input type="radio"/> *YES   |
| Collect Open/Close?  | <input checked="" type="radio"/> *NO <input type="radio"/> *YES   |
| iFileAudit Member  | <input type="text" value="IF002375"/> # rclds: 9 , Size: .2 MB  |
| User Profile Selection   | <input checked="" type="radio"/> *INCALL <input type="radio"/> *INCLUDE <input type="radio"/> *EXCLUDE  |
| Program Name Selection   | <input checked="" type="radio"/> *INCALL <input type="radio"/> *INCLUDE <input type="radio"/> *EXCLUDE  |
| Job Name Selection   | <input checked="" type="radio"/> *INCALL <input type="radio"/> *INCLUDE <input type="radio"/> *EXCLUDE  |
| <input type="button" value="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 dark gray buttons may be displayed and will do the functions indicated:

**ANALYZE** Will run the iFileAudit file analysis process for this file now to bring the tracking information up to date.

|         |   |
|---------|---|
| SHOW    | Will display the current iFileAudit analysis information for this file.   |
| REMOVE  | Will remove this file from the iFileAudit file registration. This can only be done if the file has been changed to inactive status first.           |
| FIELDS  | 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. |
| PURGE   | Lets you purge transaction history for the registered file.   |
| GO BACK | Takes you back to the file list with the current file shown at the top of the list.   |

### Optional Links

There are some optional links that may also appear on this panel depending on how the file is registered.

If the file does not have a built in key structure, a link will be displayed to the right of the “File Key Type” section that will read MAINTAIN KEYS. This will display a list of the fields in the registered file and allow you to manually build a key structure so that record identification in iFileAudit will be easier to accomplish. To build a key, click on the ADD link next to the field you want to use. To build a key using multiple fields, add them in order of priority. The actual structure of the key will be shown at the top of the panel. If you want to change the key structure, use the CLEAR KEY link at the top of the panel.

If the file is registered to be able to select tracking based on the user profile doing an update, then an option link will be shown next to the “User Profile Selection” section that will read MAINTAIN USERS. You can either include users or exclude users. Once that is set you will need to enter a list of the user profiles that you want to use. Selecting the link will bring up the list set up for this registered file.

If the file is registered to be able to select tracking based on the program name doing an update, then an option link will be shown next to the “Program Name Selection” section that will read MAINTAIN PROGRAM NAMES. You can either include updates made by specific programs or exclude them. Once that is set you will need to enter a list of the program names that you want to use. Selecting the link will bring up the list set up for this registered file.

If the file is registered to be able to select tracking based on the name of the job doing an update, then an option link will be shown next to the “Job Name Selection” section that will read MAINTAIN JOB NAMES. You can either include updates made by specific jobs or exclude them. Once that is set you will need to enter a list of the job names that you want to use. Selecting the link will bring up the list set up for this registered file.

## Show Analysis

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

| Work With | Record Identifier | Aud                     | Update Date | Update Time | Field    | Before | After                  |
|-----------|-------------------|-------------------------|-------------|-------------|----------|--------|------------------------|
| ■         | 123451234 9       | FU-Field update         | 2022-08-02  | 11.48.07    | ADTYPE 7 | 7      | 9                      |
| ■         | 456456456 9       | FU-Field update         | 2022-08-02  | 11.48.07    | ADTYPE 7 | 7      | 9                      |
| ■         | 123451234 7       | FU-Field update         | 2022-08-02  | 11.50.45    | ADTYPE 9 | 9      | 7                      |
| ■         | 456456456 7       | FU-Field update         | 2022-08-02  | 11.50.45    | ADTYPE 9 | 9      | 7                      |
| ■         |                   | FP-iFileAudit Purge Run | 2022-08-02  | 20.22.08    |          |        | 2021-01-01-*NO-0000052 |
| ■         | 123451234 9       | FU-Field update         | 2022-08-05  | 12.51.40    | ADTYPE 7 | 7      | 9                      |
| ■         | 456456456 9       | FU-Field update         | 2022-08-05  | 12.51.40    | ADTYPE 7 | 7      | 9                      |

The blue buttons on the right above the record content display allow you to move around in the history trace. The << button will always take you to the oldest record. The >> button will always take you to the most recent records. The < and > buttons will roll the display contents back and forth by the browser roll factor that you have set (see the Settings section in this documentation). If you want to go to a specific date and time, you can enter those values in the boxes provided and use the Go To button. When entering a date, the format is yyyy-mm-dd and it includes the dashes. The time field is in the format hh.mm.ss and it includes the dot character.

The drop down “View by” box will let you view the field history in different sequences as follows:

DATE

The history will be shown in chronological sequence starting with the oldest transaction on file.




|             |  |
|-------------|--|
| USER        | The history will be shown in User Profile, Date and Time sequence. You can zero in on a specific user profile and specific dates and times when field changes were made. |
| FIELD       | The history will be shown in field name, date and time sequence. You can use this to zero in on a specific field to view history.  |
| KEY         | This history will be shown by record key, date and time sequence. This will let you zero in on a specific record for a file to see a picture of how fields have changed. |
| KEY & FIELD | The history will be shown by record key, field, date and time sequence which will further let you zero in on specific file updates.                                      |

The three dark grey buttons provide the following functions:

|         |  |
|---------|--|
| REPORT  | Will let you generate a listing with record selection parameters. The listing can be displayed or routed to a printer device on your system. See the separate documentation section on “Reports” for more details. |
| EXPORT  | Will let you export transaction history to a file for your own analysis purposes. See the separate documentation section on “Exports” for more details.  |
| GO BACK | Will return you to the list of registered files.   |

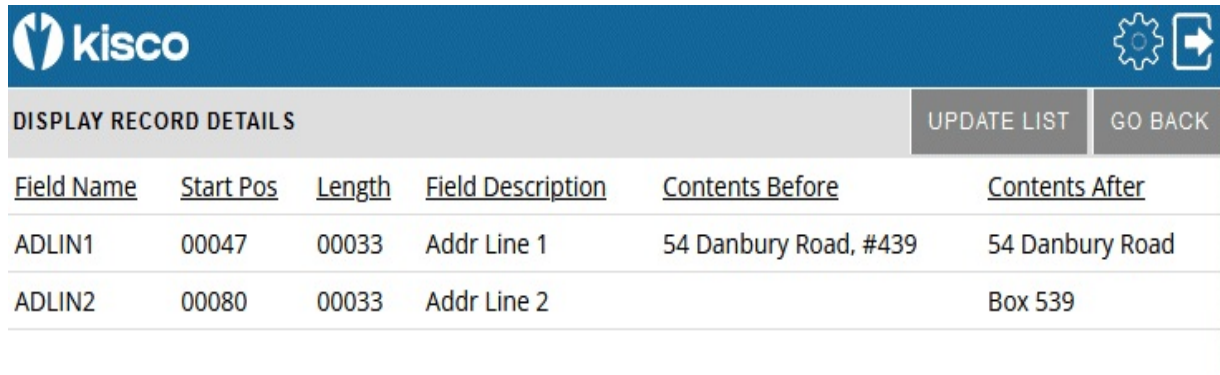
This detail on this display shows the basic information about each field update that has been captured for the registered file. For more details on a specific update, select the blue button to the left of the record.

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

|    |                            |
|---|----------------------------|
| DISPLAY UPDATE DETAILS      SHOW RECORD      UPDATE LIST      GO BACK   |                            |
| <u>Field Description</u>  | <u>Field Contents</u>      |
| Library/File/Member   | FILTEST ADDRESS ADDRESS    |
| Audit Type Code   | FU - Field update          |
| Record Length   | 00280                      |
| Record ID (key)   | 123451234 9                |
| Update Date/Time  | 2022-08-02 11.48.07.073056 |
| Update By Profile   | QSECOFR                    |
| Update By Job   | KISCO1                     |
| Update By Program   | QCMD                       |
| Program Library   | QSYS                       |
| Update By Job User  | QSECOFR                    |
| Update Job Number   | 163847                     |
| Updated From IP Addr  | 10.242.1.2                 |
| Updated From PORT#  | 58737                      |
| Field Name/Description  | ADTYPE Address Type        |
| Field Start Pos/Length  | 00013 00001                |
| Field Type  | A Character                |
| Field Contents Change:  |                            |
| Before:   | 7                          |
| After:  | 9                          |

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 by using the UPDATE LIST button or you can return to the list of registered files by using the GO BACK button.

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 RECORD** 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:



| <u>Field Name</u> | <u>Start Pos</u> | <u>Length</u> | <u>Field Description</u> | <u>Contents Before</u> | <u>Contents After</u> |
|-------------------|------------------|---------------|--------------------------|------------------------|-----------------------|
| ADLIN1            | 00047            | 00033         | Addr Line 1              | 54 Danbury Road, #439  | 54 Danbury Road       |
| ADLIN2            | 00080            | 00033         | Addr Line 2              |                        | Box 539               |

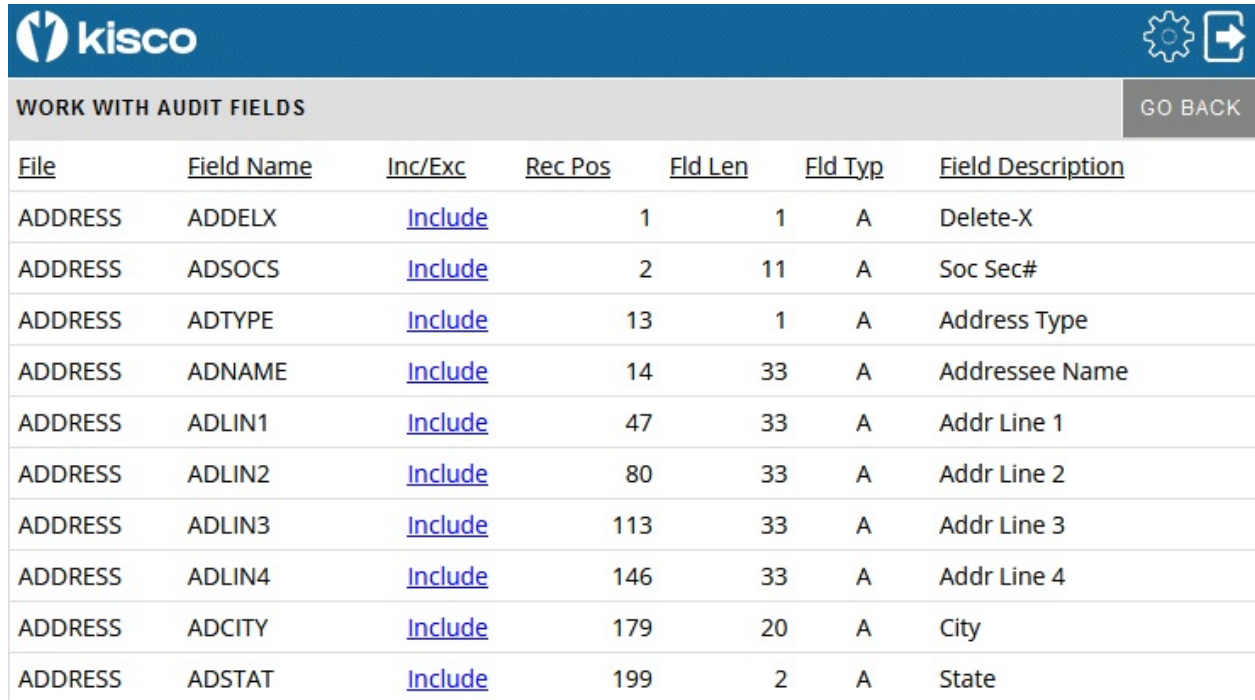
All the updates shown on this panel were done at the same time as the original update that you selected. This will help you to see all of the updates that were applied at the same time.

From here, you can return to the list of updates for this file by using the **UPDATE LIST** button or you can return the list of registered files by using the **GO BACK** button.



## Field Selection

iFileAudit allows you to control which fields you want to track in each registered file. From the detail display of the file registration, you can use the FIELDS button at the top of the page to bring up the following display:



| File    | Field Name | Inc/Exc                 | Rec Pos | Fld Len | Fld Typ | Field Description |
|---------|------------|-------------------------|---------|---------|---------|-------------------|
| ADDRESS | ADDELX     | <a href="#">Include</a> | 1       | 1       | A       | Delete-X          |
| ADDRESS | ADSOCS     | <a href="#">Include</a> | 2       | 11      | A       | Soc Sec#          |
| ADDRESS | ADTYPE     | <a href="#">Include</a> | 13      | 1       | A       | Address Type      |
| ADDRESS | ADNAME     | <a href="#">Include</a> | 14      | 33      | A       | Addressee Name    |
| ADDRESS | ADLIN1     | <a href="#">Include</a> | 47      | 33      | A       | Addr Line 1       |
| ADDRESS | ADLIN2     | <a href="#">Include</a> | 80      | 33      | A       | Addr Line 2       |
| ADDRESS | ADLIN3     | <a href="#">Include</a> | 113     | 33      | A       | Addr Line 3       |
| ADDRESS | ADLIN4     | <a href="#">Include</a> | 146     | 33      | A       | Addr Line 4       |
| ADDRESS | ADCITY     | <a href="#">Include</a> | 179     | 20      | A       | City              |
| ADDRESS | ADSTAT     | <a href="#">Include</a> | 199     | 2       | A       | State             |

The default is that every field in the file is included. To exclude a field, click on the [Include](#) button and it will change to show that the field is now excluded. To change it back to be included, click on the same link again. When a field shows as excluded, any updates to that field will be excluded from consideration by iFileAudit when the file analysis process is run.

Keep in mind that when a field is excluded and an Analysis run has been completed; if you change it back to include the field, past history for the field will not be recovered.

## Reports

When you select the REPORT dark grey button from a file analysis panel, the following selection display will be shown:

| <u>Options</u>       | <u>Selections</u>   |
|----------------------|---|
| User Profile(s):     | <input type="text" value="*ALL"/> Profile, GENERIC*                                 |
| Field Name:          | <input type="text" value="*ALL"/> *ALL, Field Name                                  |
| Start Date:          | <input type="text" value="*START"/> *CURRENT, *START, *YESTERDAY, *WEEK, YYYY-MM-DD |
| Start Time:          | <input type="text" value="*AVAIL"/> *AVAIL, HH.MM.SS                                |
| End Date:            | <input type="text" value="*CURRENT"/> *CURRENT, *YESTERDAY, YYYY-MM-DD              |
| End Time:            | <input type="text" value="*AVAIL"/> *AVAIL, HH.MM.SS                                |
| Record Key:          | <input type="text" value="*ALL"/> *ALL,<br>Record Key                               |
| Printer Device:      | <input type="text" value="PRT01"/> Device Name, * (Show Report Here)                |
| Output Queue/Library | <input type="text" value="*DEV"/> <input type="text" value="*LIBL"/> *DEV, *DFT     |

The file being reported on will be shown at the top of the panel. You can use the selection fields to customize what you want to be included in your report by specifying the selection fields. If you leave the Printer Device or Output Queue is set to \*DFT, the printer or output queue used will be the printer specified in the Settings. See that section of this documentation. If the Output Queue is set to \*DEV, the output queue for the specified printer will be used. When shipped from Kisco, the value PRT01 is preset for the device and the output queue is set to \*DEV. These can be changed on the Settings panel.



## Export

When you select the EXPORT dark gray button from the file analysis panel, the following selection panel will be displayed:

| Options                 | Selections  |
|-------------------------|---|
| Export To File Name:    | <input type="text" value="TEST"/> File name   |
| Library Name:           | <input type="text" value="FILEAUDTA"/> Library name   |
| Replace or add records: | <input checked="" type="radio"/> *ADD <input type="radio"/> *REPLACE                                  |
| Create file?:           | <input checked="" type="radio"/> *YES <input type="radio"/> *NO                                       |
| Start Date:             | <input type="text" value="*START"/> *CURRENT, *START, *YESTERDAY, *WEEK, YYYY-MM-DD                   |
| Start Time:             | <input type="text" value="*AVAIL"/> *AVAIL, HH.MM.SS  |
| End Date:               | <input type="text" value="*CURRENT"/> *CURRENT, *YESTERDAY, YYYY-MM-DD                                |
| End Time:               | <input type="text" value="*AVAIL"/> *AVAIL, HH.MM.SS  |
| Export format:          | <input checked="" type="radio"/> *SHORT <input type="radio"/> *LONG                                   |
| Export source:          | <input checked="" type="radio"/> *CUR (Current history) <input type="radio"/> *ARC (Archived history) |

The file being processed is shown at the top of the panel. This option will let you extract and export transaction details from iFileAudit so that you can perform your own analysis. The library name that you use must be an existing library, but you can assign any file name that you want. Fill in the selection criteria that you want to use before pressing the Run Export button. Specific date selections must be entered in yyyy-mm-dd format including the dash characters. Specific time selections must be entered in hh.mm.ss format including the dot characters. Partial date and time values are allowed. The \*LONG option on the Export format setting should be used if any individual fields in the file are longer than 32 characters.

## Purge

When you select the dark gray PURGE button on either the initial display panel or from the file registration panel, the following will be shown:

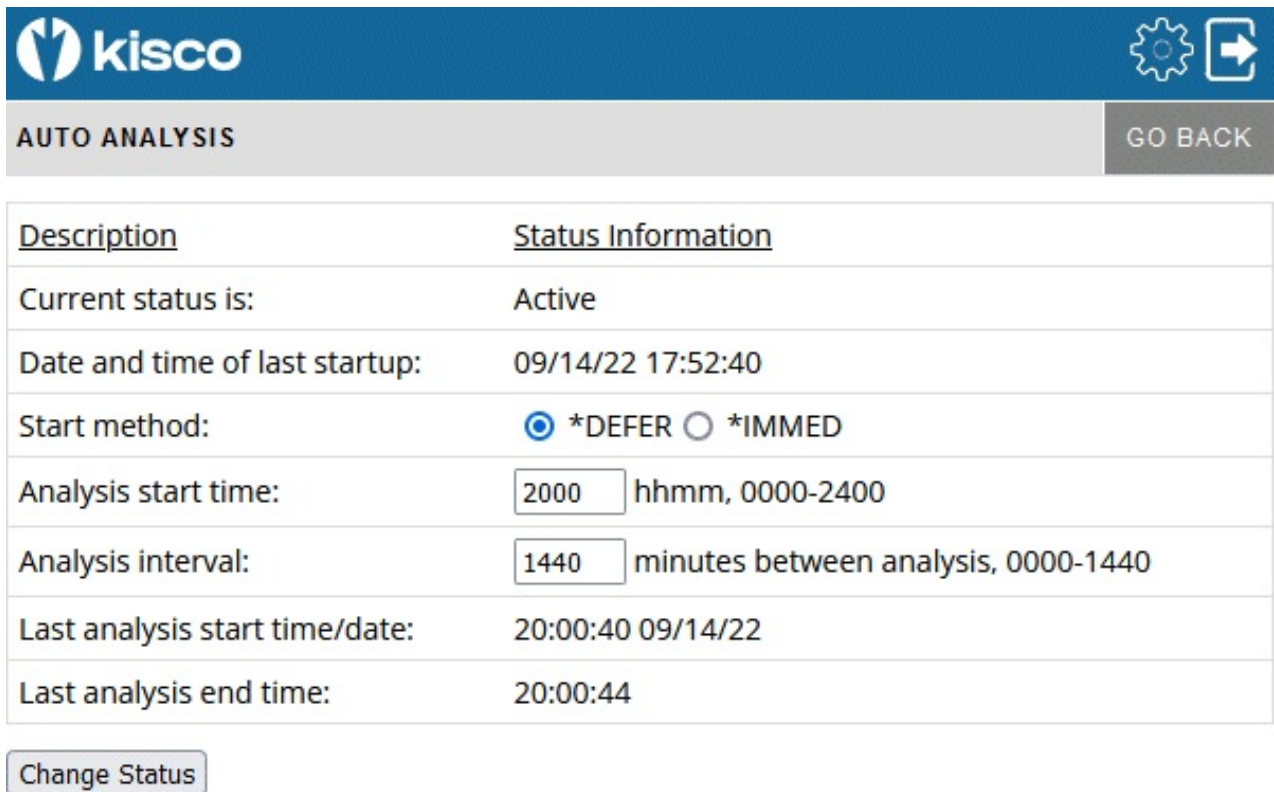
| <u>Description</u>        | <u>Status Information</u>                                       |
|---------------------------|---|
| File(s):                  | <input type="text" value="ADDRESS"/> Filename, GENERIC*, *ALL   |
| Library:                  | <input type="text" value="FILTEST"/> Library name               |
| Purge Date:               | <input type="text" value="yyyy-mm-dd"/> Purge prior to date     |
| Keep History in Archive?: | <input checked="" type="radio"/> *NO <input type="radio"/> *YES |

If you get here from the file registration panel, the file name and library will already be filled in. The filename can be specified to purge all files registered in iFileAudit for the library (special value \*ALL) or you can purge a group of files using the GENERIC\* file option. The date must be specified in yyyy-mm-dd format with the dash characters included. A valid date is required.

When you specify that the history be added to the archive, the records will be moved from the active history to the archive history file. If your purge objective is to free up disc space on your system, the archive file members should be removed once they have been created. The archive file is named FAANZARC in library FILAUD and it is a multiple member database file. Do not remove the entire file, just the file members.

## Auto Analysis

From the initial display panel, you can use the AUTO ANALYSIS button to check the status of automatic analysis and control the settings for it. Auto Analysis, when active, runs in the background on your system and periodically analyzes transaction history for all registered files and updates each file in iFileAudit. When you select this option, the following panel will be displayed:



| <u>Description</u>             | <u>Status Information</u>   |
|--------------------------------|---|
| Current status is:             | Active  |
| Date and time of last startup: | 09/14/22 17:52:40   |
| Start method:                  | <input checked="" type="radio"/> *DEFER <input type="radio"/> *IMMED  |
| Analysis start time:           | <input type="text" value="2000"/> hhmm, 0000-2400                     |
| Analysis interval:             | <input type="text" value="1440"/> minutes between analysis, 0000-1440 |
| Last analysis start time/date: | 20:00:40 09/14/22   |
| Last analysis end time:        | 20:00:44  |

This display will tell you if this feature is active, when it was last started and the time of the most recent analysis run.

If the auto analysis is active, you must first change it to inactive before you can change any of the settings. Selecting the \*DEFER option means that the analysis will not run until the time you have set. Using the \*IMMED option will cause an analysis to start right away and then settle into the schedule that you specify for additional analysis processing.

## 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 iFileAudit and help control how it is implemented on your system. The Settings panel appears as follows:

| Description                  | Setting   |
|------------------------------|---|
| Journal process scope        | <input checked="" type="radio"/> *CURCHAIN (recommended) <input type="radio"/> *CURRENT |
| Member name prefix           | <input type="text" value="IF"/> 2 letter code   |
| Record level changes only?   | <input checked="" type="radio"/> *NO (recommended) <input type="radio"/> *YES           |
| Default date & time stamp    | <input checked="" type="radio"/> *NONE <input type="radio"/> *CURRENT                   |
| File views disposition       | <input checked="" type="radio"/> *KEEP <input type="radio"/> *DROP                      |
| Default journal library      | <input type="text" value="FILAUDJRN"/> Library name                                     |
| DSPJRN *ALLFILE scope        | <input checked="" type="radio"/> *NO <input type="radio"/> *YES                         |
| Read trace user control      | <input checked="" type="radio"/> *INCLUDE <input type="radio"/> *EXCLUDE                |
| Read trace jobname control   | <input type="radio"/> *INCLUDE <input checked="" type="radio"/> *EXCLUDE                |
| Exclude batch read tracing?  | <input type="radio"/> *NO <input checked="" type="radio"/> *YES                         |
| Use QTEMP for customer data? | <input type="radio"/> *NO <input checked="" type="radio"/> *YES                         |
| Browser roll factor          | <input type="text" value="012"/> # of lines   |
| Default print device         | <input type="text" value="FAPRT"/> Device name  |
| Default output queue         | <input type="text" value="*DEV"/> *DEV, Queue name                                      |
| Output queue library         | <input type="text" value="*LIBL"/> Library name   |

Set these parameters as follows:

Journal process scope

\*CURCHAIN - recommended - when the iFileAudit analysis process runs, all journals on the system for a file will be searched for transaction activity.

|                            |   |
|----------------------------|---|
|                            | *CURRENT - only the current active journal will be searched.  |
| Member name prefix         | Only change this value at the direction of support staff from Kisco Systems.  |
| Record level changes only? | *NO - recommended - all field level changes will be captured and reported by iFileAudit.<br><br>*YES - not recommended - only record level information will be captured. No field level information will be reported. (Normally only used for customers who have existing journalling in place that does not report both the “before” and “after” record images.)   |
| Default date & time stamp  | This parameter controls how the initial file update analysis will be run by iFileAudit. Enter one of the following values:<br><br>*NONE The last transaction date and time stamp will be set up as blank fields. When iFileAudit runs its initial analysis, it will search all available journal for activity going back as far as possible, assuming the first option here is *CURCHAIN. For some installations, this can be time consuming. (Recommended setting).<br><br>*CURRENT The last transaction date and time stamp will be set to the current date and time when the file is registered. Then, the first analysis run will only start from this point in time. |
| File views disposition     | This parameter lets you control whether or not the various logical views of the tracking history in iFileAudit will be maintained permanently or created as needed and then removed.<br><br>*KEEP Setting this value to *KEEP will speed up display and reporting operations in iFileAudit but may result in additional overhead for processing during iFileAudit analysis. Keeping the views active may also use up additional disk space.<br><br>*DROP Setting the LFOPR to *DROP will save disk space and improve analysis processing speed, but will cause iFileAudit to rebuild these views as needed for display and reporting purposes.                            |
| Default journal library    | Enter the name of the library you want to use for default journals created by iFileAudit. This is shipped from Kisco with the library name FILAUDJRN which is created during install processing. You can change this to whatever name you want to use if you want to specify a different library.   |
| DSPJRN *ALLFILE Scope?     | Gives you control over the way iFileAudit extracts information from your journals for analysis processing.  |

Kisco recommends that this be set to \*NO unless you specifically want to track changes to source physical files.

\*NO This is the recommended setting. When set this way, journal extract processing will be just for the registered files from the iFileAudit registration.

\*YES When set to \*YES, iFileAudit will always extract all activity from the journal. This can slow down journal analysis processing, but in the rare case when you need all activity for source physical files, this is the only way to do so.

If you want to track file activity for source physical files, then you will have to change this value to \*YES since not all journal activity codes will be retrieved otherwise. Keep in mind, however, that tracking changes in source physical files is problematic in iFileAudit due to the way their maintenance is normally implemented. For more information about this, please see the Frequently Asked Questions section of the iFileAudit Customer Support website at <https://www.kisco.com/ifa/support/iffaq.html#faq007>

Read trace user control When using the option to trace file read activity, iFileAudit requires that you limit the access by user profile selection and jobname selection. If you choose to include activity for specific user, you must then exclude selection for jobname and vice versa.

\*INCLUDE Read trace activity will only be recorded in iFileAudit for users specifically set up for any file where read tracing has been activated.

\*EXCLUDE Read trace activity will only be recorded in iFileAudit for all users except those users specifically set up for any file where read tracing has been activated.

Read trace jobname control When using the option to trace file read activity, iFileAudit can filter the activity based on the jobname. The setting here cannot match the setting for the immediately previous option.

\*INCLUDE Read trace activity will only be recorded in iFileAudit for jobnames specifically set up for any file where read tracing has been activated.

\*EXCLUDE Read trace activity will only be recorded in iFileAudit for all jobnames except those jobnames specifically set up for any file where read tracing has been activated.

Exclude batch read tracing This global setting controls read tracing activity for jobs running in batch. Kisco recommends that you set this value to \*YES and this is the default value as shipped. When set to \*YES, no read tracing activity for batch jobs will be recorded in iFileAudit for files that are tracking read activity.

## Use QTEMP For Customer Data?

Some customers specifically do not want any company data stored in the QTEMP library. This option allows them to make that change.

- \*YES Customer data processed during iFileAudit processing may be stored temporarily in the system QTEMP library (recommended setting).
- \*NO Customer data will never be stored in the system QTEMP library during iFileAudit processing. Instead, customer data will be temporarily stored in a user library in the customer ASP.

**Note:** If you specify \*NO for this setting, then the ASP number where your data will be processed must be entered in positions 185-191 of the CONTROL data area in library FILAUD. This value must be the same as the ASP value where your FILAUD library is stored. As an example, if you will be using ASP #2, you can update the data area using the following command:

```
CHGDTAARA DTAARA(FILAUD/CONTROL (185 7))
VALUE ('2      ')
```

## 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: Install the HTTP Server objects for iFileAudit
- Step 4: Start the new IFileAudit 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 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: Install the HTTP Server objects for iFileAudit

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

```
GO FILAUD/INSTALL
```

Run option #10 (Install HTTP Server Instance Objects) from this menu. This will install the HTTP server objects needed by iEventManager.



Step 4: 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:8080
```

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

Step 5: Update End User Table

For the browser interface to work correctly, the special IBM user profile QTMHHTTP must be added to the End User Table in iFileAudit. Run option #8 on the INSTALL menu and add QTMHHTTP as an administrator (User Type A). Check the profile to make sure it has a password that is set to \*NONE.

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/ifalagon.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 login 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/i 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. 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 IFILEAUDIT application.
  7. Start the updated KISCOIFA 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.

Take the following actions when the Web Administration Tool has started:

1. Select the “HTTP Servers” tab.
2. Use the Servers window and select the KISCOIFA 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 “FILEAUDIT” 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, 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 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 “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 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 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 6 - 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 7 - 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 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 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 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.