

iEventMonitor **User's Guide**

Version 8

As of April 2024



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

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

Table Of Contents

Introduction	1
Overview	1
Quick Start	2
What's New in Release 8	3
What Was New in Release 7.10	3
What Was New in Release 7	3
What Was New in Release 6	4
What Was New in Release 5	4
Notification Address(s)	5
Kisco Connect Integration Option	5
Off-Shift Default Notification Feature	6
Installation and Security	7
Kisco Software Support	7
World Wide Web Support	8
The Master Menu	9
Controlling iEventMonitor Tasks	10
Work With iEventMonitor Tasks	11
Start a Message Que Monitor	13
User Exit Program Feature	15
Suppressing Duplicate Message Queue Alerts	17
Responding To Error Messages	18
Maintain Message Routing	21
Maintain Message ID Exceptions	24
Maintain Message Overrides	26
Send An Alert	29
File Monitors	30
Display Activity Log	33
The Watch Menus	34
Message ID Watch Task	37
Watch Task Exit Program Option	39
ASP % Watch Function	41
Job Watch Function	44
Job Queue Watch	48
Utilization Monitor	50
User Profile Watch	52
Output Queue Watch	54
Lock Wait Watch	56
Excluding Jobs From Lock Wait Watch	57
Mutex-Wait Watch	58
Thread Wait Watch	60
Device Watch	62
Certificate Watch	65
Certificate Selection	66
User Profile Expiration Watch	68
Network Functions	69
Maintain Network Locations	70
Start Network Watch	72
Connection Watch	74
Audit Functions	78
The AUDIT Menu	79
Starting an Audit Monitor	81
Tracking Command Line Use	83

Finding More Details for an Audit Event	86
The Server Menu	88
Central Logging Feature	89
Getting Started with Central Logging	90
Working With The Central Activity Log	91
Display Central Activity Log	91
Listing Central Activity Log	93
Purging Central Activity Log	93
Reclaim Remote Log Entries	94
Remote Configuration Sync Feature	95
Getting Started with Remote Configuration Sync	96
Working With Sync Locations	97
Installation and Configuration	100
Installation from Download	100
Release Upgrade Installation	100
iEventMonitor Removal	100
SMTP Port# Variable	101
IEM Respond Configuration	102
The Install Menu	104
Display installation status	106
Change installation status	107
Permanent installation	108
Print additional documentation	108
Check Version Information	108
Purge Activity Log	109
Install Kisco PTF Package	110
Work With Authorized Users	111
iEventMonitor Default Values	113
Send Test Email Message	118
SIEM Feed Option	119
Optional Activity Trace	119
SETALT Command	120
Task-Specific END commands	120

Introduction

iEventMonitor is a system monitoring tool for the IBM i series of computer systems. Using iEventMonitor, you can automatically watch your system for a variety of events and then send alert notifications to either a set of email addresses, text messages or as break messages to logged in user profiles. You can monitor for messages in any message queue, watch for specific messages in any message queue, watch for changes in disc space use and much, much more.

For the purposes of this documentation, your system will be referred to as an “**IBM i**” system. This term is used generically and applies to all systems in the IBM i family, including your **Power System, i5** system, **AS/400** system or your **IBM i**.

Overview

When certain events occur on your IBM i system, you need to be able to react quickly to deal with error situations or prevent problems. If you have the luxury of having a computer operator who can sit and constantly monitor your system, then you have this covered. But traditional computer operators are few and far between these days.

iEventMonitor can be used to help you stay on top of important events happening on your IBM i system. Events monitored include:

- activity in message queues such as the system operator message queue (QSYSOPR)
- optional ability to respond to error messages remotely, included with the software
- security events posted to the QSYSMSG security message queue
- unanticipated changes in the total amount of disc space in use on the system
- file events for specific files including record adds, records changes, record deletes and even record reads (within reason) or file opens
- watching for specific messages being issued in any message queue
- watch for jobs building up in a job queue, but not running
- watch for reports building up in an output queue
- watch for a job ending, or starting, or both
- watch for security audit postings to the system audit journal
- much more

When one of these events happens, iEventMonitor can automatically notify you by email, text or by sending a break message to specific user profiles after first checking to make sure that they are currently signed onto your system. You can also specify a combination of email addresses, text addresses and user profiles.

Quick Start

If you are familiar with the IBM i OS and most IBM i software, you can get iEventMonitor up and running successfully using the following steps. Detailed documentation on each of the iEventMonitor features and functions follows for more specific details.

Step 1: Install the software using the instructions provided with the software and documentation download.

Step 2: At the end of the install process, the IEMSET command will be prompted. Before you leave this command, make sure that you enter the following parameters:

DFTID	Enter a valid email address where you want alerts to be sent. This will be used as a default address in all of the features.
SUPTID	Enter a valid email address. For alerts, this will be the address that can be used to reply to an alert.
SUPTEXT	Enter a text description. This will show up on an email alert as the sender of the email
DFTSUBJ	Enter a text description to be used as the alert email Subject.

The other defaults can be used for now. You can use the HELP key (F1) to get a description of each of the settings here. You can always come back to these settings using option #9 on the INSTALL menu.

Step 3: To verify that the email configuration is working correctly, run option #9 on the INSTALL menu to send a test email. If you find any problems, you will find some tips about typical issues with iEventMonitor email at the following link:

<http://www.kisco.com/emailconfig.htm>

Step 4: Most customers want to monitor the QSYSOPR message queue for error messages that need to be dealt with. The message queue monitor feature uses the IBM i OS Watch API feature. This depends on having the QUSRWRK subsystem active. Run the following command on your system to verify that this subsystem is active:

```
WRKACTJOB SBS(QUSRWRK)
```

If the subsystem is not active, it should be started.

Step 5: Go to the MASTER menu and run option #2 to start a message queue monitor for QSYSOPR. We recommend that you start with the severity filter set to 50. When just starting out, you can use the other default values.

At this point, you can continue to explore other monitors and watches once the above are working to your satisfaction.

If you have specific questions, you may find a quick answer at the following “Frequently Asked Questions” section of our support website for iEventMonitor:

<http://www.kisco.com/iem/support/iemfaq.htm>

What's New in Release 8

Release 8 became available in February 2024 and includes the following new features and capabilities:

- iEventMonitor now includes an Enterprise level for customers supporting multiple locations from a single node.
- The Enterprise version now supports a centralized activity logging function that will send log records from connected systems to a central server for review and administrative purposes.
- The Enterprise version also supports the ability to synchronize a configuration of iEventMonitor tasks and controls from a central location out to remote locations. This lets customers manage the configuration from a central location.
- New menus have been added to support the Enterprise logging functions and the Enterprise Synchronization function.
- On the system defined as the central logging server, the Display Activity Log function now works with the centralized log file where all records can be displayed including local log records.
- The Job Watch feature has been enhanced with an option that will issue an alert if a job is not running that should be running.
- The certificate watch has been enhanced so that you can now limit the watch to only selected certificates.

What Was New in Release 7.10

Release 7.10 was an interim release for iEventMonitor, issued in November 2023, that set the stage for new features to be added down the road, but it already included several changes and improvements since Release 7 became available. These include the following:

- The iEventMonitor Activity Log has been simplified so that there will only be a single record in the log for each alertable event. Prior to this change, if the alert was sent to multiple notification addresses, one record for each address was created.
- A new audit monitor option lets you track secure socket connections
- New start and stop commands have been added to let you start and stop specific tasks without affecting their status on the list of tasks. Previous to this, if you wanted to stop a specific task, it was removed from the list of tasks used in iEventMonitor on your system.
- The WATCH menus have been streamlined and there are now just two of them rather than the earlier three menus.
- The individual task ending commands that were previously included on the WATCH menus are still available as commands.

What Was New in Release 7

Release 7 was a major release for iEventMonitor. The following features and capabilities were added to iEventMonitor with Release 7 which became available in May 2023:

- A web browser user interface that we call “Bluescape” has been added to iEventMonitor for easier control of the application.
- iEventMonitor can now interface with Kisco’s new “Kisco Connect” software for more reliable texting of alerts via SMS.
- A new watch has been added to alert you when a Thread-Wait condition exists on your

system.

- A new watch has been added to check for digital certificates that will expire soon.
- A similar watch has also been added to check for user profiles that will expire soon.
- The Activity Log Purge now allows you to specify a number of days to keep as an option to entering a specific purge date.
- A new security audit code (SK) has been added to the Audit Monitor feature to show secure socket connections including rejections.
- The Output Queue watch now supports watching for a lot more spool files; up to 123,327.
- Email alerts can now optionally be routed through the IBM i OS using the IBM SMTP process for customers running IBM i OS 7.3 or later. When using this option, you can format the email message text in either plain text or HTML.
- An optional automatic purge of the iEventMonitor Activity Log has been implemented.

What Was New in Release 6

The following features and capabilities were added to iEventMonitor with Release 6 which became available in February 2022:

- The user profile logon/off watch has been enhanced to let you hide the user profile being watched from system users.
- A new alert escalation option has been added to the message queue monitor feature that lets you issue reminder alerts to a wider audience than your standard alert addresses.
- The Watch Task feature has been enhanced to let you watch for specific message IDs in the System History Log.
- All monitor and watch features now allow for an alternate alert subject text that can be unique to each task when it is started.
- When printing the Activity Log, you can now specify selection criteria to only show selected dates or a date range.
- The message queue monitor has been changed to suppress duplicate alerts issued within a given period of time. Initially, this is set to 5 minutes. See the documentation for more details.
- Five additional security audit codes have been added to the Audit Monitor feature including AD (Auditing changes), AX (Row and column access control), DS (DST password reset), EV (System environment variables) and ST (Use of service tools)
- The ASP Watch for specific storage levels has been modified with a reminder option if the over limit condition is not resolved within a given period of time.
- A specific message ID for a given job can be suppressed even if it qualifies for an alert.

What Was New in Release 5

The following features and capabilities were added to iEventMonitor with Release 5 which became available in May 2020:

- Prior to Release 5, the only way for customers to respond to error messages was by accessing your system remotely and responding to the messages. With Release 5, following proper configuration for an Apache HTTP server instance, a link will now be added to message queue monitor alerts that call for a response. When the link is followed, you will be able to view the full joblog and also respond to the error message. Before using this feature, check the “Installation and Configuration” section of this manual to see the additional configuration work needed to activate this feature on your system.
- A new test function was added to the INSTALL menu to use when testing the IEM Respond feature.
- A new “Text Friendly” option has been added in the WEBSET settings to make the IEM

- Respond feature easier to work with when alerting via text message.
- The reminder option on the Message Queue Monitor feature has been extended to up to 240 minutes.
- A new SETALT command has been added to allow a temporary switch to the Alternate Alert address for alerts.
- A new Connection Watch feature was added to monitor for servers connecting to your IBM i server.
- An optional SIEM Feed was added for the Message Queue Monitor alerts.
- A new file monitor option was added to alert you when a file has been opened.
- A new Audit Monitor feature was added to control how the monitor starts.
- A remote support feature was added to allow you to send diagnostic information to Kisco Systems.
- From the Task Review display, you can now show the log activity for the selected function.
- A new option to the Audit Monitor for command usage allows the alert to format the attachment in CSV format.
- The Message Queue Monitor function has been completely re-engineered to improve performance and guarantee complete alert processing.
- A possible issue for customers using security auditing for *JOBBAS or *JOBDDTA information has been resolved with a workaround. Details about this issue and the workaround can be found here: <http://www.kisco.com/iem/support/iejjobset.htm>
- A new Job Watch feature lets you report when an active job is put on hold
- The Watch option can now be used to issue an alert on a specific message ID in combination with a text string in the message.
- The Output Queue Watch will now give you the option to include spool files that are on hold in your queue count.
- The Output Queue Watch also now lets you specify and alternate alert subject text
- The Job Queue Watch now lets you watch *ALL (or GENERIC*) job queues in a given library with a single watch task.

Notification Address(s)

Each monitor or watch feature in iEventManager includes an entry field for notification address. The following rules apply on each command.

To specify an email notification, enter the email address information that you want to use. You can stack multiple addresses in the field as long as the total length does not exceed 200 characters. Separate the addresses by a semi-colon (;) character.

To specify a user profile, precede the profile with the # character. For example, to notify QSECOFR, enter the value #QSECOFR. When an alert is processed, the software will check to see if the user profile is logged into a terminal session and then send them a break message alert.

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

If you use the special value of *DFTID, then the notification addresses will be taken from the defaults set in the IEMSET command (option #9 on the INSTALL menu).

Kisco Connect Integration Option

Kisco Systems recently released a new SMS texting application called **Kisco Connect**. When you

install this new option on your system, you can take advantage of it from iEventMonitor. With Kisco Connect installed and activated in iEventMonitor, you can specify a cell phone number in any iEventMonitor Notification Address (EMAIL) field.

To specify a cell# using Kisco Connect, just enter the full cell number with no dashes or special characters. When the alert process in iEventMonitor sees the all numeric address, it will assume that you have entered a cell number and it will call Kisco Connect to send the SMS message.

Prior to this integration with Kisco Connect, SMS texts were sent using cell carrier's email-to-text feature. Since the initial release of iEventMonitor, most cell carriers have tightened up processing these email messages and delivery of these texts is no longer reliable. We strongly recommend adding Kisco Connect to obtain reliable SMS message delivery.

Off-Shift Default Notification Feature

iEventMonitor allows you to define two different default notification fields. The alternate can be used for off-shift alert notifications. This lets you define a different set of notifications for non-prime shift events.

As shipped from Kisco, this feature is turned off. To activate the feature, you must take the following actions:

1. Run the IEMSET command (menu option #9 on the INSTALL menu) and define a value Alternate Notification Address field (parameter DFTID2) using the same rules used for the Default Notification Address (parameter DFTID).

Note: Specify a special value of *NONE if you do not want to activate this feature.

2. Define the start and end time for your primary shift using the "Prime Shift Start Time" and "Prime Shift End Time" fields on the IEMSET command.
3. To treat certain days of the week as off-shift all day (such as Saturday or Sunday), enter the day of the week value in the "Off-Shift Days" field provided on the IEMSET command. If you want all days considered the same, use the special value of *NON (none).

Once you have activated this feature, whenever an alert condition is detected by iEventMonitor and the *DFTID special value has been specified for that alert monitor, then the alternate alert notification value will be used during off-shift times.

Notification to the alternate address can also be manually controlled by the SETALT command. See the topic on this command in the Installation and Configuration section of this manual.

Installation and Security

Specific installation instructions are covered in the section of this manual titled "Installation". To install your product on trial, follow those instructions. iEventManager is installed from a download file from the Internet. The initial installation will allow iEventManager to run on your system for a period of at least thirty days. At the end of the trial period, the software will no longer function.

When you decide to keep iEventManager, you must send your payment to Kisco Systems. At that time, Kisco must know the serial number for your system and the partition number where you have iEventManager installed. If you are not sure of your serial number, you can display it by using option #2 on the INSTALL menu.

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

Kisco Software Support

Kisco Systems software support is available from 7am to 6pm eastern time. You can reach software support with the following methods:

Phone: 518-897-5002
Email: support@kisco.com
Mail: Kisco Systems, LLC
54 Danbury Road, #439
Ridgefield, CT 06877

We encourage you to submit all technical support requests via email to support@kisco.com. When you do, a support ticket will be generated that will allow all of our tech support staff to keep up with your support case.

Off-hours support can be provided for all registered customers with advance notification. Contact our support staff at least 24 hours in advance when you think you will need off-hours support and we will provide instructions for contacting us during that time. If you have unscheduled off-hours support needs, you should place a phone call and send an email request. Support is generally available during off-hours.

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

The Kisco support policy program works as follows:

1. First year support is included in the purchase price. This includes unlimited telephone support, unlimited E-mail support, free release updates and free license transfers.
2. After the first year, an annual charge will apply for support and software maintenance.
3. The annual fee will be charged at the rate of 15% of the current selling price.

4. Support covered by this annual fee includes:
 - a. Unlimited telephone support (518-897-5002)
 - b. Unlimited E-mail support (Support@kisco.com)
 - c. Defect analysis and correction
 - d. Free updates to correct known defects (Kisco PTFs)
 - e. Free license transfers (when you move to a different system)
5. Customers must be active on maintenance in order to get a license transfer for the software to a new serial number.

At the end of your first year of ownership, you will receive a renewal quote from us for your next year's maintenance charge. Non-payment will be taken to mean that you decline maintenance.

World Wide Web Support

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

<http://www.kisco.com>

Support information specifically for iEventMonitor can be found at this address:

<http://www.kisco.com/iem/support>

At our Website, you will find:

- Product information about all Kisco software products for the IBM i.
- Customer support information including:
 - ▶ Latest release level information for all products
 - ▶ Technical bulletins
 - ▶ Frequently asked questions and answers
 - ▶ Problem reports including iEventMonitor PTF availability
 - ▶ Descriptions for recent enhancements to products
 - ▶ E-mail contact information for getting in touch with us
- Information about consulting services available from Kisco Systems.
- Registration for automatic notification about iEventMonitor enhancements and changes.
- and more

The first time you visit the Customer support section of our website for iEventMonitor, be sure to register for automatic notification. Once you are registered, we will automatically send Email notices to you about upgrades, enhancements and fixes for iEventMonitor as soon as they become available.

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

The Master Menu

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

```
GO IEMLIB/MASTER
```

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

```
ADDLIB IEMLIB
GO MASTER
```

The main iEventMonitor menu appears as follows:

The screenshot shows a terminal window titled "C - 2:5250 Display" with a menu titled "MASTER Menu" and "iEventMonitor Menu". The menu items are listed with their corresponding commands in the right margin. The terminal prompt is "Selection or command ==>" with a cursor pointing to the first option.

```

QSEC0FR                                MASTER Menu                                KISC01

                                iEventMonitor Menu

1.  Work With iEventMonitor Tasks          WRKIEM
2.  Start a Message Que Monitor            STRIEMON
4.  Maintain Message Routing
5.  Maintain Message ID Exceptions
6.  Maintain Message Overrides

7.  Send an Alert                          SNDALERT
8.  Work With File Monitors                WRKFILMON
9.  Display Activity Log                   WRKIEMLOG

10. To Watch Menu                          20-To Audit Monitor Menu          30-To Install Menu
15. To Network Menu                        25-To Server Menu

(c) 2015-2024 Kisco Systems LLC

Selection or command
==>

```

The terminal window also shows a command prompt "MA C" and a timestamp "22/007" in the bottom right corner.

Each menu option handles the following functions. The right margin of the menu display shows the command that is run by that option. All commands are located in the application library named IEMLIB. Each function is described in more detail later in this manual:

- | | | |
|----|-------------------------------|--|
| 1. | Work With iEventMonitor Tasks | Displays all iEventMonitor tasks that are currently configured along with current status information. Options are provided to start tasks, stop tasks and change settings. |
| 2. | Start a Message Que Monitor | Start a message queue monitor session |

- | | | |
|-----|--------------------------------|---|
| 4. | Maintain Message Routing | Allows you to specify alternate alert notifications for specific messages in specific message queues. |
| 5. | Maintain Message ID Exceptions | Update message queue ID exceptions. Lets you ignore specific messages. |
| 6. | Maintain Message Overrides | Allows you to implement additional controls over which messages will be reported or ignored for the message queue monitor function. |
| 7. | Send an Alert | Can be used to manually send an alert message |
| 8. | Work With File Monitors | Set up file action monitors and then activate or deactivate them. |
| 9. | Display Activity Log | Displays a list of alerts that have been issued by iEventManager starting with those issued most recently. |
| 10. | To Watch Menu | Displays the WATCH task menu. |
| 15. | To Network Menu | Displayed the NETWORK task menu. |
| 20. | To Audit Monitor Menu | Displays the AUDIT monitor task menu. |
| 25. | To Server Menu | Displays the IEMSVR menu for controlling the Apache HTTP server used by Bluescape and the IEM Respond feature. |
| 30. | To Install Menu | Displays the INSTALL task menu. |

Each of these menu options is discussed in the following sections of this user's guide.

Controlling iEventManager Tasks

Whenever you start a monitor or watch task in iEventManager, that function is logged on the system as active. This logging is done automatically and it captures all of the startup options that you specify, regardless of the task that you are starting.

Once the set of tasks that you want to use have all be started, it is an easy matter to end and restart them as needed. The following commands in library IEMLIB can be used:

- | | |
|-----------|--|
| STRIEM | Starts the IEMONITOR subsystem and all tasks that show when you run option #1 on the MASTER menu. |
| ENDIEM | Ends all iEventManager tasks currently running on your system and stops the IEMONITOR subsystem. |
| STRIEMTSK | Used to start an individual task that is not running. This can be used in your own CL program. |
| ENDIEMTSK | Used to end an individual task that is currently running. When you end any task using this command, it remains available for future use. |

At any time, you can review what tasks are currently defined by using menu option #1 on the MASTER menu. To add a task to the list of active tasks, just start it from the appropriate menu option. To update or change the settings for a task, just end it from menu option #1 using option 3, make the changes using option 2 and then restart it using option 1.

To end the active tasks without removing them from the task log, use the ENDIEM command.

If the tasks have been ended with the ENDIEM command, then you can restart them all using the STRIEM command. Option #1 on the MASTER menu includes function keys you can use to end or start the tasks in iEventManager that are present in the task log.

Work With iEventManager Tasks

When you select option #1 from the MASTER menu, or run the WRKIEM command, the following display will be shown:

```

E - 3:5250 Display
File Edit View Communication Actions Window Help
Type options, press Enter.
1=Start 2=Change 3=End 4=Delete 5=Display 9=Log
Type Task Watch Current Notification Addr Message Queue Ntfy
Opt sk Descriptn Name Status
-- AM Audit Mon. AFMONIT Active *DFTID *TXT
-- AM Audit Mon. CPMONIT Active *DFTID *TXT
-- AM Audit Mon. PWMONIT Active *DFTID *TXT
-- AM Audit Mon. SOMONIT Active *DFTID *TXT
-- AM Audit Mon. SVMONIT Active *DFTID *TXT
-- AS ASP% Watch ASPLVL1001 Active *DFTID
-- AS ASP% Watch ASPLVL2001 Active *DFTID
-- AS ASP% Watch ASPWTCH001 Active *DFTID
-- CN Conn Watch CNNWATCH Active *DFTID *SUMMARY
-- JQ Jobq Watch QBATCH Active *DFTID QBATCH *NO
-- JW Job Watch QTFTP* Active *DFTID
-- LW LCKW Watch *ALL Active *DFTID
-- MQ Msgque Mon QSYSMSG Active *DFTID QSYSMSG *NO
-- MQ Msgque Mon QSYSOPR Active *DFTID QSYSOPR *NO
More...
F3=Exit F5=Refresh F6=Start All F7=End All F9=Print
MA + E 09/078

```

This display allows you to work with each listed monitor or watch as follows by placing a code in the Opt field next to the task you want to work with:

- 1 Start - If the task is currently showing as Inactive, you can start it using option 1.
- 2 Change - lets you review the settings in use for the task and make changes. Changes can only be made if the task is currently showing as Inactive.
- 3 End - lets you stop an active task.

- 4 Delete - lets you delete a task from the list. A delete can only be processed when the task is showing as Inactive.
- 5 Displays the settings in use. You do not need to stop the function to use this option.
- 9 Displays the iEventManager activity log entries for this function.

The following function keys can be used for control over these tasks:

- F6 Will start all tasks provided that they are not currently running. This is the same as using the STRIEM command.
- F7 Will end all tasks if they are running. When ending tasks this way, they will not be removed from the task log. This is the same as using the ENDIEM command.
- F9 Will produce a listing of the active tasks log.

Note that tasks are added to this list when they are started using the individual functions on the various menu options in iEventManager. Once a task has been started once, you can then control it entirely using this display.

Start a Message Que Monitor

To start a message queue monitor for any message queue, run option #2 on the MASTER menu. The following prompt will be displayed:

```

B - 2:5250 Display
File Edit View Communication Actions Window Help
iEventMonitor Message Monitor (STRIEMON)

Type choices, press Enter.

Message que to be monitored . . . . .
Message que library . . . . . *LIBL
Notification address . . . . . *DFTID

-----

Severity filter . . . . . 00
Send Start/Stop Notifications? *YES
Message option . . . . . *KEEP
Reminder Alert Option . . . . . *NONE
Reminder Escalate? . . . . . *NO
Include message time? . . . . . *NO

00-99
*NO, *YES
*KEEP, *RMV
*NONE, 1-240 Minutes
*YES, *NO
*YES, *NO

Bottom
F3=Exit F4=Prompt F5=Refresh F10=Additional parameters F12=Cancel
F13=How to use this display F24=More keys

MA B 07/037
10.2.2.3:23

```

Fill in the parameters as follows:

Message que to be monitored

Enter the name of the message queue to be monitored.

Message que library

Enter the name of the library that contains the message queue. Most system message queues can use the *LIBL special value.

Notification address

See the Notification Address(s) section of this manual on page 5.

In addition, you can use the special value of *ROUTE, then the notification addresses will be determined by entries in the Route Table (option 4 on the MASTER menu). If the specific message ID does not find a match on the Route Table, then the *DFTID will be used.

Severity filter	Lets you ignore messages below a given severity level. For QSYSOPR, we recommend setting this value to 50. If you want to see every message, use the value 00.
Send Start/Stop Notifications?	Use the *YES value to sent out an alert when the message monitor is started and ended. Change the value to *NO if you do not want these messages sent.
Message option	Leave the default value *KEEP in place if you want to keep the message on the message queue after the alert has been sent (recommended). To cause these messages to be removed from the message queue, change this value to *RMV.
Reminder Alert Option	<p>This option tells iEventManager to issue reminder alerts when inquiry messages have been detected and they have not been responded to in a given period of time.</p> <p>Choose one of the following values:</p> <p>*NONE No reminder alerts will be issued.</p> <p>1-240 A variable number of minutes between reminder alerts. iEventManager will wait for the number of minutes specified and then check to see if the message has been answered. If not, a reminder alert will be issued. The reminder alerts will be repeated until the message is answered or the job in question has ended.</p>
Reminder Escalate?	<p>When set to *YES and a reminder alert is issued, in addition to the default alert notification addresses, another set of alert addresses will also be used. Before using this, make sure that the "Escalation Notification Addr" setting is updated in the IEMSET settings (option 9 on the INSTALL menu).</p> <p>When set to *YES, any reminder alerts will be issued to the escalation addresses specified in the IEMSET parameter in addition to the default notification addresses already set.</p>
Include message time?	<p>Choose one of the following values:</p> <p>*NO The message time from the message queue entry will not br shown in the alert.</p> <p>*YES The message time from the message queue entry will be shown in the alert. This may be</p>

useful for installations monitoring multiple systems across multiple time zones.

If you press the F10 key, additional parameters are presented:

Alert Subject Text

The message queue monitor allows you to use an alternate alert subject when reporting message queue alerts. To use the standard subject, just leave the special value *DFT in place.

To use an alternate subject text, enter up to 64 characters in this field. The field also supports three optional macro fields as follows:

&MSGIDX	The message ID being alerted will be used
&SYSNAME	The system name will be used
&JOB_NAMEEX	The job name that issued the message will be used
&JOBNO	The job number that issued the message will be used
&JOBID	A 28 characters value will be substituted in the following format: nnnnnn/uuuuuuuu/jjjjjjjj job number/user/job name Make sure that you leave 22 positions following the &JOBID macro to allow for the values to be posted.
&SEV	The severity level of the message will be used

Note: For the macros to work, they must be coded EXACTLY as shown in all upper case characters.

User Exit Program Feature

The iEventManager message queue monitor includes the ability to call a user exit program when a message queue monitor is triggered. When a message is detected that meets the criteria for issuing an alert message, iEventManager will check to see if a user program has been specified. If there is one, then that program will be called before the alert is issued. An option is also included to suppress the alert notification from iEventManager if you want to stop the alert message from being sent.

When the user exit program is called, a single parameter is passed with a parameter length of 4,000 characters. The layout of the parameter is fixed as follows:

Start	End	Length	Description
1	10	10	Message Queue being monitored
11	20	10	Library name as specified in the start
21	24	4	Message key - binary value
25	31	7	Message ID
32	163	132	Message text
164	165	2	Severity level
166	245	80	Message sender - see IBM documentation for details - includes information about the job that generated the message
246	250	5	Message 2 length
251	3250	3000	Variable message text 2
3251	4000	750	Not used - reserved for future implementations

Three additional parameters are available with the STRIEMON command. When the command is prompted, use the F10 option to show the additional parameters. The three parameters are as follows:

- Exit program (XPGM) Enter the name of the user exit program that you want to call. If you do not want to use an exit program, leave the default special value of *NONE in place.
- Exit program library (XLIB) When specifying a user exit program, enter the name of the library where it resides here.
- Send alerts (XALERT) Choose one of the following values:
- *NO No alerts will be issued.
- *YES Alerts will be issued as normal.

When a user exit program is specified, iEventManager will check to make sure it is a valid program in the library reference provided. If the program cannot be found, the monitor start will not be started. If the program is valid, it is the user's responsibility to make sure that it completes successfully. iEventManager will check for a CPF0000 error and attempt to continue processing if one is issued from the exit program, but other errors could cause the monitor to fail. Kisco recommends extensive testing before putting a user exit program into full production use.

Suppressing Duplicate Message Queue Alerts

An active application on your system could get into a looping condition issuing identical messages to your monitored message queue in a very high volume over a short period of time. This could, in turn, result in iEventManager clogging your email system or cell phone with unnecessary duplicate alerts. To avoid this situation, the message queue monitor will suppress such duplicate alerts within a given time period. When the software is initially installed, this default setting will be set to five minutes. The setting can be controlled from the IEMSET command default settings (option 9 on the INSTALL menu). Changing the setting to zero minutes will turn the suppression feature off.

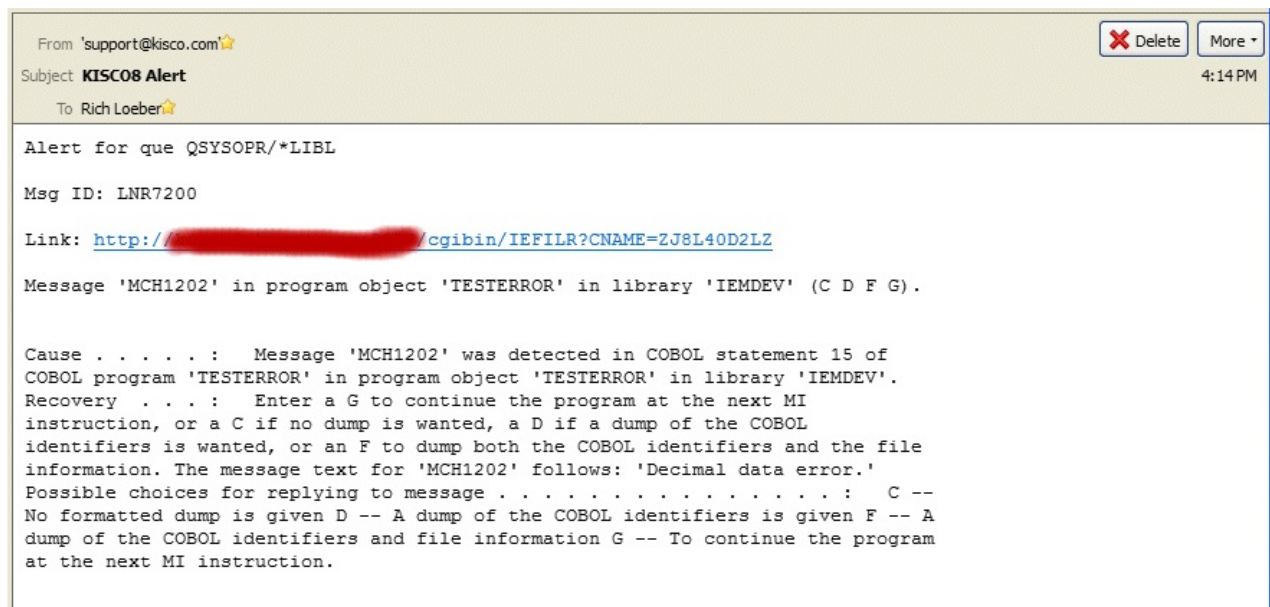
Responding To Error Messages

You can use iEventMonitor to respond to error messages remotely. Some additional installation and configuration work is required before you can use this feature. Please review the appropriate instructions in the “Installation and Configuration” section of this documentation.

When this feature is activated, an Apache HTTP server instance named IEVENTMON will be active on your system. If a message is received at a message queue that calls for a response, an HTTP link will be included in the alert issued from iEventMonitor. When you follow this link, either from an email message or a text message, a web page will be shown that will provide details about the error message.

A typical email message might look like this:

When you follow the link, a page like this will be shown to you:



When you click on the link, the following web page will be shown:



iEventMonitor Respond

<u>Info.</u>	<u>Value</u>
Message Queue	QSYSOPR - *LIBL
Message ID	LNR7200
Message Text	Message 'MCH1202' in program object 'TESTERROR' in library 'IEMDEV' (C D F G).
Extended Text	Cause : Message 'MCH1202' was detected in COBOL statement 15 of COBOL program 'TESTERROR' in program object 'TESTERROR' in library 'IEMDEV'. Recovery : Enter a G to continue the program at the next MI instruction, or a C if no dump is wanted, a D if a dump of the COBOL identifiers is wanted, or an F to dump both the COBOL identifiers and the file information. The message text for 'MCH1202' follows: 'Decimal data error.' Possible choices for replying to message : C -- No formatted dump is given D -- A dump of the COBOL identifiers is given F -- A dump of the COBOL identifiers and file information G -- To continue the program at the next MI instruction.
Job Name	TESTERROR
User Profile	QSECOFR
Job Number	100044
Date & Time	02/02/2022 13:16:11

[View Joblog](#)

Answer Message:

Send

On this web page, you can click on the “View Joblog” link to see the detailed joblog for the error message. It may be important to view the details before you answer the message. Once you have decided what the proper response for the message is, just enter it in the box at the bottom of the page and press the Send button. The message will be answered on your system.

If a problem occurs while processing your message response, you may receive an error feedback display. Errors that can occur include:

- This link is no longer available for use - indicates that the link has already been cleared from the system. All links are cleared on your system whenever iEventMonitor is restarted using the STRIEM command.
- Blank reply not processed - the message answer was left blank.

- Reply not processed, already answered - the message was answered already by a local source on your system.
- Reply not processed, message now gone - the message is no longer available to be answered.
- Your error respond session has encountered an internal error - indicates an internal error of some kind. If this happens, contact Kisco Systems.

Note: If you want to respond to an error message based on a text message to your cell phone, this is possible with certain conditions taken into effect. Keep in mind that the amount of information included in a text is limited to a fixed number of characters for many text services. To limit the number of characters on the text, please consider the following:

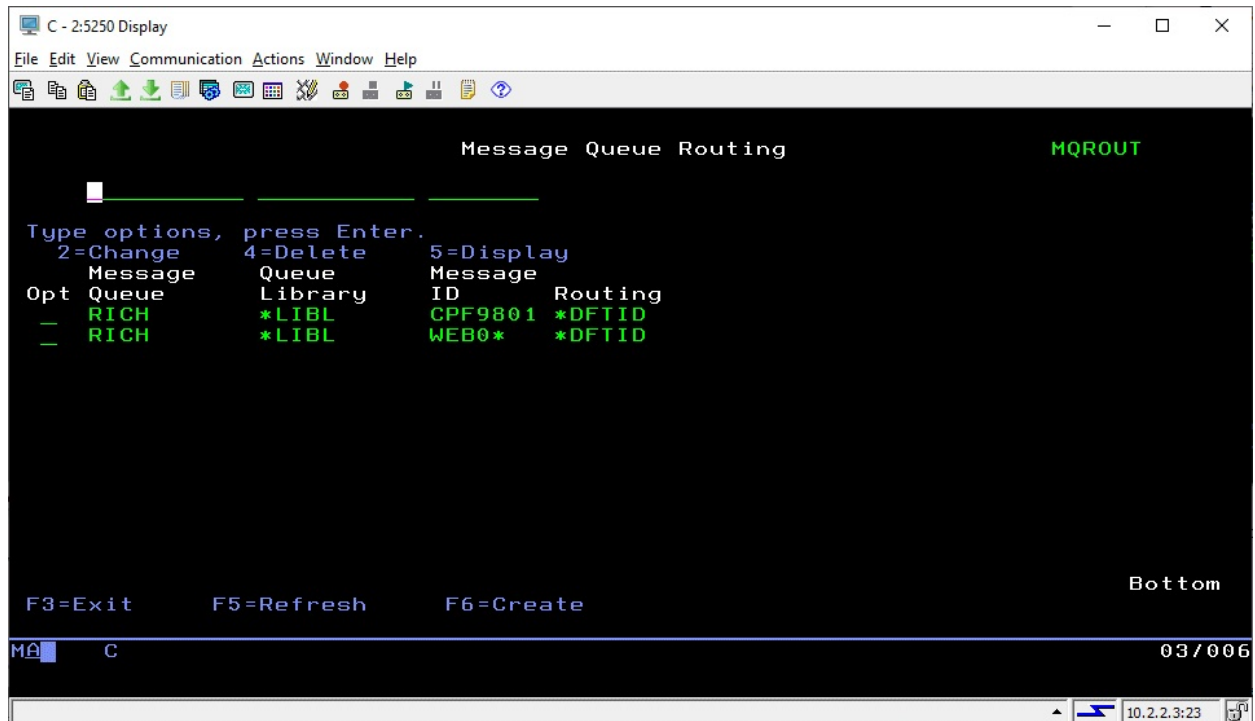
- In the IEMSET settings (option #9 on the INSTALL menu), keep the text entries for the following setting as short as possible:
 - Change the “Text Friendly Alerts?” setting to *YES
 - Support Name Description
 - Default Alert Subject
 - IEM Browser Respond IP
- Also in the IEMSET settings, specify *NO for Include Job Info in Alert?
- When you start the message queue monitor, specify *NO for Include message time?

These steps will result in a shorter text message and provide you with a useable link to follow. When you do follow the link, all of the information about the error, including the joblog, will be available. If you are using Kisco Connect, the character limit for SMS messages is 1,600 characters, so this is less of a consideration.

Maintain Message Routing

Your installation may want alerts issued to specific individuals for specific messages posted to a monitored message queue. The Message Routing process in iEventMonitor allows you to set this up. Routing instructions are message queue specific. You must provide the monitored message queue details for each routing rule created. The queue and library must be specified exactly the same way that they were started.

To create a routing or to work with any existing routings, run option #4 on the MASTER menu.

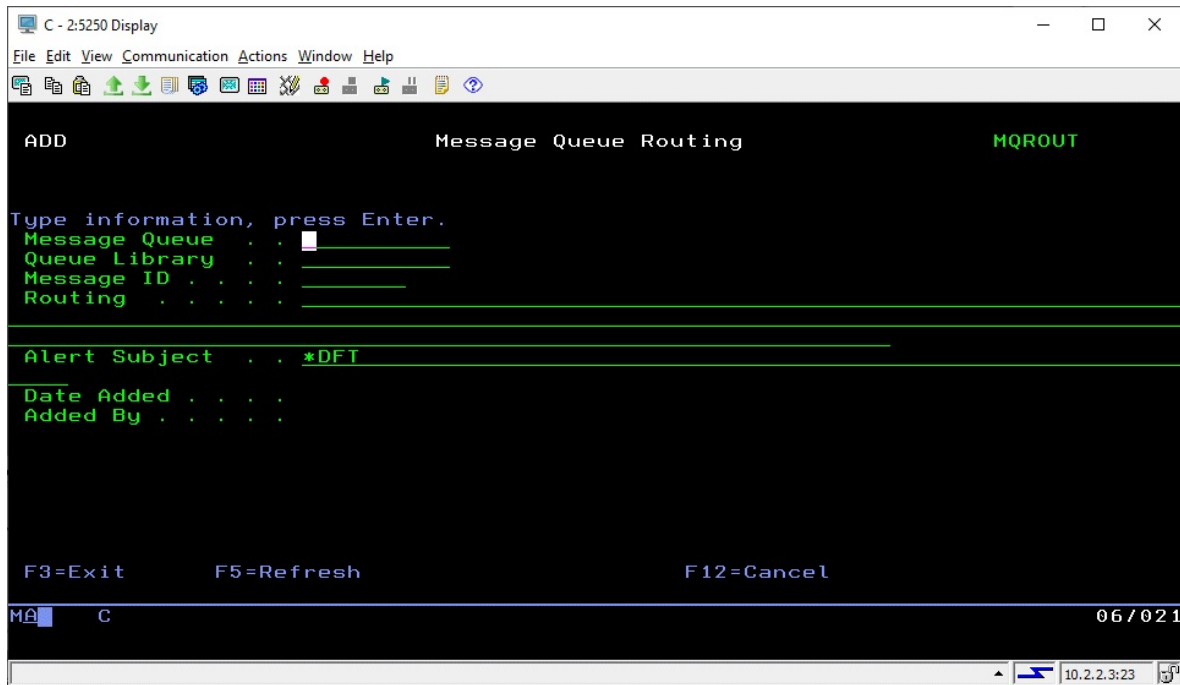


From this display, you can choose the following options in the left hand “Opt” column:

- 2 Gives you access to change an existing routing.
- 4 Deletes an existing routing.
- 5 Displays the details for an existing routing.

See the next page for creating or maintaining a routing.

To create a new routing, press the F6 key. The following will be displayed:



If you use option 2 or 5 on the initial routing display, this same display will be shown but the current settings will appear.

Complete these fields as follows:

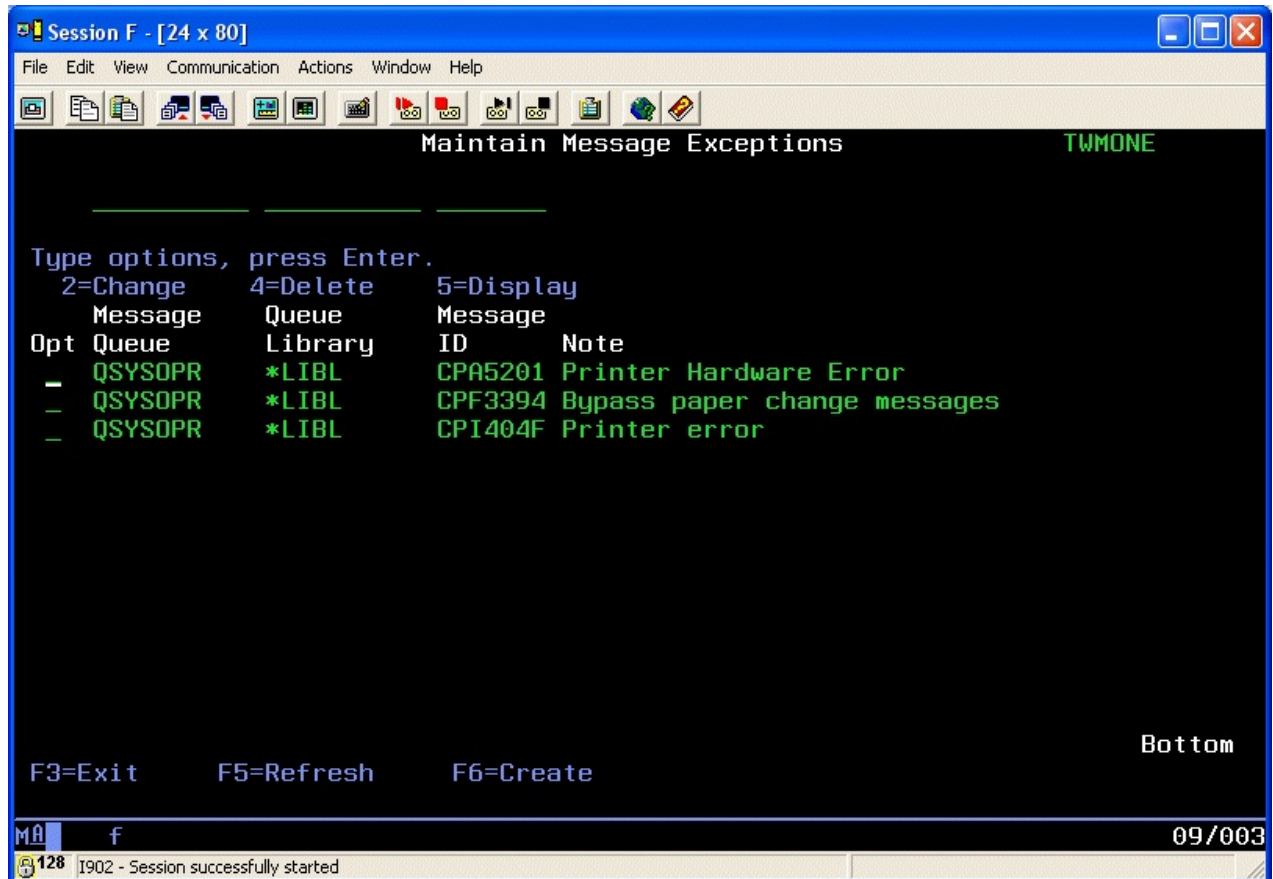
Message Queue	Enter the message queue name where you want this override to apply.
Queue Library	Enter the library reference for the message queue. This must match the library reference used when the message queue monitor was set up.
Message ID	Enter the message ID that you want this routing to apply to. The message ID must be in standard 7 character IBM i OS message format of AAAXXXX. IEventMonitor will accept a message ID with an asterisk as a wild card character. For example, if you enter a value of ABC1*, then any message that is received that starts with ABC1 will be routed using this routing rule.
Routing	See the Notification Address(s) section of this manual on page 5.
Alert Subject	Enter a specific alert subject that you want for this routing. If you want to use the standard default alert subject, use the special value *DFT.

When you press ENTER, the routing rule will be checked and then, if valid, it will be posted along with your user profile and the current date. Future references to this rule will show the profile and date information.

After a routing rule has been created, any time the monitored message arrives at the monitored message queue, regardless of message severity, it will be sent to the notification address(s) specified here with the specified alert subject text.

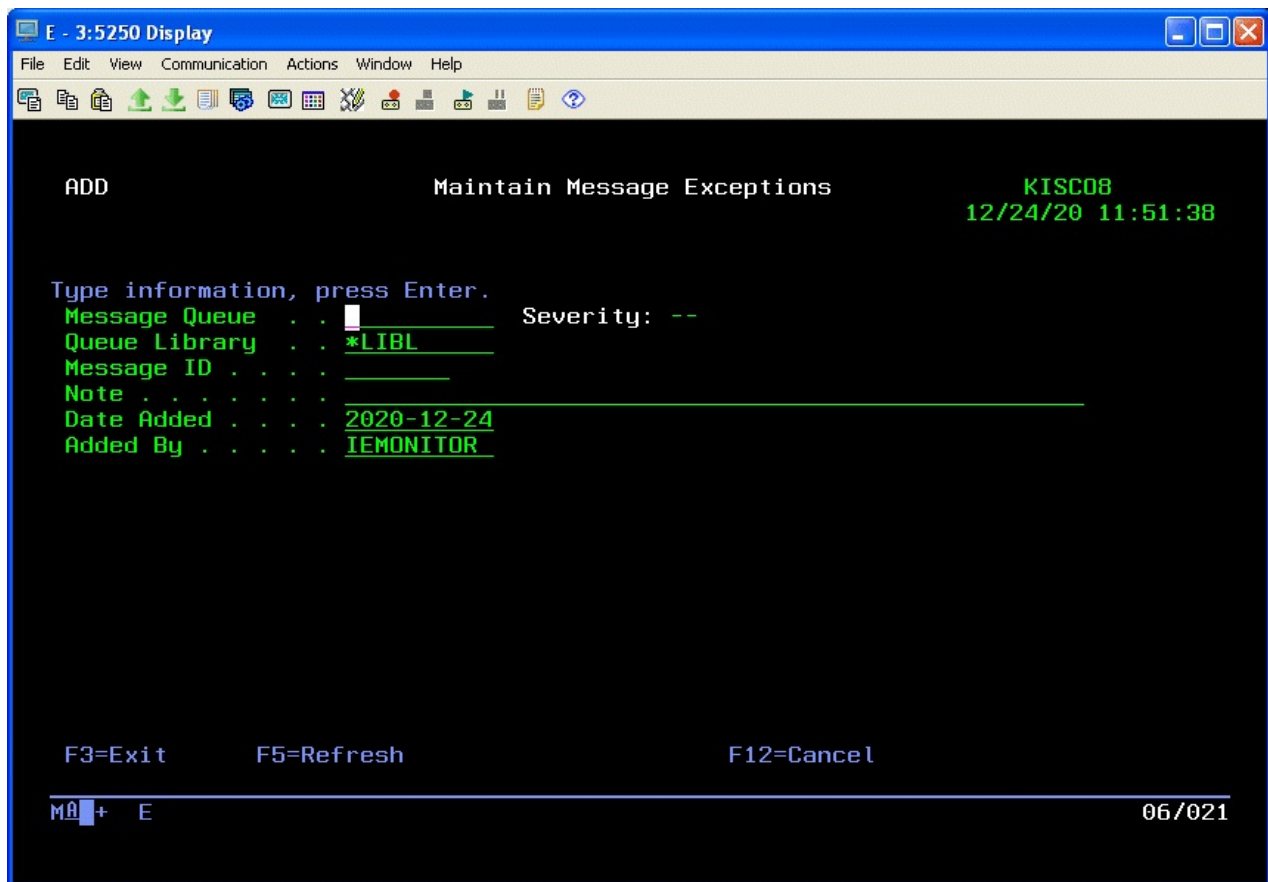
Maintain Message ID Exceptions

The message queue monitor allows you to ignore specific messages from processing by the monitor for a specific message queue. Using this feature, you can select to ignore messages for paper changes on printers and other hardware related situations. You can set these up using option #5 on the MASTER menu. When you select this option, a list of current message Ids will be presented:



When you first start this option, the list will be blank. To create a new entry, use the F6 function key.

When you start the process to create a new entry, the following display will be presented:



Enter the fields as follows:

- | | |
|---------------|--|
| Message Queue | Enter the name of the monitored message queue where you want this message to be ignored. |
| Queue Library | Enter the library reference for the message queue. If you start your monitor with a *LIBL reference, you MUST also use that same reference here. |
| Message ID | Enter the 7 character message ID that you want to ignore. |
| Note | Enter any descriptive information for the entry that you want. |

Once you press ENTER and record the new entry, messages with this message ID will be ignored for the monitored message queue.

Maintain Message Overrides

iEventManager has additional controls added to the product to allow for flexibility to the message queue monitor function. These add controls by job name, user profile, program name and time.

With these options, you can override the control by message severity and have iEventManager either always alert messages that arrive at the message queue or always suppress the alert. The criteria used can be the user profile that sent the message, the job name that sent the message, the name of the program that sent the message or a time override on repeating a message. In each category, you can instruct iEventManager to either always alert messages that match or never alert messages that match.

When iEventManager checks for these overrides, it will always check for the user profile first, then the job name and lastly the program name. If any override is found, the first one found will apply. If no overrides are found, then the logic of using the message severity code will apply and the message ID will be checked against the Message ID Control table.

To create an override, use option #6 on the MASTER menu. When you start this option, a screen like the following will be displayed:

```

C - 2:5250 Display
File Edit View Communication Actions Window Help
Maintain Monitor Overrides
KISC01
2/08/22 12:34:52

Type options, press Enter.
 2=Change   4=Delete   5=Display
Message    Queue      Over  Override  Message Over
Opt Queue   Library    Type  Set       ID      Cd  Override Description
_ QSYSOPR  *LIBL     *JOB  DAILYSAVE *ALL   A  For testing
_ RICH     *LIBL     *TIME FAD9001  *ALL   T

F3=Exit    F5=Refresh  F6=Create

MA C
03/006
  
```

To create a new override, use the F6 function key. When you do, the following detail screen will be displayed:

```

C - 2:5250 Display
File Edit View Communication Actions Window Help
ADD                               Maintain Monitor Overrides                               KISCO1
                                                                              2/08/22 12:36:44

Type information, press Enter.
Message Queue . . . . .
Queue Library . . . . . *LIBL      *LIBL, Library name
Override Type . . . . .           *JOB, *USER, *PGM or *TIME
Override Set . . . . .
Message ID . . . . . *ALL      Message ID or *ALL
Override Code . . . . . _ A=Aways/C=Combined/T=Time/X=Exclude
Override Description . . . . .
Delay Minutes . . . . .           1-1440
Date Added . . . . .           2022-02-08
Added By . . . . .           QSECOFR

F3=Exit      F5=Refresh      F12=Cancel

M C                               06/027
  
```

An override must be associated with a specific message queue. The message queue must also be referenced exactly the same way that the monitor is started. If you start the monitor referring to the message queue library using the *LIBL library list option, then the override must also be created this way.

Fill in the fields as follows:

Message Queue	Enter the name of the message queue
Queue Library	Enter the library for the message queue
Override Type	Choose one of the values as follows: *USER: The override set is a user profile *JOB: The override set is a job name *PGM: The override set is a program name *TIME: The override set is for a time delay on repeated messages
Override Set	Enter the override set to be checked against the message received. If you entered *USER above, enter the user profile here. If *JOB, enter the job name. If *PGM, enter the program name.

Override Code	Choose one of the values as follows:
A	Always alert the qualifying message
X	Never alert the qualifying message
C	Combines Always alert (as stated above with code A) with message ID Exceptions. If the message should always be reported but there is an active ID Exception for it, it will be suppressed.
T	Use this value for a time exception. See also the “Delay Minutes” setting below.
Message ID	Enter the value *ALL for most entries. If you want to override a specific message ID handling for a given job (Override Type *JOB), then you can enter that message ID here. For example, if you want to suppress just a given error message from a job, you can do that here. To suppress all messages from a given job, use the *ALL value.
Override Description	Enter your own description for the override condition.
Delay Minutes	For a Time exception, enter the number of minutes that you want to suppress the message for. This will prevent a regularly occurring message from being alerted over and over. A value of 1 to 1440 may be entered.

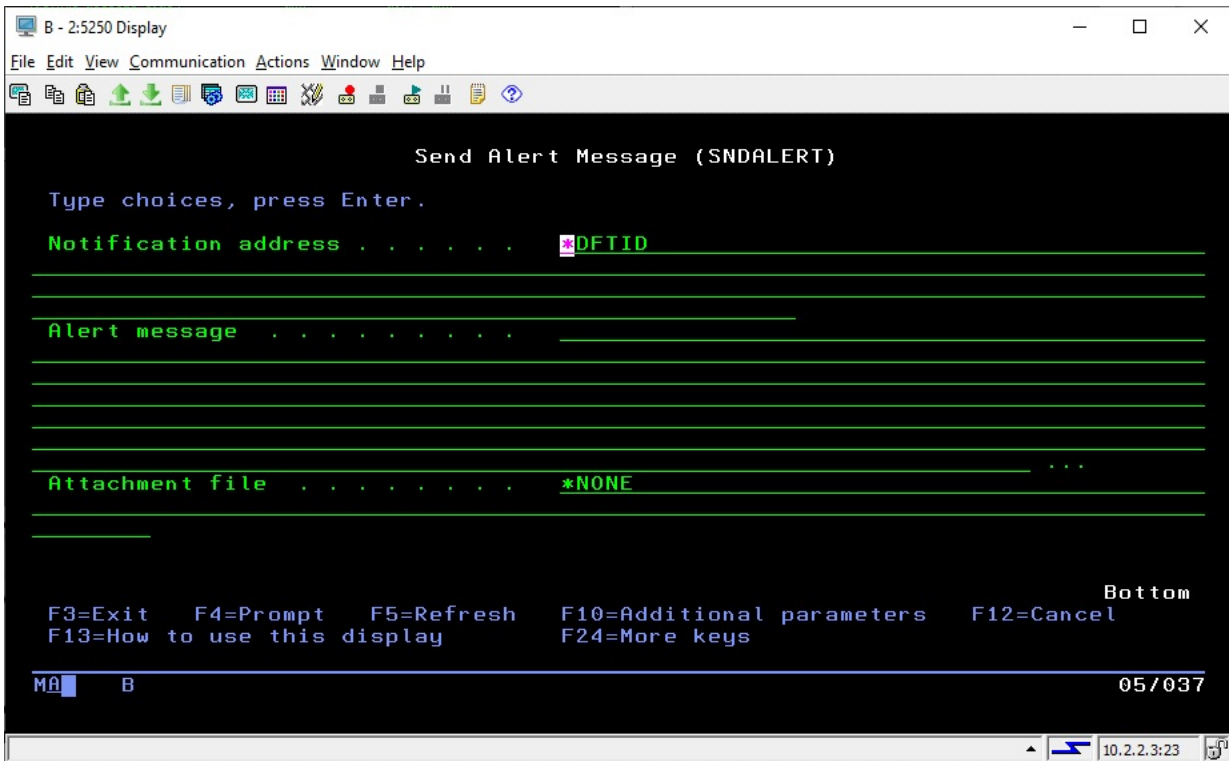
Note: Using Override Code C, you can get all messages issued for a job, user or program, but still suppress specific messages that you are not interested in seeing, like paper changes or printer alignment.

Note: An example of the *TIME override might be when your system is low on storage. When this happens, your system will issue the CPI099C message every 30 minutes until the low storage situation no longer exists. Before this change, iEventManager would issue a fresh alert on this message every time it was issued. After this change, you can control how often this error is repeated as an alert. You might want it to be issued as an alert every 4 hours instead of every 30 minutes.

When all fields have been entered, press ENTER to record the override in the table. Once created, messages monitored on the message queue will check this table first before checking for severity and message ID exceptions.

Send An Alert

When you select menu option #7 or prompt the SNDALERT command in library IEMLIB, the following display will be shown:



This can be used to manually send an alert message. Fill in the parameters as follows:

- | | |
|----------------------|---|
| Notification address | See the Notification Address(s) section of this manual on page 5. |
| Alert message | Enter up to 1,024 characters that you want to send as your alert message. |
| Attachment File | <p>Enter the path for an attachment file that you want to include with the alert notification. As an example, if you want to include a file named myfile.txt that is stored in the tmp folder in the IFS, then this parameter would look like this:</p> <p>/tmp/myfile.txt</p> <p>If you leave the default value *NONE, then no attachment file will be included.</p> |

You can also access a unique alert subject text field for this command by using the F10 key. If you do so, please leave the other additional parameters set the way they appear.

Note that this command can be used either from the command line or within your own CL programs. When you process the command, the alert message text will be sent to all addresses specified.

File Monitors

When you select option #8 from the MASTER menu, or run the WRKFILMON command, the following display will be shown:

```

E - 3:5250 Display
File Monitor Files List                                IEMFIL

Type options, press Enter.
1=Activate      2=Change      4=Delete      5=Display      6=Deactivate
File
Opt Library    File Name    File Description    In Dl Up Rd Opn Typ Status
1 IEMDEV      INVESTR     Inv Master          X              D Active

F3=Exit      F5=Refresh    F6=Create

MA+ E                                               09/002

```

This display shows a list of files that are set up for the File Monitor feature in iEventMonitor. A File Monitor will “watch” an IBM i database file for selected types of process activity. You can configure your file monitor to look for record adds, record changes, record deletes, file opens or file record read processing. When any selected event occurs, iEventMonitor will send an alert with the details. You can specify for detailed information on each event or summary information after every *nth* event.

The above sample display shows one file monitor that is in Active status. Once a monitor has been created, you must then activate it before it will start reporting. You can always deactivate a monitor but leave the configuration in place for future use.

To create a new File Monitor, press the F6 function key and the following screen will be presented to you:

```

B - 2:5250 Display
File Edit View Communication Actions Window Help
ADD File Monitor Files List IEMFIL
Type information, press Enter.
File Library . . . . .
File Name . . . . .
File Description . . . . .
Monitor Type . . . . . D=Detail/S=Summary
Summary Threshold Level . . . . . Report summary after nth event
Insert . . . . . X=Notify when records added
Delete . . . . . X=Notify when records delete
Update . . . . . X=Notify when records updated
Read . . . . . X=Notify when records read
Open . . . . . X=Notify any access - Must be used alone
Notification Address *DFIID
Current Status: Inactive
Only check between times . . . . . and . . . . . Blank checks all times
Check all day on . . . . . Sat: _ Sun: _ X Notify on Sat/Sun as selected
F3=Exit F5=Refresh F12=Cancel
MA B 04/029
10.2.2.3:23

```

Fill in the fields as follows:

- | | |
|-------------------|--|
| File Library | Enter the name of the library where the file resides. |
| File Name | Enter the name of the file to be monitored. |
| File Description | Leave this blank when creating the monitor. The system will pick this field up for the file description. |
| File Monitor Type | D: Detail level monitor. For every selected event, iEventManager will issue an alert.
S: Summary level monitor. iEventManager will issue a summarized alert each time the Summary Threshold has been reached. |
| Summary Threshold | For summary monitors only. Enter the number of events between alerts. |
| Insert | Enter X if you want to monitor for records being added to the file. |
| Delete | Enter X if you want to monitor for records being deleted from the |

	file.
Update	Enter X if you want to monitor for records being updated in the file.
Read	Enter X if you want to monitor for records being read from the file.
WARNING!!	We strongly advise that you not use a Read monitor when you are running a Detail monitor. This could easily result in an excessive number of alerts being issued and possible system and/or application degradation.
Open	<p>Enter X if you want to monitor for the file being opened. When you use this option, the following additional restrictions apply:</p> <ul style="list-style-type: none"> ● It can be the only option specified. Insert, Delete, Update and Read must all be blank. ● The Monitor Type must be set to S ● The Summary Threshold must be set to zero <p>You will receive a file alert whenever a user accesses the file. The alert will not be repeated until either of the following conditions occur:</p> <ul style="list-style-type: none"> ● A different user accesses the file. ● The same user accesses the file after the date has changed.
Notification Address	See the Notification Address(s) section of this manual on page 5.
Only check between Time	This is an optional entry. If you leave it blank, there will be no restriction on the time of day when the monitor will run. If you want to limit the time period when the monitor will be active, enter the time span when you want the monitor to run. Two fields are provided to allow you to span the time period from midnight to the next morning.
Check all day on	If you want the file monitor to be active on Saturday and Sunday, place an X in the field for those days.

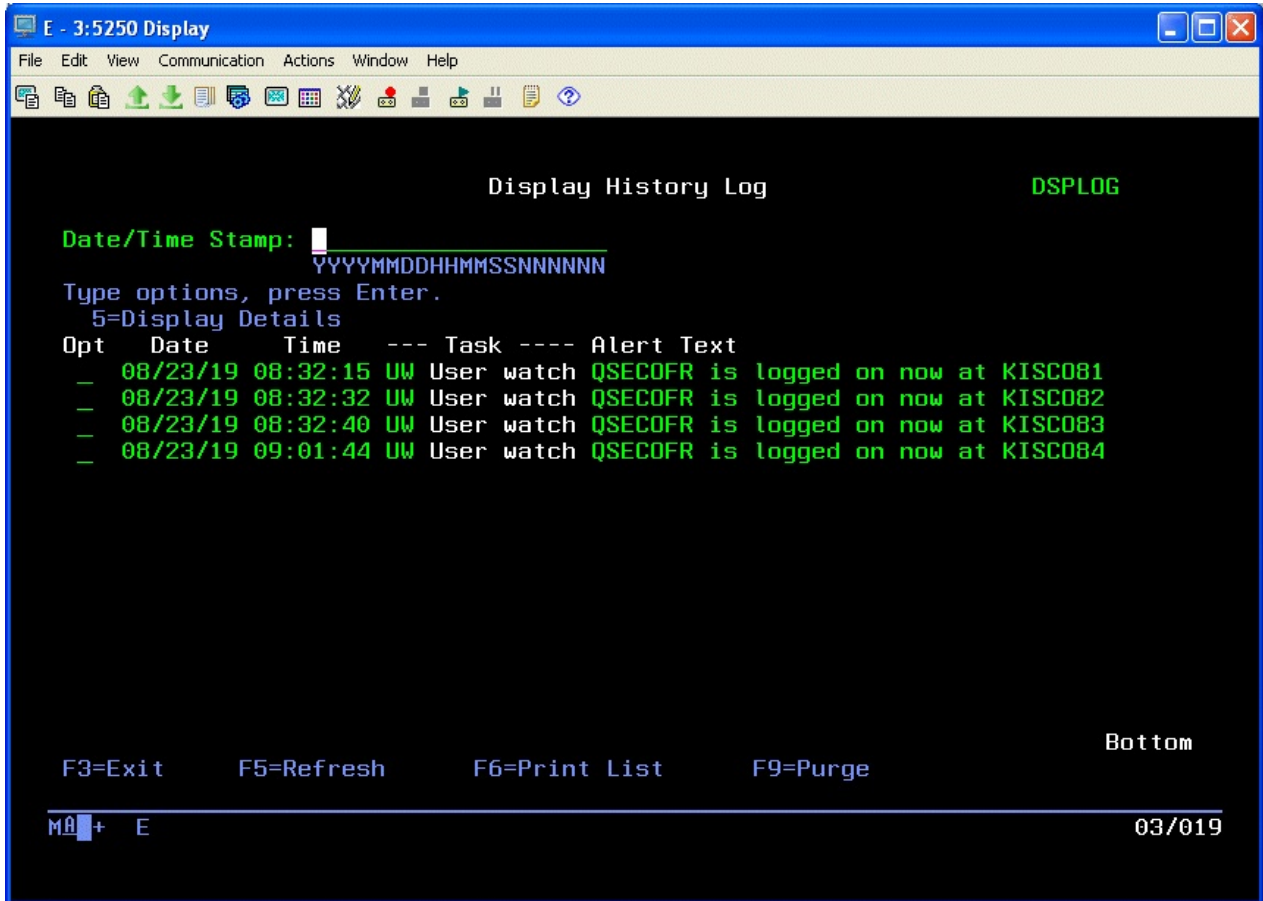
Once you have the monitor configured, press ENTER to store the configuration. The display will return to the list of monitors and the monitor will be configured in "Inactive" status. No file monitoring actions will be taken until you activate the monitor.

To activate a monitor that you have configured, locate it in the list of monitors and place a '1' next to it in the option (Opt) column and press the ENTER key. This will activate the monitor and start tracking activity immediately.

To stop a monitor that is active, find it in the list and place a '6' next to it in the option column and press the ENTER key. This will stop all file monitor activity immediately.

Display Activity Log

When you select option #9 on the MASTER menu or use the WRKIEMLOG command, a list of alerts that have been issued by iEventMonitor on this system along with administrative actions will be displayed starting with events from the current date. If the system where you are using option 9 on the MASTER menu has been defined as a central logging server (see the documentation about this feature in a separate section of this documentation), then the central activity log will be shown. That is documented in the central logging feature section of this manual.



The screenshot shows a window titled "E - 3:5250 Display" with a menu bar (File, Edit, View, Communication, Actions, Window, Help) and a toolbar. The main content area is titled "Display History Log" and "DSPLOG". It displays a table of alerts with columns for Date, Time, Task, and Alert Text. The table contains four entries, all with the task "User watch" and the alert text "QSECOFR is logged on now at KISC081-084". Below the table, there are function key shortcuts: F3=Exit, F5=Refresh, F6=Print List, F9=Purge, and Bottom. The status bar at the bottom shows "MA + E" and "03/019".

```

Date/Time Stamp: 
                    YYYYMMDDHHMMSSNNNNNN
Type options, press Enter.
  5=Display Details
Opt  Date      Time    --- Task ---- Alert Text
--  --  --  --  --
--  08/23/19  08:32:15  UW  User watch  QSECOFR is logged on now at KISC081
--  08/23/19  08:32:32  UW  User watch  QSECOFR is logged on now at KISC082
--  08/23/19  08:32:40  UW  User watch  QSECOFR is logged on now at KISC083
--  08/23/19  09:01:44  UW  User watch  QSECOFR is logged on now at KISC084

F3=Exit    F5=Refresh    F6=Print List    F9=Purge
Bottom
MA + E                                03/019

```

To view the details about a specific alert, put a 5 next to it and press ENTER.

You can list the contents of the log using the F6 function key. When you use the list function, a prompt display will let you either print all entries or a selection of entries.

The F9 function key will allow you to purge the contents of the log of all entries prior to a given date. The purge process can also be performed using the DSPLOGPRG command.

The Watch Menus

iEventManager contains a number of watch features that will monitor for specific situations and events on your system. The Watch menus control these functions and looks like this:

WATCH Menu:

```

WATCH                                     WATCH Menu
                                     iEventManager Watch Task Menu

1.  Start a Watch Task                    STRIEMWAT
2.  Start ASP % Watch                     STRWCHASP
3.  Start a Job Watch Task                IEMJOBWCH
4.  Start a Job Queue Watch               STRWCHJQ
5.  Start a Utilization Monitor           STRIEMUTIL
6.  Start User Profile Watch              STRUSRWCH
7.  Start Output Queue Watch              STRWCHOQ
8.  Start Lock Wait Watch - LCKW          IEMLCKWCH
9.  Start Mutex Wait Watch - MTXW         IEMMTXWCH
10. Start Thread Wait Watch - THDW        IETHDWWCH

20.  To WATCH2 Menu
30.  To MASTER Menu

(c) 2015-2024 Kisco Systems LLC

Selection or command
==>

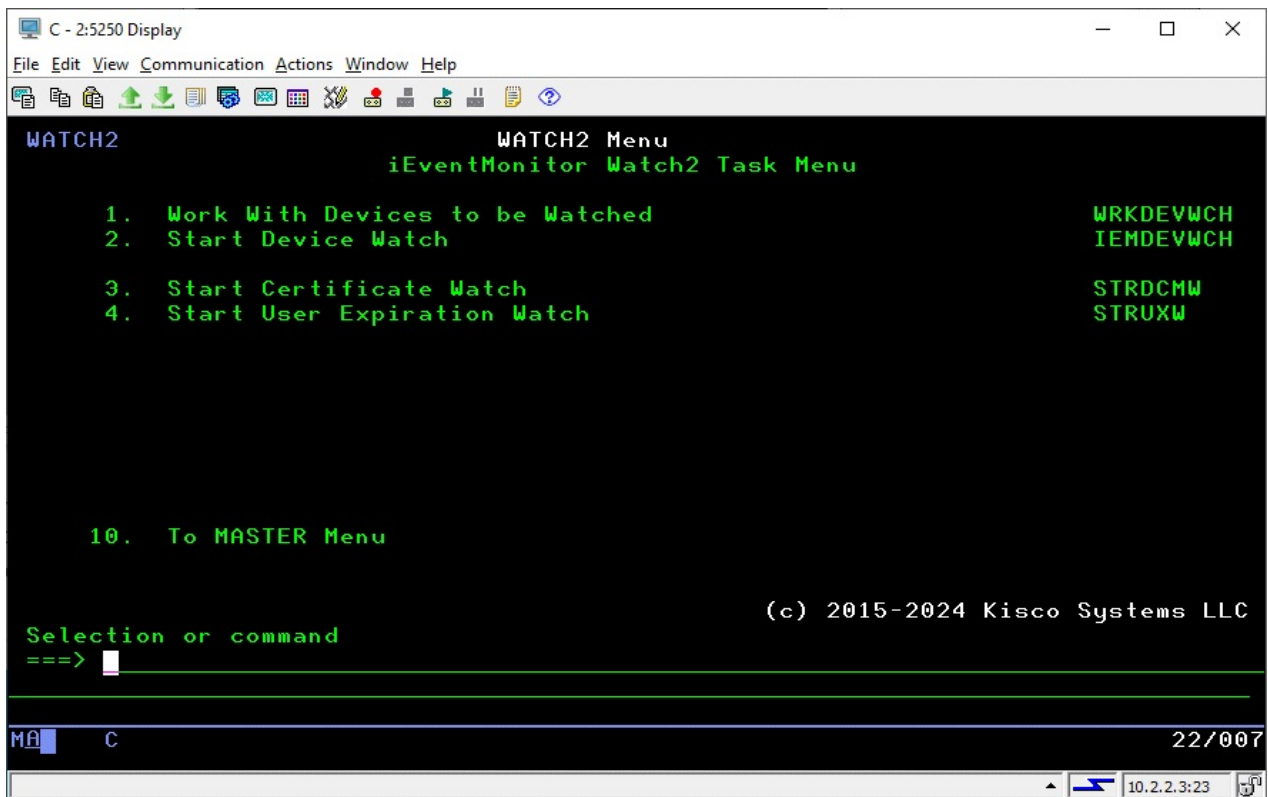
```

The options on this menu are as follows:

- | | |
|--------------------------------|---|
| 1. Start a Watch Task | Start a watch for a specific message ID on a message queue or in the System History Log |
| 2. Start ASP % Watch | Start a watch for significant storage level changes |
| 3. Start a Job Watch Task | Start a watch for a specific or a generic* job name |
| 4. Start a Job Queue Watch | Start a task to watch a specific job queue to see if it gets backed up with jobs not starting or gets put on hold |
| 5. Start a Utilization Monitor | Start a watch for a specific subsystem looking for jobs with very high CPU utilization |
| 6. Start User Profile Watch | Start a watch looking for a specific user profile logging on to your system with a terminal session. |
| 7. Start Output Queue Watch | Start and output queue watch. |

- | | |
|-----------------------------|---|
| 8. Start Lock Wait Watch | Start a Lock-Wait watch (LCKW) |
| 9. Start MTXW Watch | Start a watch looking for jobs entering MTXW status. |
| 10. Start Thread Wait Watch | Start a Thread-Wait watch (THDW) |
| 20. To WATCH2 Menu | Transfer to the WATCH2 menu for additional Watch functions. |
| 30. To MASTER Menu | Return to the MASTER menu |

Additional Watch Tasks are on the WATCH2 Menu:



The options on this menu are as follows:

- | | |
|------------------------------------|---|
| 3. Work With Devices to be Watched | Work with devices names to be watched |
| 2. Start Device Watch | Start a watch for specific devices on the system to issue alerts when they are not available for use. |
| 3. Start Certificate Watch | Start a daily check for digital certificates that are expiring soon. |
| 4. Start User Expiration Watch | Start a daily check for user profiles that will be expiring |

soon.

10. To MASTER Menu

Return to the MASTER menu

Each of these functions is described in the following sections of this documentation.

Message ID Watch Task

iEventManager includes a feature that will allow you to set watches for specific message IDs arriving at any message queue you want to watch or in the System History Log. This watch function is different from the message queue monitor feature in that the watch will check for a specific message ID regardless of the message severity level whereas the monitor looks at all messages that have a severity code at a selected level or higher. This is also the only way to watch for a message on the System History Log.

You can also set a watch to look for a specific text string appearing in a message posted to a message queue or in the history log.

You can set a single watch or multiple watches using this feature. It will let you monitor the system operator message queue at the same time that you have the iEventManager message queue monitor function active. You can also set watches for any other message queue in your system including user profile message queues.

From the WATCH menu, you can start a watch, end a watch.

Each watch that runs on your system must be assigned a unique 10 character name. As a watch task is started, it is logged into the iEventManager system. At any time, you can view the names of the active watches by running option #1 from the MASTER menu by checking the WT (Watch Task) entries.

To start a new Watch task, select option #1 from the WATCH menu. The following screen will be displayed:

```

B - 2:5250 Display
File Edit View Communication Actions Window Help
Start IEM Watch (STRIEMWAT)

Type choices, press Enter.

Watch name . . . . . Unique name
Notification address . . . . . *DFTID

-----
Message to watch for . . . . . Msg ID, GENERIC*, *ALL, *IMMED
Message que to be monitored . . . . . Queue name, *HSTLOG
Message que library . . . . . *LIBL Library name, *LIBL
Send Start Email? . . . . . *YES *NO, *YES
Message Text . . . . . *NONE

F3=Exit F4=Prompt F5=Refresh F10=Additional parameters F12=Cancel
F13=How to use this display F24=More keys

Bottom
MA B 05/037

```


Enter the command parameters as follows:

Watch name	This must be a unique watch event name. You can set multiple watches, but each one must have a unique name. You will need to know this name when you want to end the watch event at a later time.
Notification Address	See the Notification Address(s) section of this manual on page 5.
Message to watch for	Enter the message ID that you want to monitor for with this watch task. *ALL Search all messages posted to the message queue *IMMED Search just the immediate messages that are posted to the message queue
Message que to be monitored	Enter the name of the message queue that you want to monitor. You can watch for a specific message in the System History Log by using the special value *HSTLOG. When you use this option, you must be watching for a specific message ID and you cannot specify a Message Text selection.
Message que library	Enter the name of the library where the message queue is located.
Send Start Email?	Leave the default value *YES if you want iEventMonitor to issue an

alert reporting that this watch task is being activated. Change it to *NO if you do not want the alert to be issued.

Message Text If you are not searching for a specific text string, leave this set to *NONE.

If you are searching for a text string, enter the string here. Keep in mind that the string is case sensitive and uses embedded blanks.

Using the F10 function key, additional parameters will be shown:

Alert Subject Text iEventManager will issue an alert with the default subject text if you leave this set to *DFT. If you want a unique alert subject text used, enter that value here and it will be used if an alert is issued.

See below for the Exit Program options that are also shown.

Watch Task Exit Program Option

The Watch Task includes an optional exit program interface. To access the additional parameters needed for this feature, press the F10 key and you will see the following additional options:

Exit program If you want to call your own exit program during watch processing, enter the name of the program here. When the watch is satisfied, the exit program will be called passing a single parameter that contains information about the message issued. The amount of information is determined by the setting of the Exit Level parameter (see below). If you are not using an exit program, then the special value of *NONE should be used.

Exit program library If you are calling your own exit program, enter the name of the library where it is stored on your system. You can use the *LIBL value if the library is in the system user library list.

Send alerts This value controls whether iEventManager will send out an alert when you have specified an exit program.

Choose one of the following values:

*NO - No alerts will be issued.

*YES - Alerts will be issued as normal.

Exit level Choose the level of exit data that you want passed to your exit program.

Choose one of the following values:

*STD The single parameter with a length value of 7 will be passed.

It will contain the message ID value.

*ADV A single parameter of 1024 characters will be passed which represents the full message detail available from the message ID being watched for. This can be used for a variety of user objectives. The full message data stream is included.

ASP % Watch Function

Option #2 on the WATCH menu can be used to start up to three special watch functions that will monitor disc space utilization changes. The ASP % (Auxilliary Storage Pool) represents the amount of disc space that has been used. On the IBM i system, if this percentage reaches 100%, the system can abnormally terminate all processing, so it is critical that you know when this percentage is making unplanned changes.

The Interval ASP Watch function will start a job that will periodically check on the ASP % for your system and when it changes by a rate that you set, an alert will be issued advising you of the change and reporting the new ASP % rate for you. This will let you react well in advance of a catastrophic event on your system. Alternately you start one or two Level ASP Watch Functions that will issue alerts when the ASP% exceeds specific given levels.

To start any ASP Watch functions, select option #5 on the WATCH menu or issue the STRWCHASP command in the IEMLIB library. The following display shows the options you will need to set when starting this feature:

```

C - 2:5250 Display
File Edit View Communication Actions Window Help
Start ASP Use Watch (STRWCHASP)

Type choices, press Enter.

Aux Storage Pool Number . . . . . 001          001-255 (001=System)
Notification Address . . . . . *DFTID

-----

Check interval . . . . . 15          Minutes
Percentage change . . . . . 5          % difference
Watch type . . . . . *INT          *INT, *LVL1, *LVL2
Alert On . . . . . *BOTH          *BOTH, *INCR, *DECR

Bottom
F3=Exit   F4=Prompt   F5=Refresh   F10=Additional parameters   F12=Cancel
F13=How to use this display   F24=More keys

MA C 05/037
  
```

Fill in the parameters as follows:

Aux Storage Pool
Number

Enter the ASP number that you want to watch. ASP number 001 is the default system ASP. This value must be entered as a 3 digit number in the range of 001 - 255. If you are setting an ASP Watch, we recommend that you always include ASP #001 which is the system ASP. ASP numbers greater than 032 are iASP's

	(Independent ASPs).
Notification Address	See the Notification Address(s) section of this manual on page 5.
Check interval	Enter the interval in minutes. This tells iEventManager how frequently you want the system to check the current status of the ASP (disc) utilization.
Percentage change	<p>For an Interval Watch, enter the percentage change that you want to be notified about. The default value is 5%. Using this value, when the utilization on the ASP increases or decreases by 5%, a notice will be issued. If you need to react to a problem on your system, this should provide you with some advance warning.</p> <p>For a Level Watch, set the specific ASP% level you want an alert issued for. For example, if you want an alert when the ASP% reaches 70% and another when it reaches 85%, set the *LVL1 (see below) to 70 and the *LVL2 to 85.</p>
Watch type	<p>Select one the the following. Only one watch of each type can be started:</p> <p>*INT An Interval Watch will be started.</p> <p>*LVL1 The first Level Watch will be started.</p> <p>*LVL2 The second Level Watch will be started.</p>
Alert On	<p>This option controls how the *INT watch type works.</p> <p>Choose one of the following values:</p> <p>*INCR Whenever the disc utilization increases by the given percentage, an alert will be issued.</p> <p>*DECR Whenever the disc utilization decreases by the given percentage, an alert will be issued.</p> <p>*BOTH Whenever the disc utilization either increases or decreases</p>

Using the F10 function key will display an additional parameters as follows:

Level Reminder	<p>When using the *LVL1 or *LVL2 Watch Type, you can ask iEventManager to send a reminder alert if the over level condition is not corrected after a period of time. If you do not want a reminder, leave this set to zero. Otherwise, enter the number of minutes before you want a reminder alert issued if the over limit situation has not been resolved. When using this option, keep in mind that the INTERVAL setting will still control how often the level is checked. So, if you have the INTERVAL set to 15 minutes and the LREMIND set to 25 minutes, the watch will check every 15 minutes.</p>
----------------	--

Alert Subject Text iEventManager will issue an alert with the default subject text if you leave this set to *DFT. If you want a unique alert subject text used, enter that value here and it will be used if an alert is issued.

When you start an ASP Watch function, it will set a flag within the software indicating that the function is active. Once this flag is set, it is available for automatic restart after an IPL or an ENDIEM command.

Job Watch Function

iEventManager includes options for you to watch specific jobs on your system. The option lets you be notified when a job starts on your system, when a job ends or both. You can watch a specific job name started by a specific user profile or you can watch for a job name that you specify using a GENERIC* reference. For example, if you want to make sure that the FTP server stays active on your system, you can set a watch for the job name QTFTP* ending and, if the FTP server stops running for any reason, you will receive an alert from iEventManager.

To start a job watch, select option 3 from the WATCH menu or use the command named IEMJOBWCH in library IEMLIB. You will be prompted with the following:

```

C - 2:5250 Display
File Edit View Communication Actions Window Help
iEventManager Job Watch (IEMJOBWCH)

Type choices, press Enter.

Job Name To Watch . . . . .
User Profile . . . . .
Watch Option . . . . . *STRSTP
Check Interval . . . . . 15
Reminder Interval . . . . . 0
Run Time Check . . . . . 0
Notification address . . . . . *DFTID

Name or GENERIC*
User Profile or *ALL
*ONEND, *ONSTART, *BOTH...
Seconds 1-9999
Minutes, 0-60
Minutes, 0-1440

Bottom
F3=Exit F4=Prompt F5=Refresh F10=Additional parameters F12=Cancel
F13=How to use this display F24=More keys

MA C 05/037

```

Enter the parameters as follows:

Job Name To Watch

Enter the specific job name that you want to watch or enter a Generic* job name ending with an asterisk characters (*). The watch task will as look for job names that qualify based on this name.

Note: If you start a GENERIC* job watch, be aware that the notification email will only be sent when there are no longer any jobs running that match the GENERIC* job name used. If you have several jobs running under a similar name and

one ends but not all, you will not be notified.

User Profile

Enter the specific user profile that started the job you want to watch or use the special value of *ALL to check for the job running under any user profile.

Watch Option

Choose one of the five options offered:

*STRSTP Recommended.

When you use this option, the job watch will check to see if the specified job (or jobs) is running. If it is currently running, then it will issue an alert when it ends. If it is currently not running, then an alert will be issued when it starts. In either case, the job watch will then stay active to report again if the job ends or starts. The only way to end this job watch is by using the ENDIEM command, issuing a stop from option #1 on the MASTER menu or with the IEMJOBWEND command.

Note: When you use the *STRSTP option, an additional parameter will be prompted. See “Alert if on Hold?” below.

*LRUN The job watch will note when a job starts and then only issue an alert when the Run Time Check minutes have been exceeded. At that point, an alert will be issued indicating that the job is running longer than expected. If you specify *LRUN, then the Run Time Check value cannot be set to zero.

*NRUN The job watch will issue an alert when the job is not running. This can be used to alert when mission critical jobs are not running but should be running.

*ONEND Use this option to send an alert when the specified job has ended. This assumes that the task is currently running. When an alert is issued, this watch will then terminate. (Not recommended)

*ONSTART Use this option when you want an alert sent with the specified job starts. This assumes that the task is not currently running. When an alert is issued, this watch will then terminate. (Not recommended)

*BOTH Use this option to send an alert when the specified job starts and then again when it

ends. This assumes that the job is not currently running. Once both conditions have been met, the watch will terminate. (Not recommended)

Check Interval	Enter how frequently you want to check for the job starting or ending, in seconds.
Reminder Interval	<p>This setting is only valid on a Job Watch where the *STRSTP or *NRUN option is being used.</p> <p>Enter the number of minutes that you want to lapse before a reminder alert is sent when the job being watched has stopped but not restarted yet. If you enter the value of zero, then no reminder alerts will be issued.</p>
Notification address	See the Notification Address(s) section of this manual on page 5.
Run Time Check	<p>This setting is only valid on a Job Watch where the *STRSTP or *LRUN option is being used along with a specific job name and a specific user profile.</p> <p>Enter the number of minutes that you want to lapse before a reminder alert is sent if the job in question starts and then does not end. This value should be your expected run time. The alert will advise you that the job is running longer than expected.</p> <p>A value of zero means that no alert will be issued.</p>

If you specify the *STRSTP option, the following additional parameter will be prompted:

Alert if on Hold?	<p>This option lets iEventMonitor issue an alert when the watched job is put on hold. This option is only available when the *STRSTP Watch Option is used and the job name being watched is not GENERIC*.</p> <p>Enter one of the following options:</p> <p>*NO No alerts will be issued when the watched job is put on hold.</p> <p>*YES If the watched job is held, an alert will be issued. If it is subsequently released and then held again, a new alert will be issued.</p>
-------------------	--

Using the F10 function key will open one additional optional field for your use as follows:

Alert Subject Text

The job watch allows you to use an alternate alert subject when reporting alerts. To use the standard subject, just leave the special value *DFT in place.

To use an alternate subject text, enter up to 64 characters in this field. The field also supports three optional macro fields as follows:

&SYSNAME The system name will be used

&JOB_NAMEEX The job name that issued the message will be used

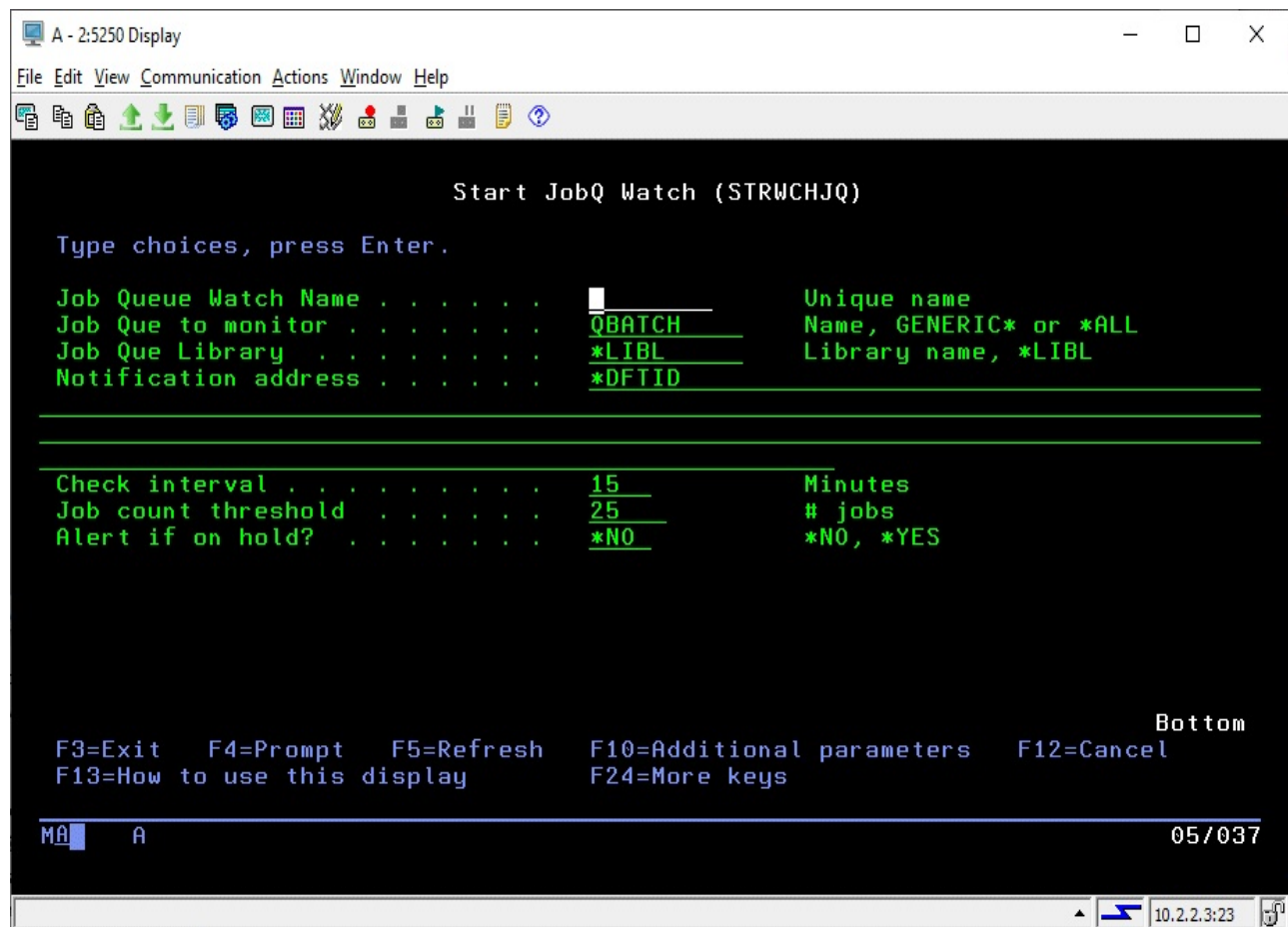
&JOBNO The job number that issued the message will be used if available.

Note: For the macros to work, they must be coded EXACTLY as shown in all upper case characters.

Job Queue Watch

For some customers, it is important that the job queues not get backed up with batch jobs that are not getting run. iEventManager allows you to set a watch on any job queue in the system. Once set, if the watched job queue exceeds the threshold of jobs waiting to run that you specify, an alert will be sent advising you of a potential issue. You can also be alerted when the job queue is placed on hold.

To start a job queue watch, select option #4 on the WATCH menu or use the STRWCHJQ command. The following will be displayed:



Enter the parameters as follows:

Job Queue Watch Name

Enter a unique name that will be assigned to this job queue watch task. This name will be used as part of the watch job name with the letters "IW" added before it. It will also be used when ending the job queue watch.

Job Que to monitor	<p>Enter the name of the job queue that you want to monitor or one of the following special values:</p> <p>*ALL All job queues in the specified library will be watched. A specific library name must be used when *ALL is specified.</p> <p>GENERIC* All job queues in the specified library with names that start with specified string will be watched. A specific library name must be used when *ALL is specified.</p> <p>When either of the special values is used, each job queue that qualifies will be watched. When ever any of these queues has an alert condition detected, an alert will be issued.</p>
Job Que Library	Enter the name of the library where the queue is located. The special value *LIBL will use all libraries in the current session library list.
Notification address	See the Notification Address(s) section of this manual on page 5.
Check interval	Enter a value, in minutes, that indicates how frequently you want to check the job queue stack. The default value is 15 minutes but you can specify as low as 1 and as high as 999, but 15 minutes is a good setting to start with.
Job count threshold	Enter the number of jobs that you want to be advised about. When the job queue contains more than this number of jobs that are waiting to be run, an alert will be generated. This alert will be repeated at each check interval until either the monitor is stopped or the number of jobs waiting to run returns to a lower level.
Alert if on hold?	<p>This value controls whether iEventMonitor will send out advisory alerts when this job queue is placed on hold.</p> <p>Choose one of the following values:</p> <p>*NO No job queue on hold alerts will be issued.</p> <p>*YES An alert will be issued when this job queue is placed on hold. The alerts will continue until the job queue is released.</p>

Using the F10 function key will display an additional parameter as follows:

Alert Subject Text	iEventMonitor will issue an alert with the default subject text if you leave this set to *DFT. If you want a unique alert subject text used, enter that value here and it will be used if an alert is issued.
--------------------	---

When you start the Job Queue Watch, it will run in the IEMONITOR subsystem.

Utilization Monitor

iEventManager includes a Utilization Monitor feature. Using this feature, you can monitor interactive subsystems, such as QINTER, for jobs that are using too much CPU capacity. High use of CPU can be an indication of a runaway job or an application that is poorly designed.

Option #5 on the WATCH menu will start a utilization monitor. When you start a Utilization Monitor, the following will be displayed:

```

A - 2:5250 Display
File Edit View Communication Actions Window Help
iEventManager Utilization Mnr (STRIEMUTIL)
Type choices, press Enter.
Notification address . . . . . *DFTID
Subsystem . . . . . QINTER      Name or *ALL
Check interval . . . . . 30      Seconds, 15-999
Utilization threshold . . . . . 50  CPU rate

F3=Exit  F4=Prompt  F5=Refresh  F10=Additional parameters  F12=Cancel
F13=How to use this display  F24=More keys

MA A 05/037

```

Fill in the parameters as follows:

Notification address	See the Notification Address(s) section of this manual on page 5.
Subsystem	Enter the sub-system name that you want to watch. The default value of QINTER will watch jobs running in the system default interactive subsystem. Kisco does not recommend using this feature to monitor jobs in a batch processing subsystem. To monitor total system utilization, use the special value of *ALL.
Check interval	Enter a value in seconds. The monitor will check for excess utilization every specified interval.

Utilization threshold Enter the utilization threshold value that you want the monitor to check. This is expressed as a percentage of the CPU utilization for the job.

Using the F10 function key will display an additional parameter as follows:

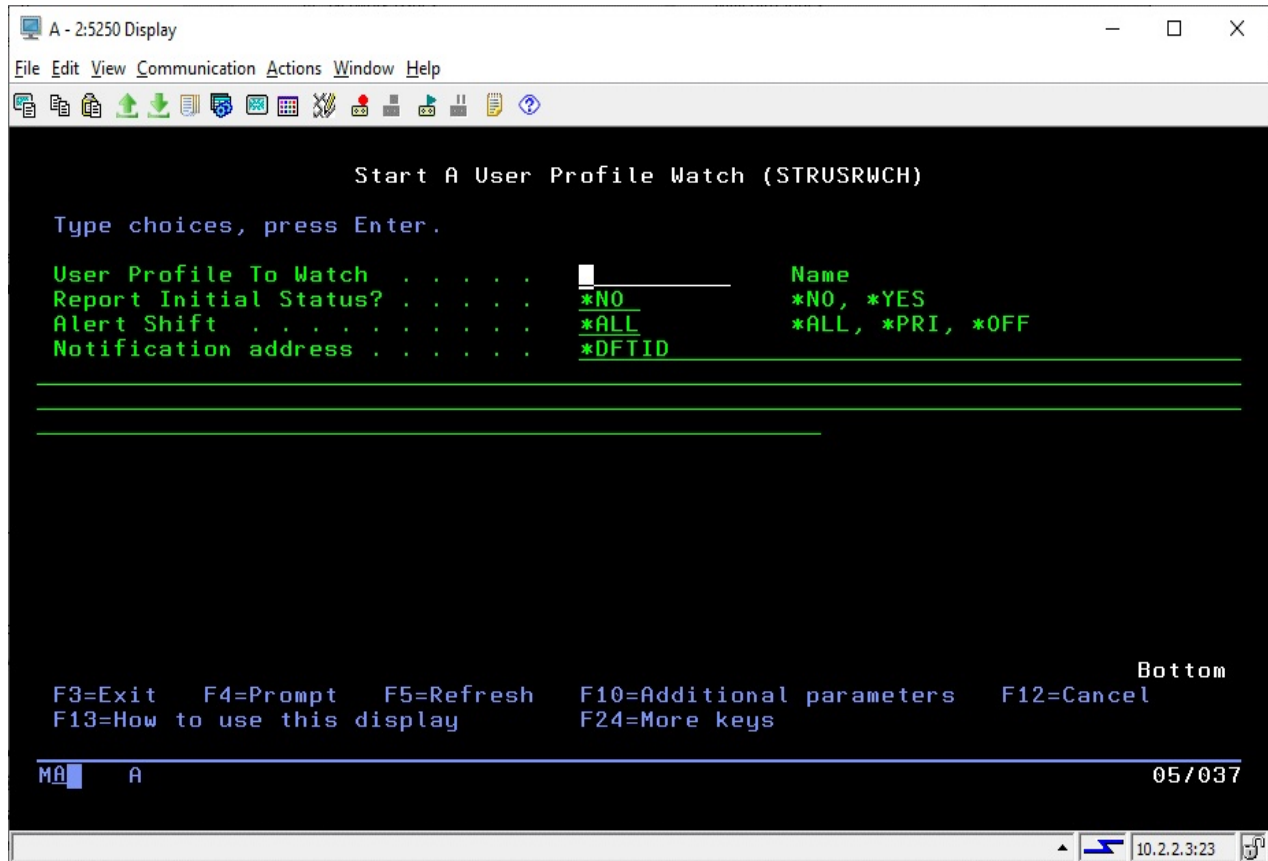
Alert Subject Text iEventMonitor will issue an alert with the default subject text if you leave this set to *DFT. If you want a unique alert subject text used, enter that value here and it will be used if an alert is issued.

With this monitor running, jobs in the specified subsystem (or all jobs if you used the *ALL option) will be checked at each interval break. If any jobs are showing CPU utilization in excess of the threshold value entered, an alert will be generated. If the situation persists, additional alerts will continue to be reported until either the monitor is stopped or the utilization issue is resolved.

User Profile Watch

The User Profile Watch feature will let you track user profile use for interactive sessions. When a user profile watch is started, it will alert when a user profile is used for an interactive signon process or a signoff process. The watch will stay active and continue watching for signon and signoff activity.

Option 6 on the WATCH menu will start a user profile watch. The startup display is as follows:



The options are as follows:

- | | |
|------------------------|---|
| User Profile To Watch | Enter the name of the user profile that you want to track. |
| Report Initial Status? | Controls the initial status reporting for the specified user profile. |
| | Choose one of the following values: |
| *NO | The current status of the user profile sessions will not be alerted. |
| *YES | At startup, the current status of the user profile sessions will be issued as an alert. |

Alert Shift Controls whether alerts are issued all the time or only during prime or off-prime shift times.

Choose one of the following values:

*ALL Alerts will be issued regardless of the shift time.

*PRI Alerts will only be issued when they occur during the time period identified as prime shift.

*OFF Alerts will only be issued when they occur during the time period identified as off shift.

Note: Shift times and days of the week are set on the IEMSET command. See option #9 on the INSTALL menu.

Notification address See the Notification Address(s) section of this manual on page 5.

There are two optional parameters that you can access using the F10 function key as follows:

Watch name Earlier versions of iEventMonitor used a job name that included the user profile when they were active. This has been changed to provide you with the following options:

*USER The job that iEventMonitor uses for this user profile watch will run with a job name of the user profile being watched.

*GEN The job that iEventMonitor uses for this user profile watch will run with a generated job name in the form of UWnnnnnn where nnnnnn is a sequential number assigned by the software at each job start. Each time the watch is started, a different job name will be used.

Name The job that iEventMonitor uses for this user profile watch will run with a job name entered here.

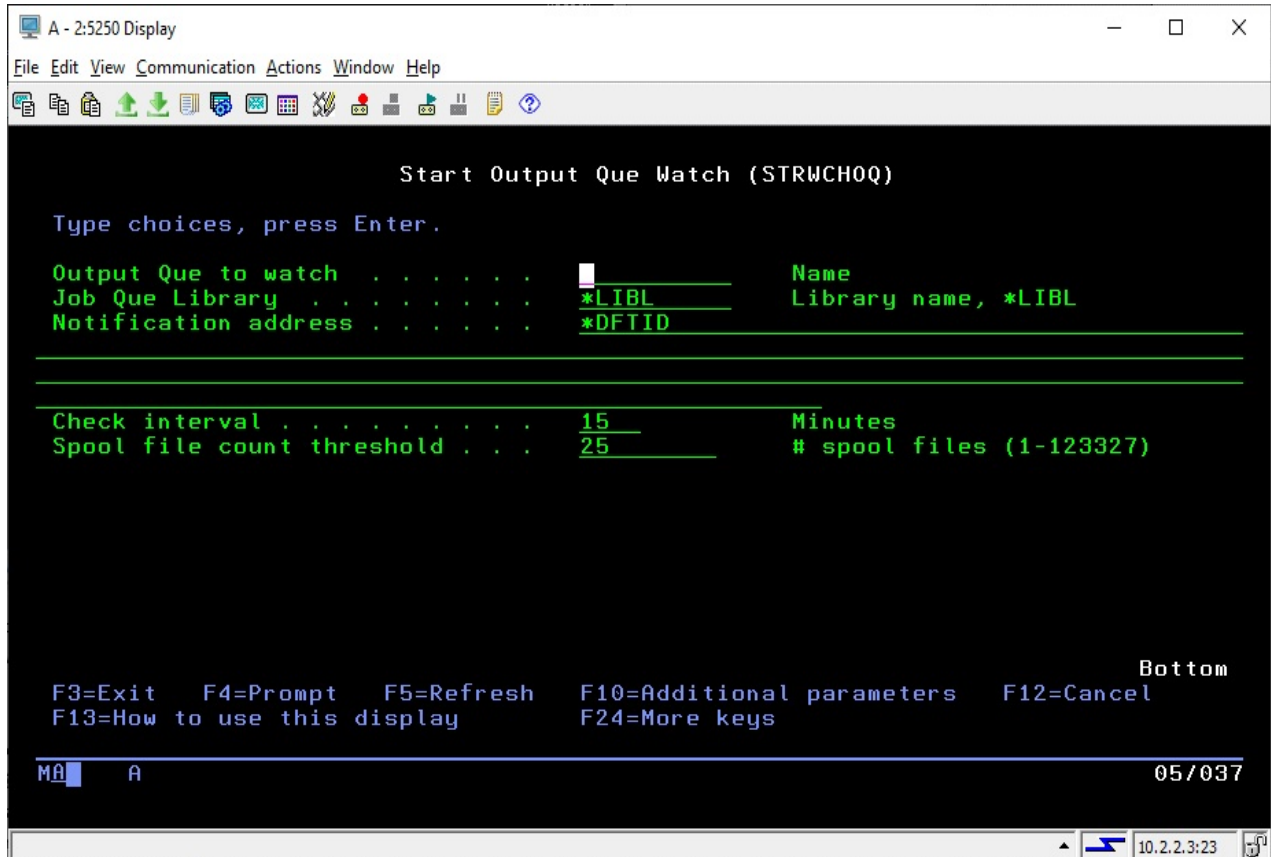
Alert Subject Text iEventMonitor will issue an alert with the default subject text if you leave this set to *DFT. If you want a unique alert subject text used, enter that value here and it will be used if an alert is issued.

Once a user profile watch has been started, whenever the user profile is used for an interactive logon or whenever an interactive session for the user ends, an alert will be generated.

Output Queue Watch

iEventMonitor can watch an output queue for unprocessed spool files in ready status. When the number of spool files exceeds a threshold value that you set when the watch is started, an alert will be issued.

To start an output queue watch, run option 7 from the WATCH menu or just issue the STRWCHOQ command. The following prompt will be shown:



Enter the parameters as follows:

Output Que to watch	Enter the name of the output queue that you want to watch.
Job Que Library	Enter the name of library where the output queue is located.
Notification address	See the Notification Address(s) section of this manual on page 5.
Check interval	Enter a value, in minutes, that indicates how frequently you want to check the output queue. The default value is 15 minutes but you can specify as low as 1 and as high as 999, but 15 minutes is a good setting to start with.
Spool file count threshold	Enter the spool file threshold that you want checked. When the number of spool files in ready status waiting to be

processed exceeds this value during a check cycle, then an alert will be issued. Any value up to 123,327 can be used.

There are two optional additional parameters available. To access these additional settings, press the F10 key and the following will be prompted:

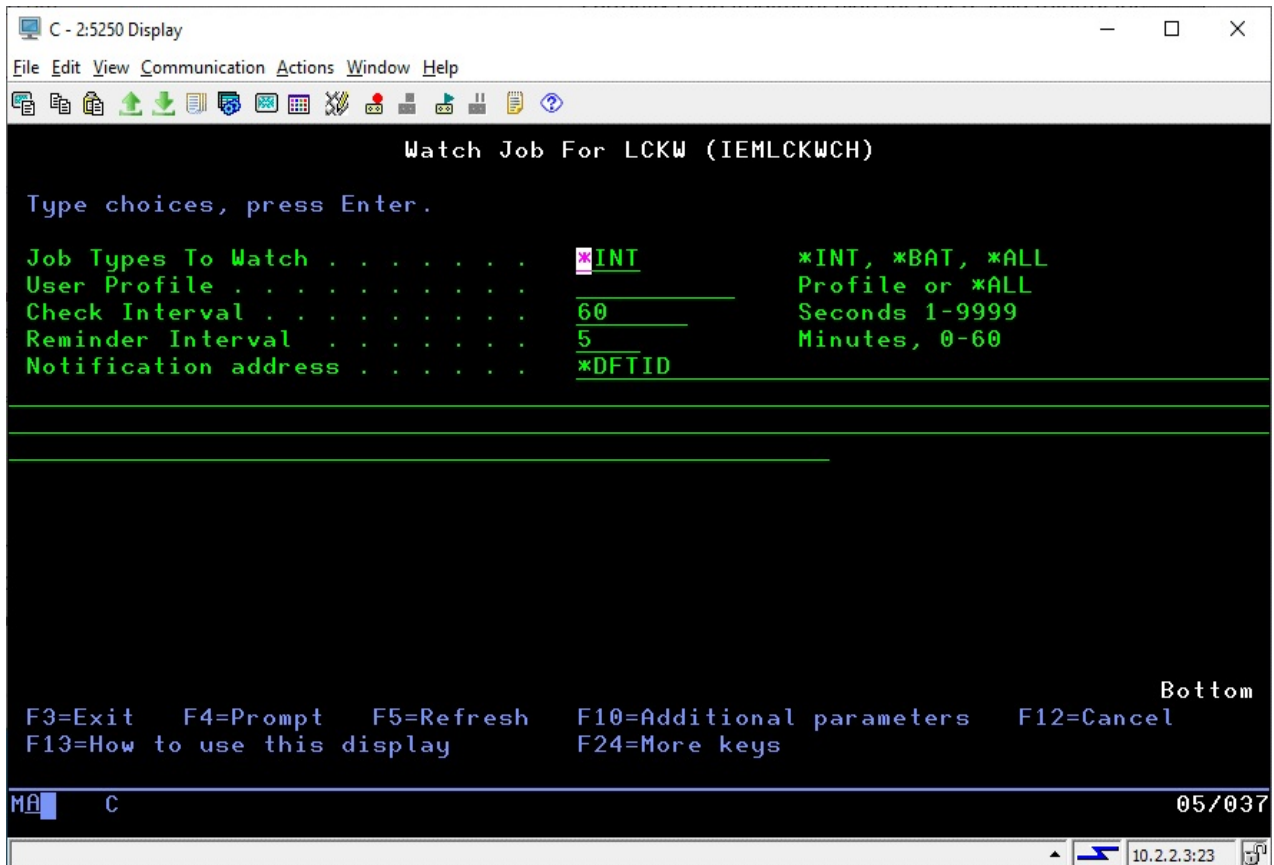
Include Holds?	The default value of *NO will exclude reports that are on hold in the output queue from being counted. By changing this to *YES, reports that are on hold will be included along with those that are ready to print.
Alert Subject Text	iEventManager will issue an alert with the default subject text if you leave this set to *DFT. If you want a unique alert subject text used, enter that value here and it will be used if an alert is issued.

Press ENTER to start the output queue watch. Whenever the number of spool files waiting to be processed exceeds the level that you set, an alert will be issued. This can be helpful with an output queue where the printer should always be active or for an output queue that is being monitored automatically for output email processing or spool file conversion processing. When spool files start to stack up, iEventManager will alert you.

Lock Wait Watch

This feature watches for Lock Wait status (LCKW) to be reported for a job running for the indicated type and user profile. Once the task has reported LCKW status for a full interval specified, then an alert will be issued.

To start a Lock Wait Watch, run option 8 on the WATCH menu or use the IEMLCKWCH command. The following screen will be prompted:



Fill in the parameters as follows:

Job Types To Watch

Indicates the type of jobs to be watched on your system.

Choose one of the following values:

*INT Just check for lock waits on interactive jobs.

*BAT Just check for lock waits on batch jobs.

*ALL Check for lock waits on all jobs.

User Profile

You can check for lock waits for a specific user profile or *ALL user profiles.

Check Interval	Enter how frequently you want to check for jobs in lock wait status, expressed in seconds.
Reminder Interval	Enter the number of minutes that you want to lapse before a reminder alert is sent after an initial alert has been issued. If you enter the value of zero, then a reminder will be sent for each INTERVAL value seconds that you have set in the previous parameter setting.
Notification address	See the Notification Address(s) section of this manual on page 5.

Using the F10 function key will display an additional parameter as follows:

Alert Subject Text	iEventMonitor will issue an alert with the default subject text if you leave this set to *DFT. If you want a unique alert subject text used, enter that value here and it will be used if an alert is issued.
--------------------	---

Once a task has been found to be in LCKW status, the watch will wait for the period of time specified by the REMIND parameter and then check again. If the job persists in LCKW status, it will issue the alert again. This will continue until the LCKW status is resolved. If a reminder setting of zero is used, the reminder alerts will be issued for every check interval.

When a Lock Wait Watch job is started, it will be logged into the list of iEventMonitor tasks (option 1 on the MASTER menu). Once this has been done, then the STRIEM and ENDIEM commands can be used to start and end this task along with all other listed iEventMonitor tasks.

Excluding Jobs From Lock Wait Watch

Some customers using this watch report that lock waits occur regularly on their system and they are expected, so they would like to have the ability to ignore certain lock wait alerts. iEventMonitor can now ignore lock wait alerts issued for certain specific jobnames. This ignore feature has a capacity for specifying up to 20 jobnames to be ignored.

To activate this feature, you need to create a special data area in the iEventMonitor application library. You can create the data area using the following command:

```
CRTDTAARA DTAARA(IEMLIB/LCKWOK) TYPE(*CHAR) LEN(200) VALUE(' ')
TEXT('Optional Lock-Wait Ignore List')
```

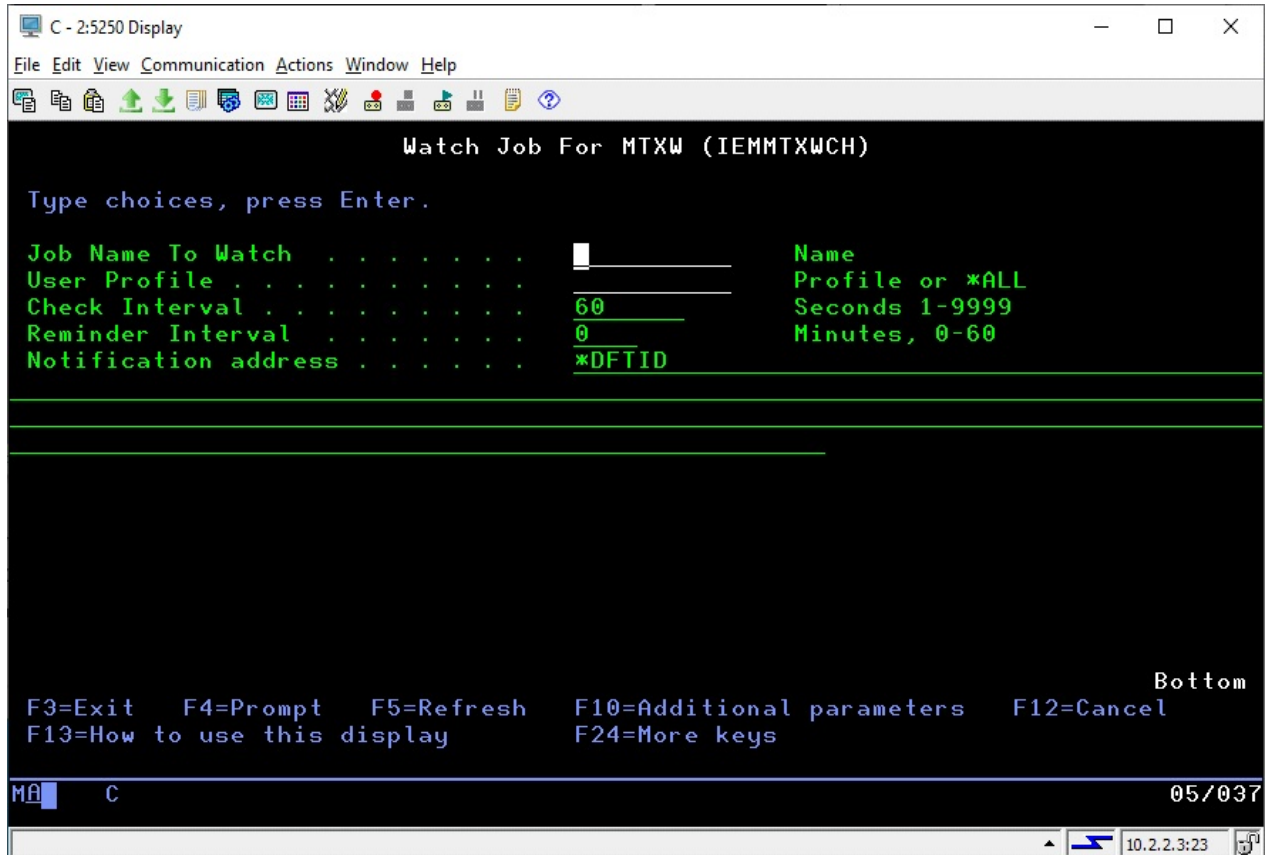
Once the data area has been created, you can specify up to 20 jobnames that you want iEventMonitor to ignore for lock wait alerts. The jobnames are stored every 10 characters in the data area. Do not leave any 10 character slot blank as the process will stop checking once it finds a 10 character slot that is blank. The entries do not need to be in any particular sequence.

After the data area has been created and populated with jobnames, then the next time the lock wait watch starts on your system, any lock wait conditions that happen in a job that is in the data area will be ignored for alert posting purposes.

Mutex-Wait Watch

This feature watches for Mutex Wait status (MTXW) to be reported for a specified job running for a specific user profile. Once the task has reported MTXW status for a full interval specified, then an alert will be issued.

To start a Mutex Wait Watch, run option 9 on the WATCH menu or use the IEMMTXWCH command. The following screen will be prompted:



Enter the parameters as follows:

Job Name To Watch	Enter the specific job name that you want to watch. If there are multiple jobs with the same name, all of them will be watched.
User Profile	Enter the specific user profile that started the job you want to watch. If you want to watch all instances of the requested job name, use the special value of *ALL .
Check Interval	Enter how frequently you want to check for the job showing the MTXW status, in seconds. The default value of 15 seconds is a good starting point.
Reminder Interval	Enter the number of minutes that you want to lapse before a reminder alert is sent after an initial alert has been issued. If

you enter the value of zero, then no reminder alerts will be issued.

Notification address See the Notification Address(s) section of this manual on page 5.

Using the F10 function key will display an additional parameter as follows:

Alert Subject Text iEventManager will issue an alert with the default subject text if you leave this set to *DFT. If you want a unique alert subject text used, enter that value here and it will be used if an alert is issued.

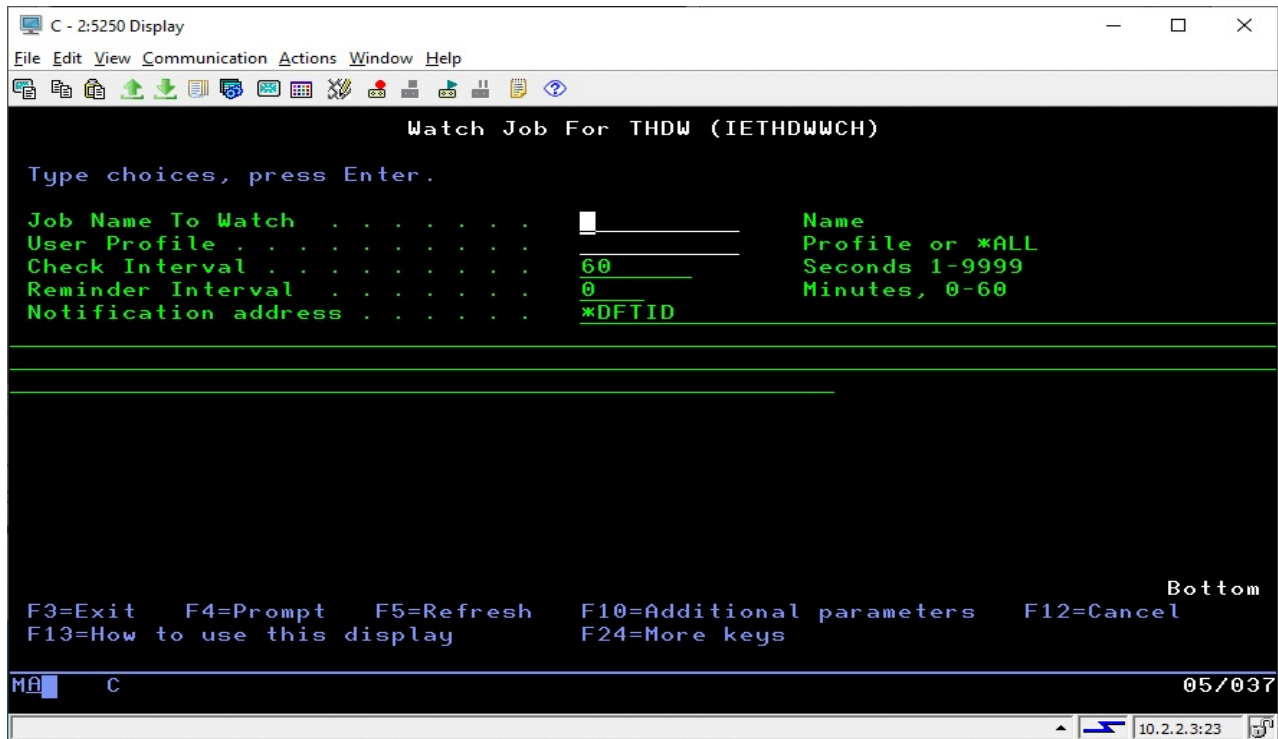
To start the MTXW watch, press ENTER when all parameters have been set. Whenever a requested job enters MTXW status, iEventManager will note that and then check again at the next requested interval. If it remains in MTXW status, then an alert will be issued. If a reminder is specified, then reminder alerts will be issued with the frequency specified on that setting.

When a Mutex Wait Watch job is started, it will be logged into the list of iEventManager tasks (option 1 on the MASTER menu). Once this has been done, then the STRIEM and ENDIEM commands can be used to start and end this task along with all other listed iEventManager tasks.

Thread Wait Watch

This feature watches for Thread Wait status (THDW) to be reported for a job running for the indicated type and user profile. Once the task has reported THDW status for a full interval specified, then an alert will be issued.

To start a Thread Wait Watch, run option 10 on the WATCH menu or use the IEMTHDWCH command. The following screen will be prompted:



Fill in the parameters as follows:

Job Name Watch	Enter the specific job name that you want to watch. If there are multiple jobs with the same name, all of them will be watched.
User Profile	You can check for thread waits for a specific user profile or *ALL user profiles.
Check Interval	Enter how frequently you want to check for jobs in thread wait status, expressed in seconds.
Reminder Interval	Enter the number of minutes that you want to lapse before a reminder alert is sent after an initial alert has been issued. If you enter the value of zero, then a reminder will be sent for each INTERVAL value seconds that you have set in the previous parameter setting.
Notification address	See the Notification Address(s) section of this manual on page 5.

Using the F10 function key will display an additional parameter as follows:

Alert Subject Text iEventManager will issue an alert with the default subject text if you leave this set to *DFT. If you want a unique alert subject text used, enter that value here and it will be used if an alert is issued.

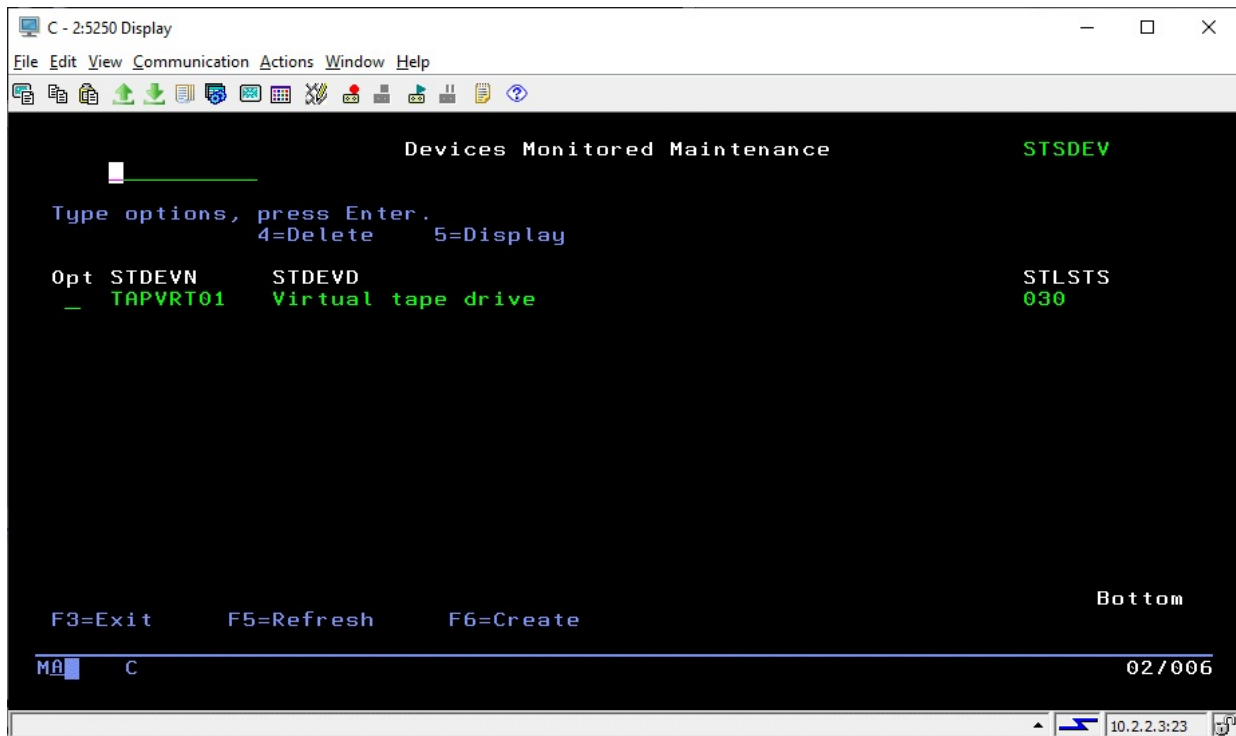
Once a task has been found to be in THDW status, the watch will wait for the period of time specified by the REMIND parameter and then check again. If the job persists in THDW status, it will issue the alert again. This will continue until the THDW status is resolved. If a reminder setting of zero is used, the reminder alerts will be issued for every check interval.

When a Thread Wait Watch job is started, it will be logged into the list of iEventManager tasks (option 1 on the MASTER menu). Once this has been done, then the STRIEM and ENDIEM commands can be used to start and end this task along with all other listed iEventManager tasks.

Device Watch

This feature watches for specific devices on your system and will issue an alert when a specified device is not in a useable state. This feature is implemented on the WATCH2 menu as options 1 and 2.

Before you can use this watch, you must first let iEventManager know which specific devices that you want to watch. This is done using option #1 on the WATCH2 menu or by using the WRKDEVWCH command in library IEMLIB. When you start this command, the following will be shown:



Options on this display will let you view details for the device status (option 2) or delete the device from the list (option 4).

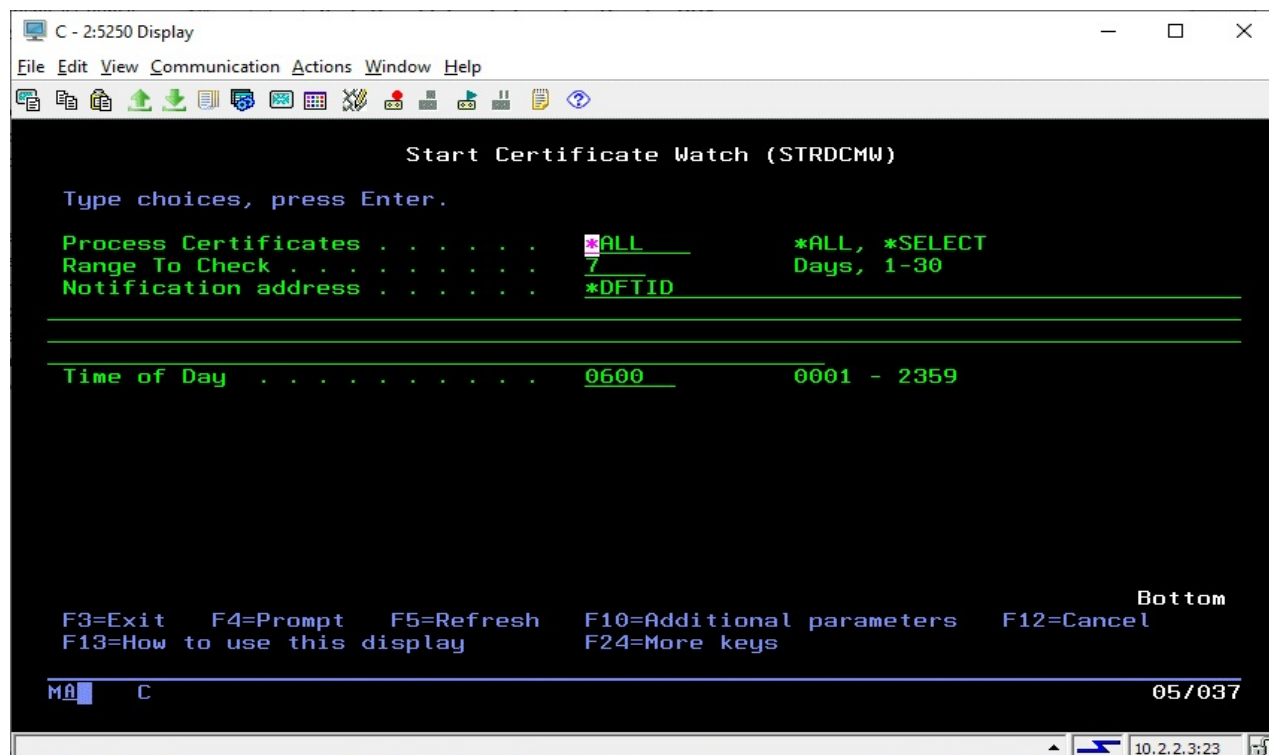
To add a new device, use the F6 function key and the display on the following page will be shown:

Fill in the parameters as follows:

- | | |
|----------------------|---|
| Range To Check | Enter a value that represents how often you want the Device Watch to run. The value entered will be the number of minutes. |
| Notification address | See the Notification Address(s) section of this manual on page 5. |
| Alert Subject Text | iEventManager will issue an alert with the default subject text if you leave this set to *DFT. If you want a unique alert subject text used, enter that value here and it will be used if an alert is issued. |

Certificate Watch

This feature scans the digital certificates on your system once per day and issues an alert when one or more will expire within a specified period of time from when the scan is run. To start the Certificate Watch, use option #3 on the WATCH2 menu. The following display will be shown:



Fill in the parameters as follows:

- | | |
|----------------------|---|
| Process Certificates | Choose one of the following options:
*ALL All certificates will be checked for expiration.
*SELECT Only the certificate that you have specified in the certificate selection process will be checked. |
| Range To Check | Enter a value that represents how many days until the expiration date that you want to receive an alert. |
| Notification address | See the Notification Address(s) section of this manual on page 5. |
| Time of Day | Enter time of day when you want this watch to run. When you start the watch, it will run immediately. Once it has been started, then it will run once per day at the time that you specify. |

Using the F10 function key will display an additional parameter as follows:

- | | |
|--------------------|---|
| Alert Subject Text | iEventManager will issue an alert with the default subject text if you leave this set to *DFT. If you want a unique alert subject text used, enter that value here and it will be used if an alert is issued. |
|--------------------|---|

Important Note: This feature will only work if your system is running IBM i OS release level 7.3 or newer and you have the most recent technology release from IBM installed.

Certificate Selection

If you want to limit the certificate watch to only certain certificates, you can do so by using the *SELECT option on the watch. To specify which certificates to include, use option 3 on the WATCH2 menu to create and maintain the list of certificates to be checked for expiration. When you start the process, the following will be shown:

```
Maintain Selected Digital Certs          DCMSEL
-----
Type options, press Enter.
 4=Delete   5=Display

Opt Certioficat Name

F3=Exit   F5=Refresh   F6=Create          Bottom
```

From this display you can add certificates, remove certificates or view the certificate entries. When a certificate is added, the user profile that added the certificate is captured for reference purposes.

Use the F6 option to create new entries.

```
ADD                               Maintain Selected Digital Certs          DCMSEL

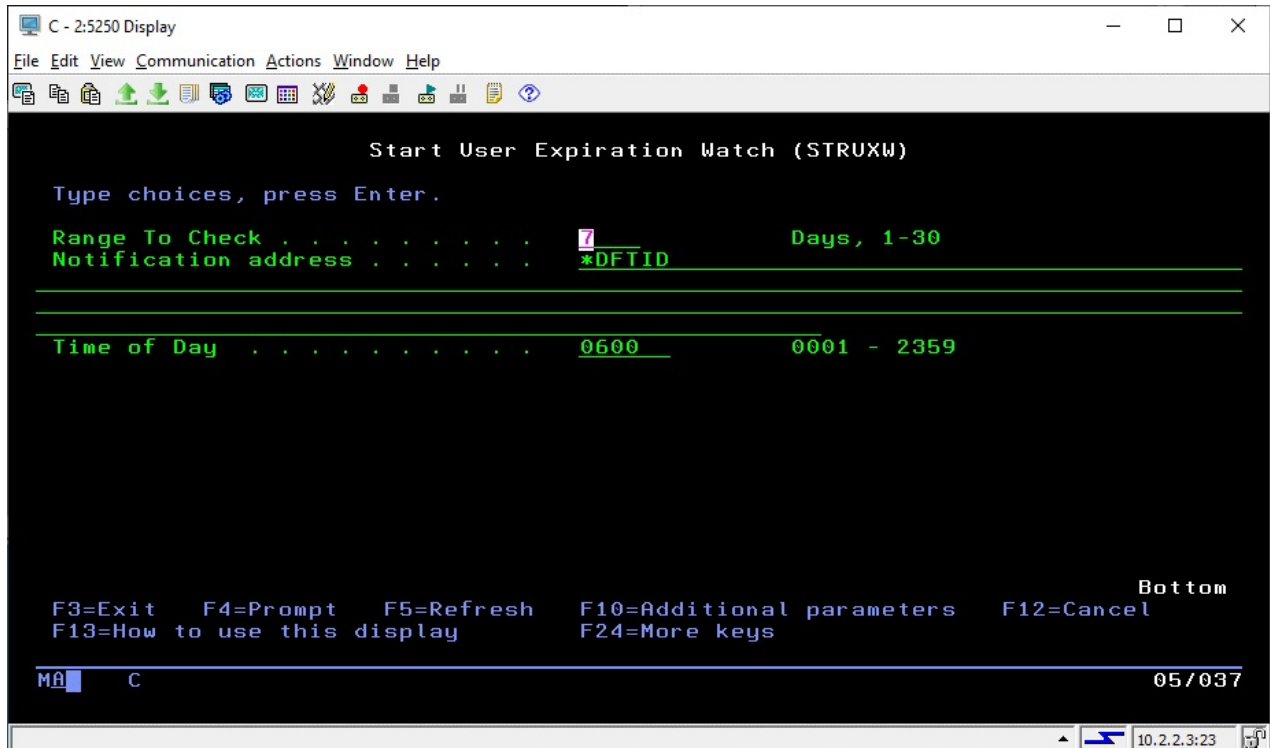
Type information, press Enter.
Selected Cert. . 
-----
Created By . . .
Created Date . .

F3=Exit      F5=Refresh      F12=Cancel
```

Enter the name of your certificate and press ENTER to record it. Keep in mind that the certificate name is case sensitive.

User Profile Expiration Watch

This feature scans the active user profiles on your system once per day and issues an alert when one or more will expire within a specified period of time from when the scan is run. To start the User Profile Expiration Watch, use option #4 on the WATCH2 menu. The following display will be shown:



Fill in the parameters as follows:

- | | |
|----------------------|---|
| Range To Check | Enter a value that represents how many days until the expiration date that you want to receive an alert. |
| Notification address | See the Notification Address(s) section of this manual on page 5. |
| Time of Day | Enter time of day when you want this watch to run. When you start the watch, it will run immediately. Once it has been started, then it will run once per day at the time that you specify. |

Using the F10 function key will display an additional parameter as follows:

- | | |
|--------------------|---|
| Alert Subject Text | iEventManager will issue an alert with the default subject text if you leave this set to *DFT. If you want a unique alert subject text used, enter that value here and it will be used if an alert is issued. |
|--------------------|---|

Network Functions

iEventManager includes features to watch network connections to your IBM i system. A Network Watch will periodically test the connection to a remote system to make sure that it is active. If the connection goes inactive or there are problems detected on the connection, an alert will be issued. A Connection Watch will check for incoming connections established and can alert you about connections from untrusted locations.

The NETWATCH menu supports this feature:

```

C - 2:5250 Display
File Edit View Communication Actions Window Help
NETWATCH
NETWATCH Menu
iEventManager Network Watch Menu

1. Maintain Network Locations WRKNETW
2. Start Network Watch STRNETW

6. Work With Connection IP Addresses WRKCNNR
7. Start Connection Watch STRCNNW

10. To MASTER Menu
(c) 2015-2024 Kisco Systems LLC
Selection or command
===>
MA C 22/007
10.2.2.3:23

```

The menu options are as follows:

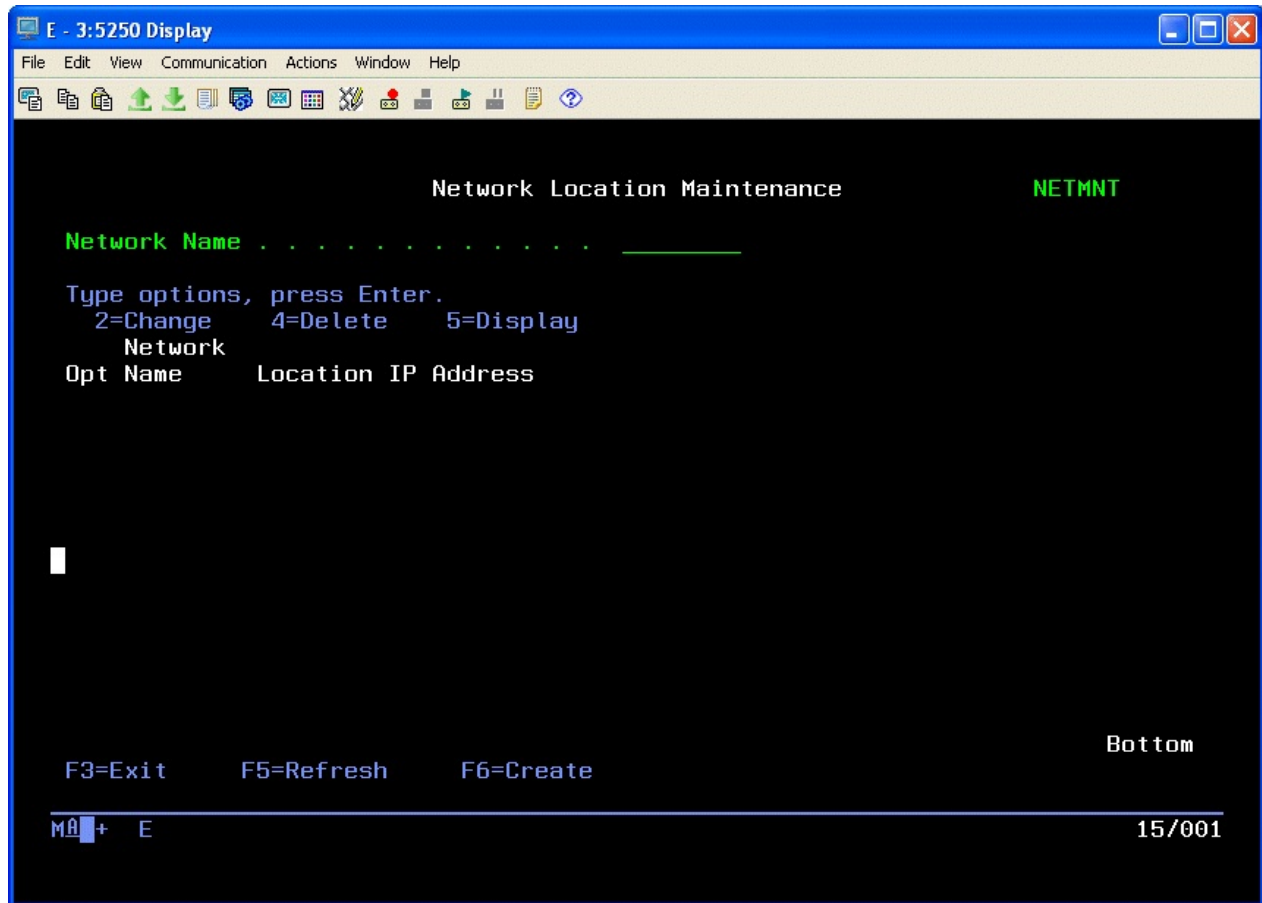
- | | |
|--------------------------------------|---|
| 1. Maintain Network Locations | Maintain a list of network locations that can be used for monitoring. |
| 2. Start Network Watch | Starts a Network Watch for a registered locations. |
| 6. Work With Connection IP Addresses | Work with valid connection IP addresses |
| 7. Start Connection Watch | Start the Connection Watch feature |

Each of these menu options is discussed in this section of the user's guide.

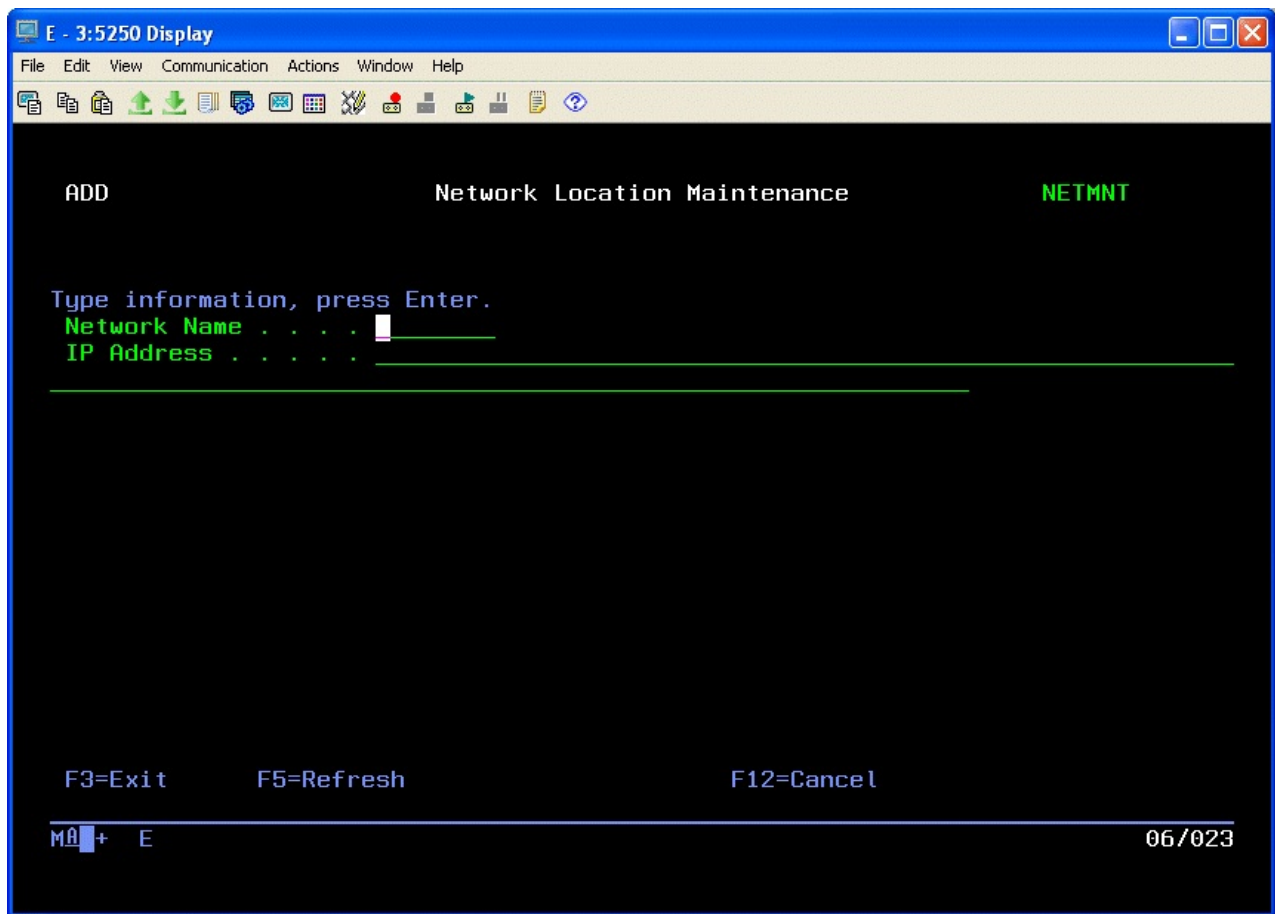
Maintain Network Locations

iEventMonitor's network location watch can issue an alert when a connection that you depend on is not working or is reporting lost packets or other interruptions.

Before a network location can be watched, it has to be defined to iEventMonitor. Using option #1, you can create a record for each network address that you want to be able to watch. When you start option #1, the following screen will be displayed:



Use the F6 function key to add a new entry to the list of network connections to be monitored.



When you add a record to the Network Location file, you assign a unique short, 8 character, name to the location and then associate that with a specific IP address. The IP address can be either a numeric address such as "10.1.2.3" or a named address such as companyname.com.

Enter the values as follows:

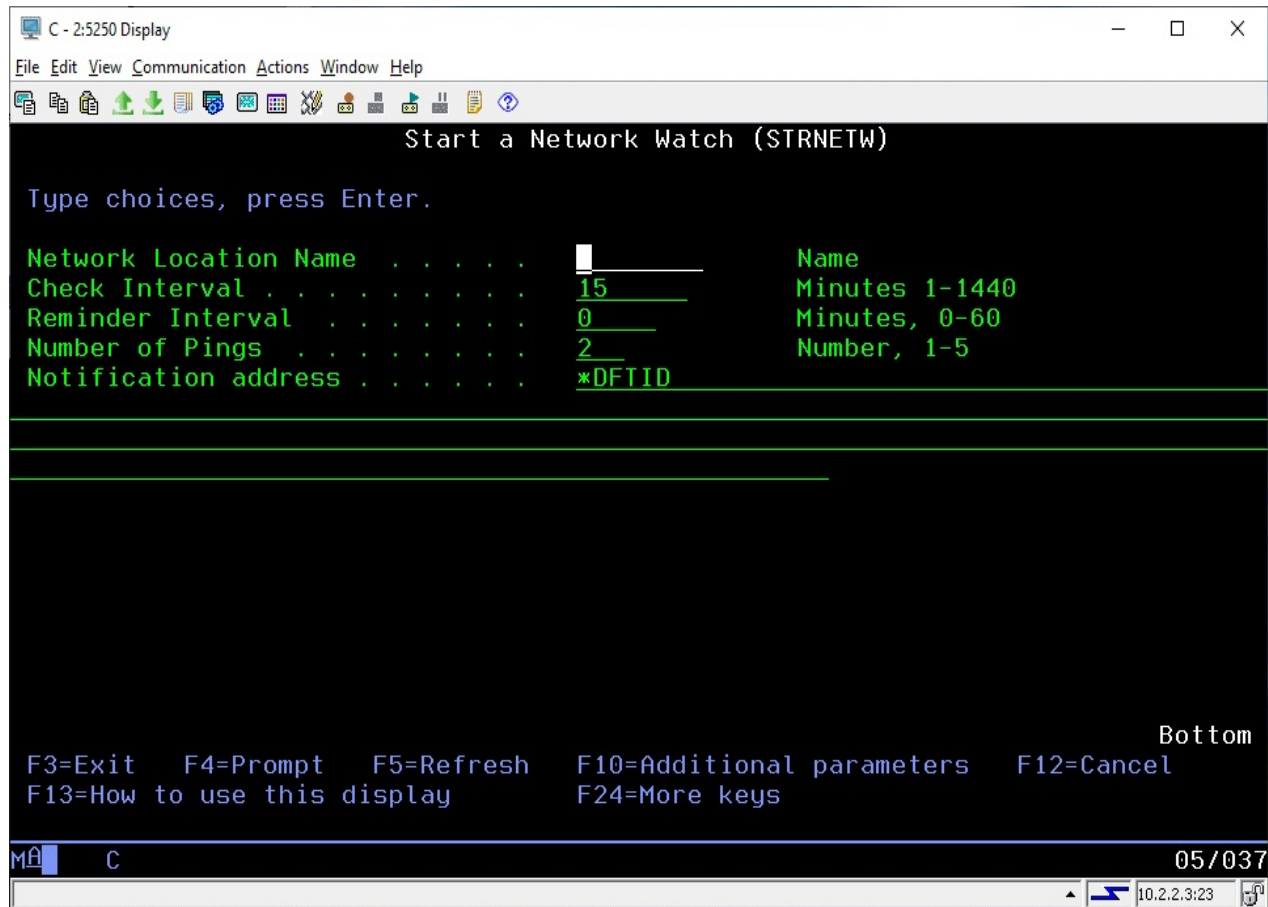
Network Name Enter the unique 8 character name you have assigned to the network location to be monitored.

IP Address Enter the IP address to be monitored.

When you create an entry, the IP address will be validated. If the address cannot be validated, the entry cannot be completed.

Start Network Watch

Once a location has been added to the Network Location file, you can then start a monitor for it using option #2 or the STRNETW command. The parameters for this command are as follows:



Fill in the parameters as follows:

Network Location Name	Enter the 8 character network name that was created in the Network Locations list using option #1 on the NETWATCH menu. A Network Watch can only be run for a location established on this list.
Check Interval	Enter how frequently you want iEventManager to check the network connection in minutes.
Reminder Interval	If you want delayed reminders issued when a problem is found, enter that delay time here in minutes. An entry of zero will cause the alerts to be re-issued based on the INTERVAL setting.
Number of Pings	Enter the number of remote pings that you want iEventManager to use when checking the network connection. We recommend a minimum setting of at least 2.

Notification address See the Notification Address(s) section of this manual on page 5.

Using the F10 function key will display an additional parameter as follows:

Alert Subject Text iEventManager will issue an alert with the default subject text if you leave this set to *DFT. If you want a unique alert subject text used, enter that value here and it will be used if an alert is issued.

After you start the Network Watch, the IP address will be tested immediately. If it passes, then it will be re-tested following each Check Interval time period. If a problem is found, an alert will be issued. If the Reminder Interval is left as zero, then each subsequent Check Interval will also issue an alert until the network connection resumes working normally. If you want to delay subsequent alerts, use the Reminder Interval setting. For example, you can check a location every 15 minutes (Check Interval = 15), but if a problem is found, only issue a subsequent alert once an hour (Reminder Interval = 60).

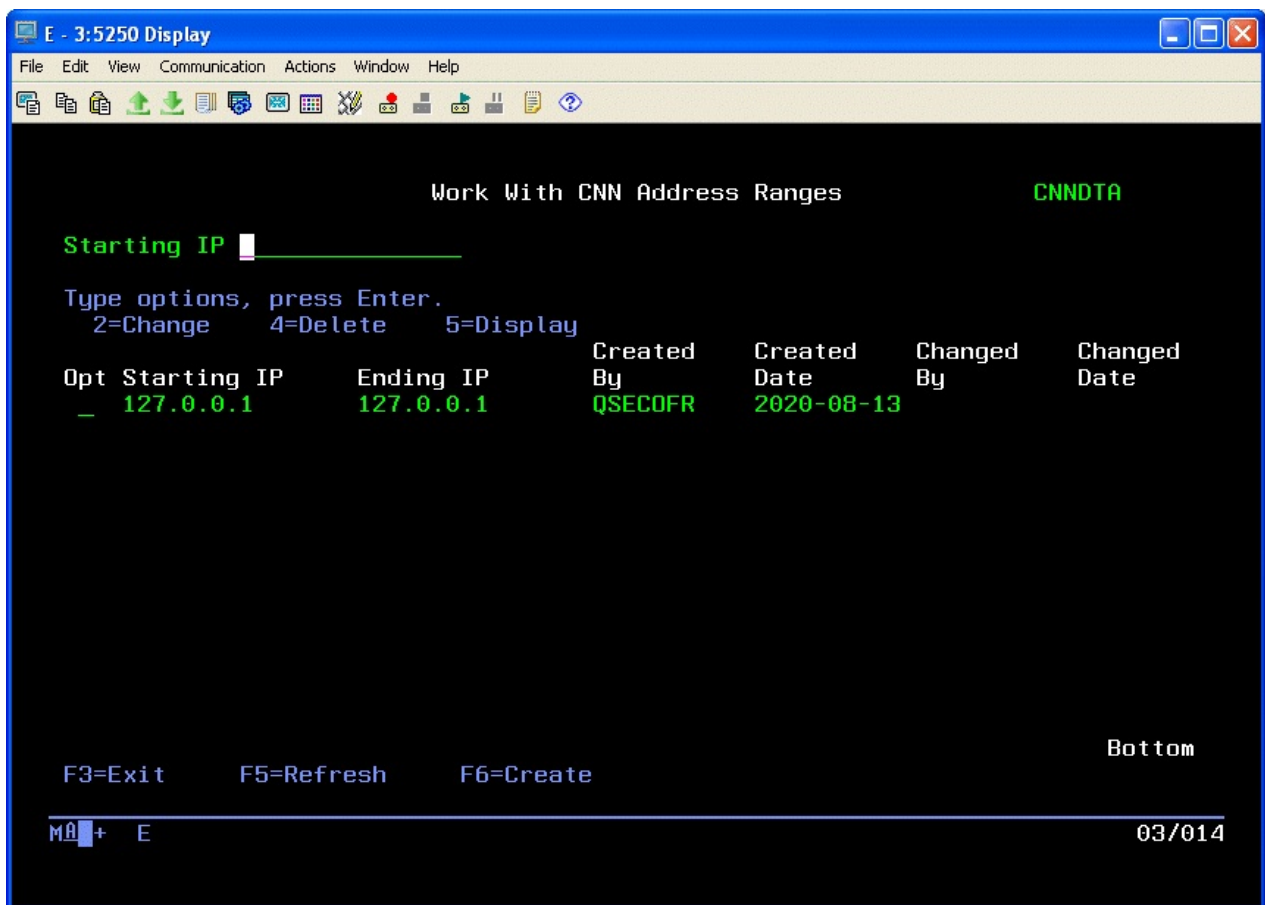
Once a Network Watch has been set, you can end it without removing it using the ENDIEM command. It will be automatically restarted the next time you use the STRIEM command. You can also manage the Network Watch using the WRKIEM (option #1 on the MASTER menu) function.

Connection Watch

iEventManager includes a feature that lets you watch for "foreign" systems connecting to your system via network connections. It allows you to define the specific IP addresses that are allowed to connect and only issues alerts when a system not authorized tries to establish a connection.

The Connection Watch includes an optional Exit Program feature. Using this exit program, you can code your own program to deal with questionable network connection attempts. There are no parameters in the call to your exit program, but when it starts running, a physical database file will be present in the QTEMP library named UTIL30. This file will contain one record for each IP address included in the current alert. Your exit program can take any additional actions you may want to take including cancelling the connection using the ENDTCPN command. You will find a source physical file name QSAMPLE in the application library IEMLIB that contains a sample CL program named CNNEXIT that you can use to see how your own exit program might be implemented. We recommend that you develop and store your exit program in a library other than IEMLIB as a future upgrade from Kisco could remove your program from the system.

Option #6 on the NETWATCH menu will let you maintain a list of IP addresses that you recognize as being legitimate for your system. When start this option, the following display will appear:

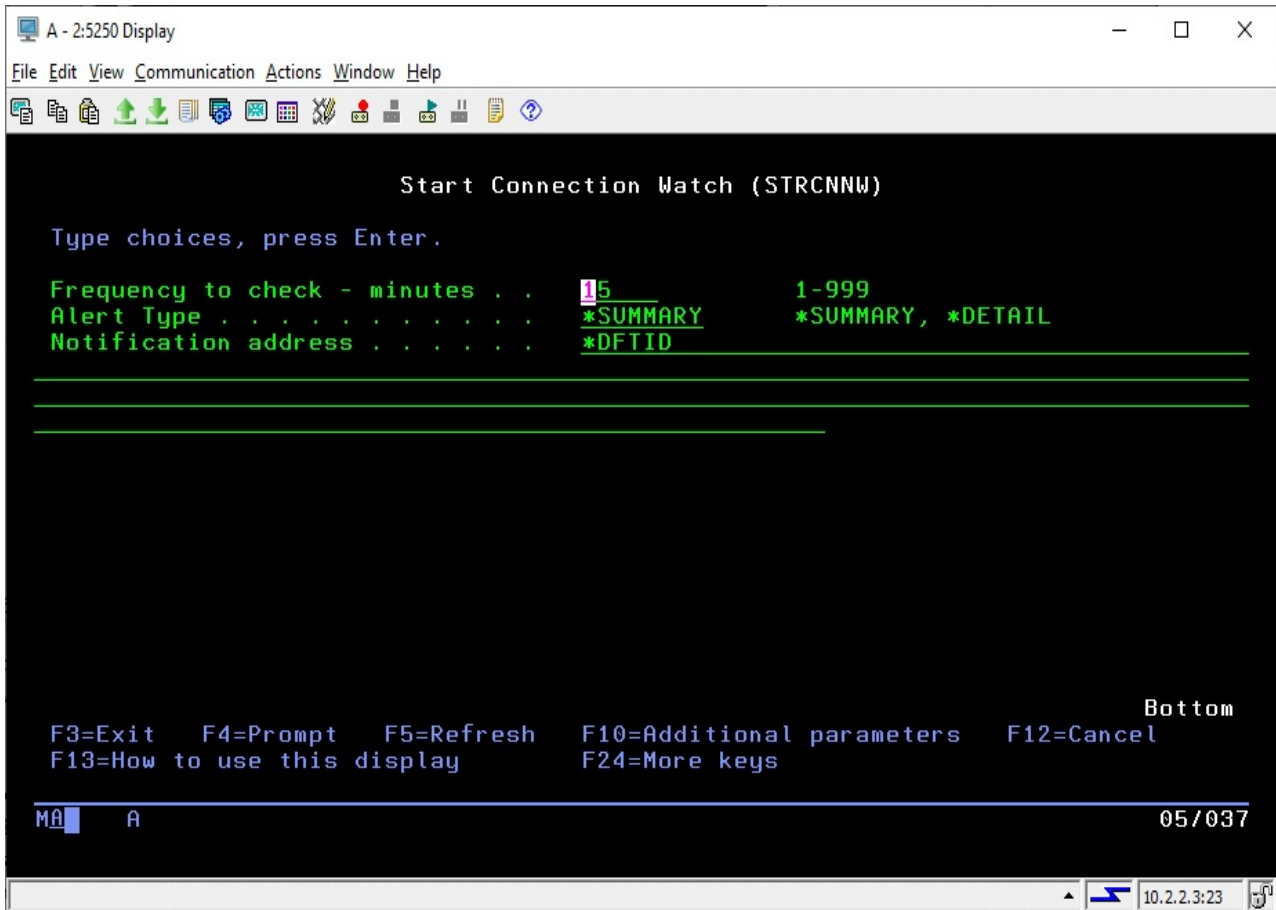


When the Connection Watch runs, it will check the active external connections to your system against this list and ignore any that are included in the list.

For example, if you use menu option #6 to define a range of IP addresses from 10.1.1.1 to 10.1.1.255, then all of those addresses will be considered to be valid when they connect to your system. Any other addresses will result in an alert.

Note that the entry for 127.0.0.1 should be included in this list for all systems.

To start a Connection Watch, use menu option #7 or use the STRCNNW command. The following display will appear:



Enter the parameters as follows:

Frequency to check - minutes

Enter a value that represents how often you want the Connection Watch to check for current connections. The value entered will be the number of minutes.

Alert Type

Controls the type of alerts that will be issued.

Choose one of the following values:

*SUMMARY

When the Connection Watch runs, if any questionable connections are found, they will be placed into a listing and sent as an email attachment. Kisco recommends

that you use the *SUMMARY option when first starting to work with the Connection Watch feature.

***DETAIL**

A separate alert notice will be issued for each questionable connection found when the Connection Watch runs. If none are found, no alert will be issued. See the Notification Address(s) section of this manual on page 5.

Notification address

When you press the F10 key, you will see the following three additional parameters:

Alert Subject Text

iEventManager will issue an alert with the default subject text if you leave this set to *DFT. If you want a unique alert subject text used, enter that value here and it will be used if an alert is issued.

Exit program

If you want to call your own exit program during alert processing, enter the name of the program here. When a Connection Watch alert is issued, your program will be called for any additional processing that you may want to do. When the exit program is called, a database file will be available in the QTEMP library for the program session. The file will be named UTIL30 (a shell version of this file is in the IEMLIB library). This file will contain one record for each IP address included in the current alert. Your exit program can take any additional actions you may want to take including cancelling the connection using the ENDTCPCNN command. You will find a source physical file name QSAMPLE in the application library IEMLIB that contains a sample program named CNNEXT that you can use to see how your own exit program might be implemented. We recommend that you develop and store your exit program in a library other than IEMLIB as a future upgrade from Kisco could wipe your program from the system.

If you do not want to call an exit program, use the default value of *NONE.

Exit program library

If you are using an exit program, enter the name of the library where your exit program is stored.

Send alerts

When you use an exit program, you can use this option to suppress the alerts issued automatically by iEventManager. This could be done to allow your exit program to decide whether or not the alert needs to be issued.

Once you have started the Connection Watch, you can monitor it using option #1 on the MASTER

menu. It will be the CN type entry. From there you can stop it, change the settings and restart it. As long as it appears in this list, it will start whenever you run the STRIEM command and it will end using the ENDIEM command.

Audit Functions

iEventMonitor has the ability to monitor your system for security events getting logged to the system security audit journal. You can set up audit monitors for one or more of specific security events. For each audit monitor, you can also specify how frequently you want the check for the audit journal entries.

The IBM i/OS contains extensive audit logging capabilities for security related events on your system. Before you can start checking for these events, the system audit function needs to be activated. In fact, it may already be active on your system. To test this, just run the following command from the command line:

```
DSPJRN JRN(QAUDJRN)
```

If information is displayed on the screen, then the system audit journal already exists on your system. If not, it needs to be created. You can do this by running the following two commands from the command line:

```
CRTJRNRCV JRNRCV(QGPL/AUDRCV0001) THRESHOLD(100000)
AUT(*EXCLUDE) TEXT('Auditing Journal Receiver')
```

```
CRTJRN JRN(QSYS/QAUDJRN) JRNRCV(QGPL/AUDRCV0001)
MNGRCV(*SYSTEM) DLTRCV(*NO) AUT(*EXCLUDE)
TEXT('Auditing Journal')
```

This process will create the initial journal receiver and then the associated journal.

Once you have either verified that the system security journal exists or you have created it, then you will need to activate the journal features that you are interested in tracking using iEventMonitor.

iEventMonitor can issue alerts for the following audit events on your system:

<u>Audit Code</u>	<u>Description</u>
AD	Audit changes
AF	Authority failures
AX	Row and column access control
CD	Command line use for registered user profiles
CP	User profiles changed, created or restored
DS	DST password reset
EV	System environment variables
OW	Object ownership changes
PS	Profile swaps
PW	Invalid passwords
SK	Secure socket connections
SO	Server security user information actions
ST	Use of service tools
SV	System value changes

To make sure that the items above are correctly captured in the security audit journal, certain system values need to be set. Use the following command to display the specific system values that you will need to work with:

```
WRKSYSVAL SYSVAL(QAUD*)
```

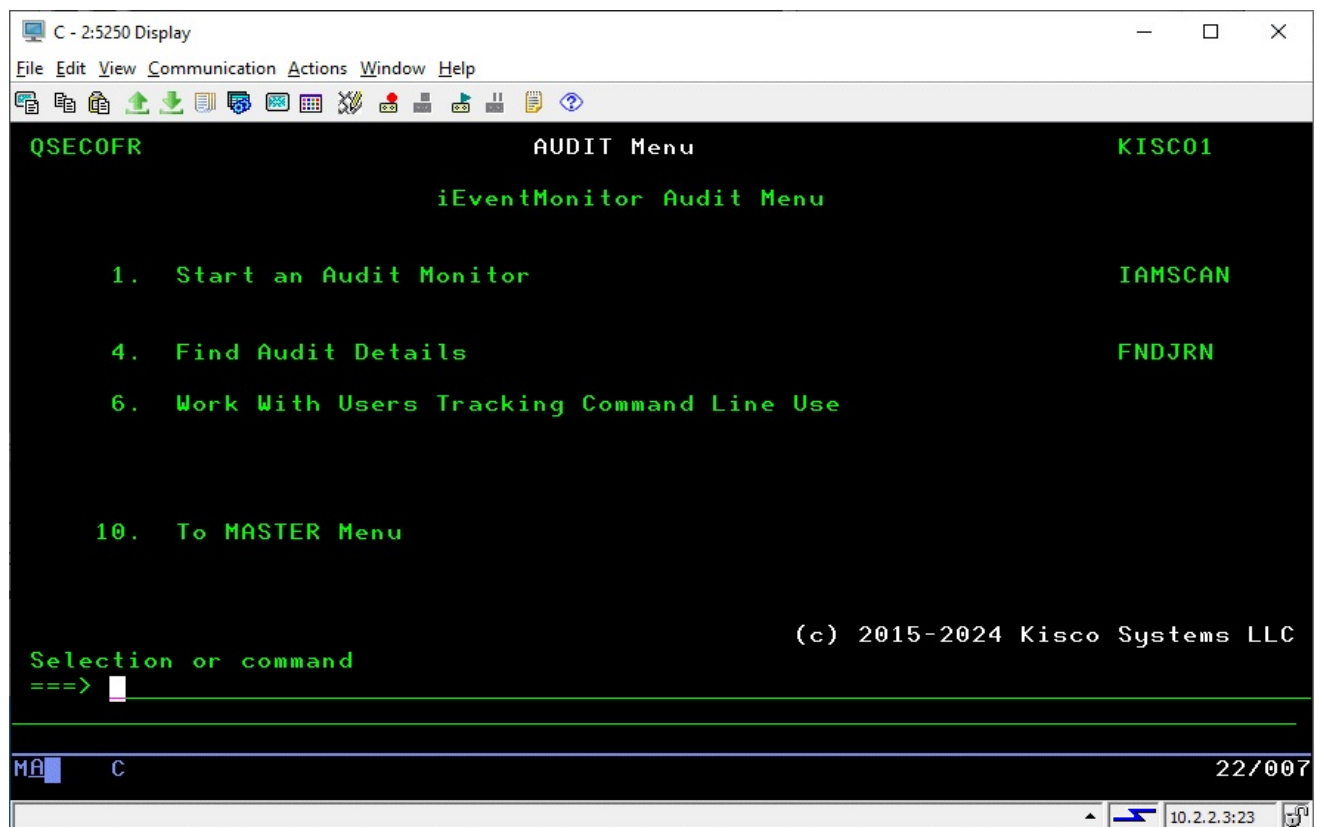
This will display the system values that are used to control audit journals. Under the QAUDCTL system value, you must have the setting of *AUDLVL set. In the QAUDLVL system value, you should have a minimum of the *AUTFAIL and *SECURITY settings. If you want to track object deletes using iEventMonitor, you will also have to add the *DELETE setting.

If you are new to using the system security audit journal, keep in mind that as the journal receivers fill up, they are periodically detached and a new journal receiver is created. Over time, these receivers may end up taking up a lot of space on your system. If you are running iEventMonitor for reporting on events, only the most recent receiver or two will be used. Unless you need the older receivers for other purposes, they can be periodically removed from your system. You can check to see if there are journal receivers to be deleted using this command:

```
WRKOBJ OBJ(QGPL/AUD*)
```

The AUDIT Menu

The AUDIT menu controls all of the iEventMonitor audit functions:



The options on the menu are as follows:

- | | |
|---------------------------|---|
| 1. Start an Audit Monitor | Starts a specific system security audit monitor task |
| 4. Find Audit Details | Used to drill down and find more details about a specific audit event that was reported by iEventMonitor. |

6. Work With Users Tracking
Command Line Use

Register and un-register user profiles for command line use tracking purposes.

Starting an Audit Monitor

To start an audit monitor task, select menu option #1 from the AUDIT menu or you can use the use the IAMSCAN command in library IEMLIB. The following will be displayed:

```

C - 2:5250 Display
File Edit View Communication Actions Window Help
Audit Scan (IAMSCAN)
Type choices, press Enter.
Audit Code . . . . . AE
Minutes . . . . . 15
Notification address . . . . . *DFTID
Start option . . . . . *RESTART
Attachment format . . . . . *TXT
Include option . . . . . *ALL
F3=Exit F4=Prompt F5=Refresh F10=Additional parameters F12=Cancel
F13=How to use this display F24=More keys
MA C 05/037

```

Enter the parameters as follows:

- | | |
|----------------------|---|
| Audit Code | Select the two character audit code that you want to track using iEventManager. You can use the HELP key (or F1 key) to see an explanation for each code. |
| Minutes | Enter a numeric value between 2 and 1440. This will be the time delay between tests for the monitored audit information. For example, if you choose a value of 2 minutes, then iAuditMonitor will check for the specified audit code every 2 minutes. A value of 1440 will cause the audit event to be checked once per day. |
| Notification address | See the Notification Address(s) section of this manual on page 5. |
| Start option | Controls how the monitor treats the startup process.
Choose on of the following values:
<ul style="list-style-type: none"> *RESTART When the Audit Scan starts, it will reset the process and start reporting new events as they occur following the startup. *RESUME When the Audit Scan starts, it will pick up from where it was when it was last stopped. |

Attachment Format Enter the format that you want for the audit alert detail attachment.

Choose from the following list:

*TXT The attachment will be a standard text file format.
 *CSV The attachment will be a comma separated values file format. (Note that this is currently only valid for Audit Code CD.)

Include option For SK audits, this controls whether all secure socket connections will be reported or just the rejections.

Choose from the following list:

*ALL All secure socket connections will be reported.
 *REJ Only rejected secure socket connections will be reported. (Note that this is currently only valid for Audit Code SK.)

When you press the F10 key, you will see the following additional parameter:

Alert Subject Text iEventManager will issue an alert with the default subject text if you leave this set to *DFT. If you want a unique alert subject text used, enter that value here and it will be used if an alert is issued.

Press ENTER and iEventManager will start your audit monitor. At every time period interval specified by the "Minutes" parameter, iEventManager will check for the specified audit events in the system audit journal. If any are found, an email will be generated and sent to the notification address(s). If no events are identified, no alert notice will be sent.

Tracking Command Line Use

The CD audit tracking option will monitor command line use for user profiles that are registered in the IBM i OS. Option 6 on the AUDIT menu lets you see which user profiles are currently configured for command line tracking. It will also let you add a user profile or remove a user profile from the list.

When you start menu option #6, the following display will appear:

```

E - 3:5250 Display
File Edit View Communication Actions Window Help
Type options, press Enter.
2=Change 5=Display
User
Opt Profile Description Class
_ IEMONITOR iEventManager Application Profile *SECOFR

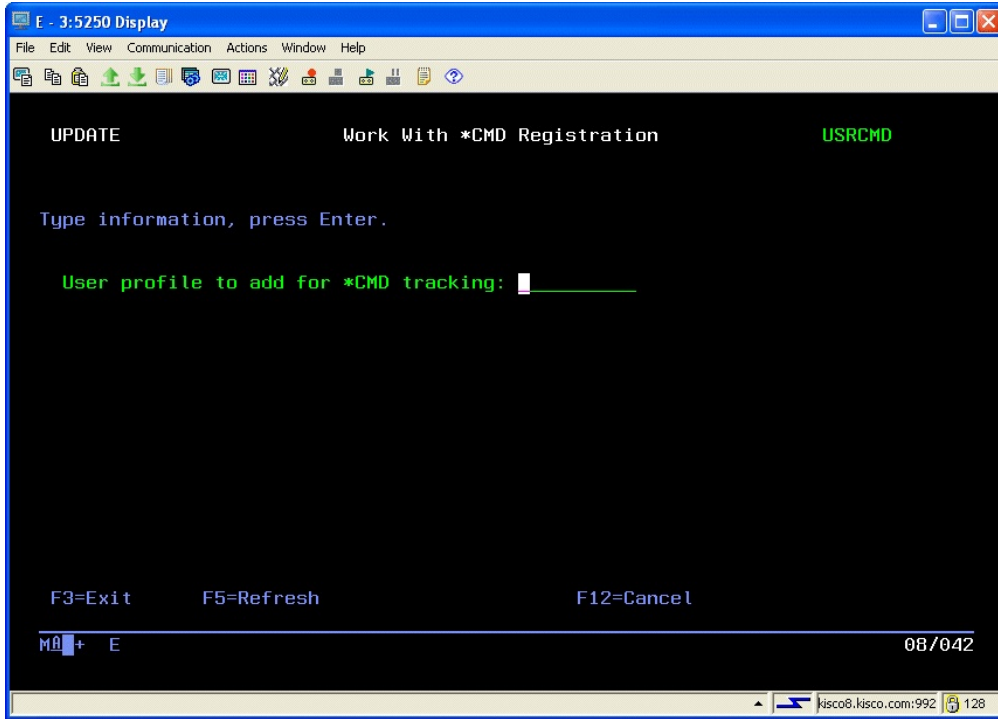
F3=Exit F5=Refresh F6=Add User Bottom
MA + E 02/006
  
```

When you first start this option, any user profiles already registered for command line audit tracking will be shown. If no users are registered, the display will be empty.

Note that this information is all stored in the IBM i OS and not in iEventManager.

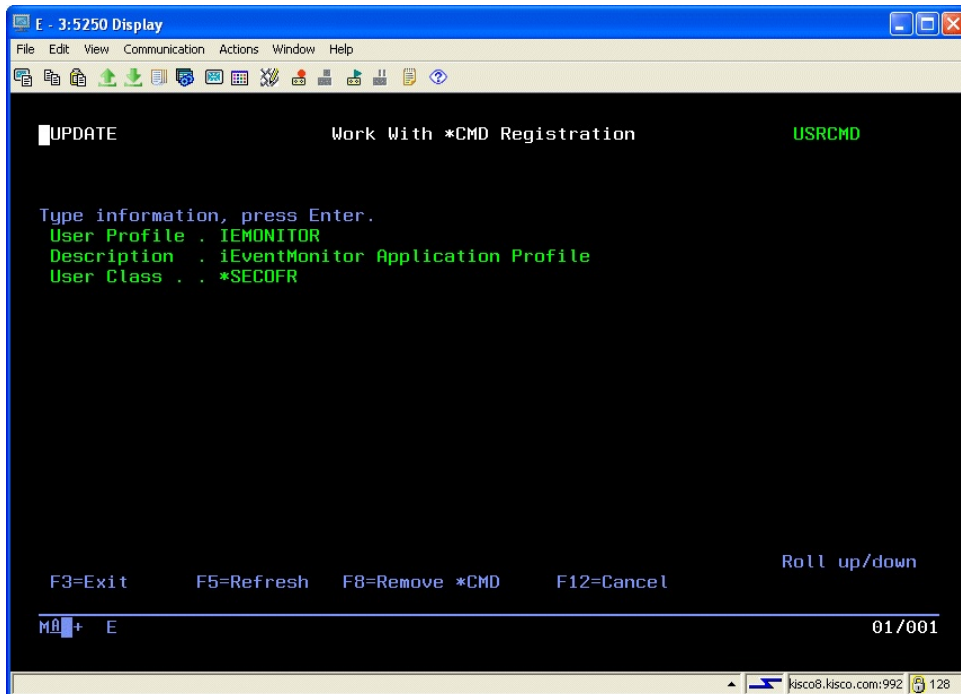
When you add a user profile to this list, all command line activity that uses a CL command, including commands used in called CL programs, will be tracked by iEventManager and reported as an alert at the specified interval with the audit watch. **If you are registering a new user profile, CD tracking reporting will start the next time they sign on to the system.**

To add a new user profile to the list, use the F6 function key. The following will be displayed:



Enter the user profile you want to register and press ENTER. You will then be returned to the AUDIT menu. Run option #6 again to confirm that the user profile is now registered.

To remove a registration, place a 2 (Change) next to the user profile and press ENTER. The following will be displayed:

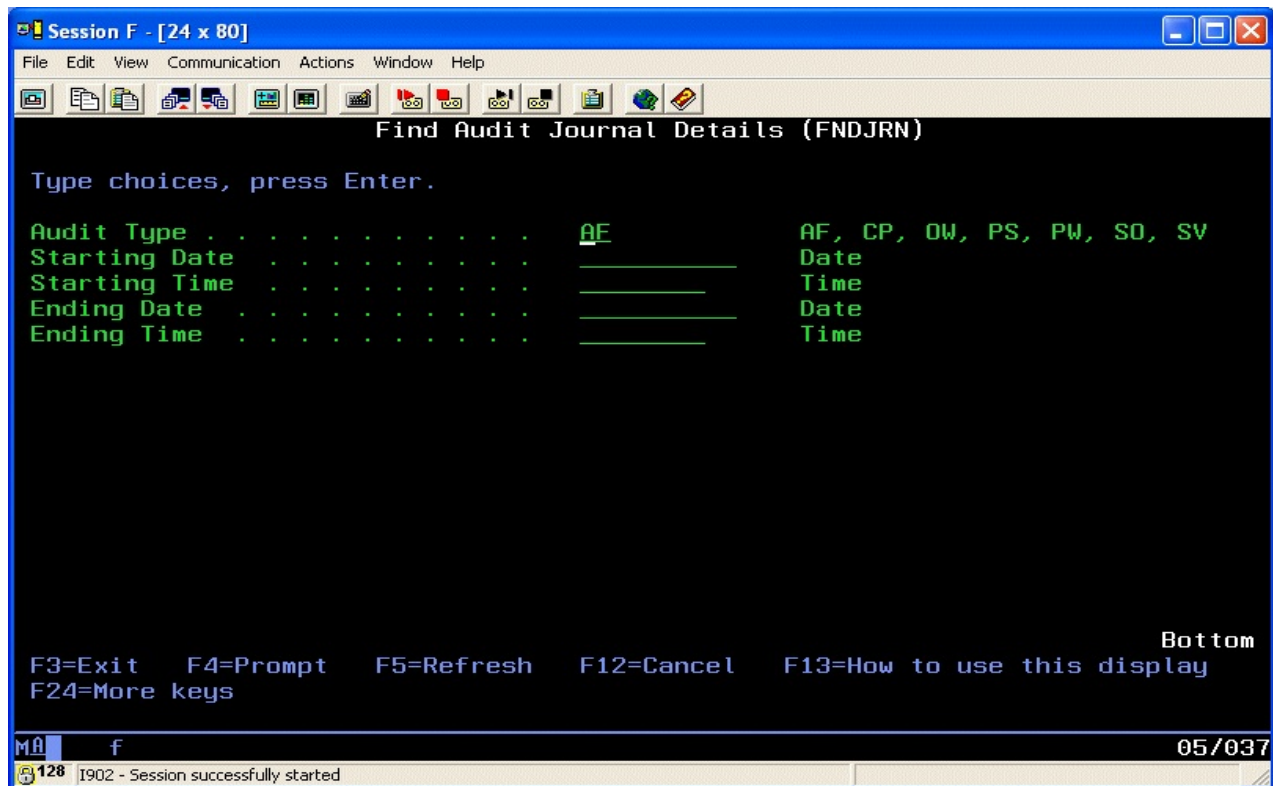


Confirm that the user profile shown is the one that you want to remove from the list. If it is correct, press the F8 key and the user profile will be removed from the list and the AUDIT menu will be re-displayed. Run option #6 on the AUDIT menu again to confirm that the user profile has been removed from the list.

Finding More Details for an Audit Event

When an audit monitor reports an event, or a series of events, a report is attached to the email that is sent. In most cases, the exact nature of the event is apparent from the information reported with the email. In some cases, however, you may want to research more and see all of the information reported in the security journal.

To find and display the details for a specific event, use option #4 on the AUDIT menu or you can also use the FNDJRN command:



Fill in the parameters as follows:

- Audit Type Enter the code for the event that you are tracking with this inquiry
- Starting Date To zero in on the event on the system audit journal, enter the date that was reported with the event by iEventMonitor. If you leave the starting date blank, all matching events will be shown
- Starting Time Enter the time that you want to start the display with. If you leave this blank, all events from the starting date will be shown.
- Ending Date To limit the amount of information displayed, enter the same date as the starting date.
- Ending Time You can also limit the amount of information displayed by specifying an ending time

When you find the specific audit record that you are looking for, you may have to refer to IBM security journal documentation to fully understand the information displayed. If you have difficulty with this, feel free to contact support at Kisco Systems for additional help.

The Server Menu

The Server Menu (IEMSVR) can be used to manually control the IEVENTMON HTTP server instance on your system. This server is used for the IEM Respond feature and also for the iEventManager Bluescape web interface for the software.

If the IEVENTMON server exists on your system, it will always be started when you run the STRIEM command when iEventManager is configured for either IEM Respond or IEM Bluescape. These settings are on the IEMSET command (option 9 on the INSTALL menu).

When you take option 25 on the MASTER menu, the following server menu will be displayed:

```

C - 2:5250 Display
File Edit View Communication Actions Window Help
QSEC0FR IEMSVR Menu KISC01
iEventManager Bluescape Server Menu
1. Start Bluescape Server
2. Stop Bluescape Server
3. Display Bluescape Server Status
10. To MASTER Menu
(c) 2015-2024 Kisco Systems LLC
Selection or command
==>
MA C 22/007
10.2.2.3:23

```

The following options are available:

- 1 - Starts the server instance
- 2 - Ends the server instance
- 3 - Displays the current status of the server by listing the server jobs currently active. If no jobs display, the server is not active.
- 10 - Returns to the MASTER menu

Central Logging Feature

For customers with multiple locations running iEventMonitor, a Central Logging feature is included in the software. The Central Logging is only available to customers who have upgraded to the Enterprise version of iEventMonitor. If you have the basic license and would like to try out the Enterprise features, please contact sales@kisco.com for more information.

To access the Central Logging features, you need to go to the LOGS menu in library IEMLIB. This is available using option 18 on the INSTALL menu or you can just use the following command:

GO MENU(IEMLIB/LOGS)

The following will be displayed:

```

C - 2:5250 Display
File Edit View Communication Actions Window Help
LOGS                                LOGS Menu
                                Central Logging Options

Select one of the following:

1. Display Central Activity Log      DSPLOGC
2. Display Current Log Settings      DSPIEMLOG
3. Change Log Settings               CHGIEMLOG
4. Generate Central Log SIEM Feed    IEMLOGEXC
5. Purge Central Log Records         DSPLOGPRGC

8. Reclaim Remote Log Entries        RCLRMTLOG

10. To MASTER menu

(c) 2015-2024 Kisco Systems LLC

Selection or command
===>
  
```

The menu options are:

- | | |
|-----------------------------------|---|
| 1. Display Central Activity Log | Display the Central Log at the central server location |
| 2. Display Current Log Settings | Display the central logging configuration settings for the local system |
| 3. Change Log Settings | Change the central logging configuration settings for the local system |
| 4. Generate Central Log SIEM Feed | Generate a SIEM feed file from the central log |

- 5. Purge Central Log Records Purge the central log file
- 8. Reclaim Remote Log Entries Used at a remote location to resend log records that failed during a connection interruption

Getting Started with Central Logging

When you have multiple systems in your network that are using iEventMonitor, Central Logging lets you configure systems in your network. One system must be chosen as the central server. This is where all of the activity log information from the other systems will be collected. There can be only one central logging server in your configuration. Before you start, decide what the role of each system will be. There will be a single central server, one or more remote servers and you can choose to have any system running iEventMonitor that does not send activity log information to the central server.

The Central Log feature works using IBM’s Distributed Data Management (DDM) feature. Before you start configuring central logging, we recommend that each of your systems be enrolled by system name in the IBM i OS Host Name Table. This is done using option 10 on the IBM menu named CFGTCP. On each remote server, the system name of the central server must be enrolled with the associated IP address of the central server. There is no special configuration work needed on the central server or on any servers where this feature will not be used.

The Central Log feature also depends on customers having the same release level of iEventMonitor installed at each participating system. This will be checked each time the logging function runs. You can check this by using option 5 on the INSTALL menu on each system.

To define the roll of a server for the Central Logging feature, select option 3 from the LOGS menu. Note that this option cannot be used while iEventMonitor is active on the server. If you just want to see what the current settings are, use menu option #2. You can shut down all iEventMonitor tasks using the ENDIEM command and then restart once configuration changes have been made using the STRIEM command.

When you select this option, the following will be displayed:

```

Change IEM Log Settings (CHGIEMLOG)

Type choices, press Enter.

Logging Role . . . . . > *CSV*      *NONE, *RMT, *CSV*
Logging Prefix . . . . . > Q0       Unique alpha code - SEE HELP
Central server location . . . . . > *NONE

```

Enter the values you want as follows:

- Logging Role Choose one of the following values:
- *NONE No central logging will be done from this system
 - *RMT This will be a remote logging server and activity log information will be sent to the central logging server

	*CSVR	This system will be the central logging server
Logging Prefix		For systems defined as *CSVR or *NONE, this value must be set to the fixed value 'Q0'. For systems defined as *RMT, this must be a unique two character value that must start with an alphabetic character. Each *RMT system in your network must have its own prefix value set.
Central server location		For systems defined as *CSVR or *NONE, this value must be set to the fixed value of *NONE. For system defined as *RMT, this must be the system name of the central logging server that has already been configured in the IBM i OS Host Name Table.

When you have the parameters set, press ENTER. The settings will be validated and the configuration will be checked. Any problems will be reported back to you at the base of the display. You can use option 2 on the LOGS menu to confirm that the values you entered have been posted to the system.

On a system defined with a logging role of *NONE or *RMT, no further actions are necessary.

Working With The Central Activity Log

Options 1, 4 and 5 on the LOGS menu can only be used on the system with the logging role of *CSVR.

Display Central Activity Log

On the central logging server, you can display the collected log records from all the remote locations by running option #1 on the LOGS menu or by using the DSPLOGC command. The following selection screen will be shown:



You can specify the system name of any system that is defined as a remote logging server and you will see the real time log entries from that system. If you specify a location name, the display will be limited to just that system. When you use the *ALL value, the display will start with the local system activity log records but you can dynamically switch to a different system from the detail display.

When you press ENTER, the following display will be shown:

```

C - 2:5250 Display
File Edit View Communication Actions Window Help
Display Central Activity Log DSPCLO
System Name: _____ Date/Time Stamp: _____
Type options, press Enter.
5=Display Details
System
Opt Name      Date/Time Stamp      Task      Alert Text
- KISC01      11/09/23 10:26:15 AD Admin  ENDIEM issued to stop all active
- KISC01      11/09/23 10:39:29 AD Admin  ENDIEM issued to stop all active
- KISC01      11/09/23 10:41:48 AD Admin  iEventMonitor Purge bypassed, no
- KISC01      11/09/23 10:41:54 AM Audit Mon. iEventAlert detected 1 event(s)-A
- KISC01      11/09/23 10:41:57 AD Admin  STRIEM issued to start all active
- KISC01      11/09/23 10:45:28 AD Admin  ENDIEM issued to stop all active
- KISC01      11/09/23 10:46:32 AD Admin  ENDIEM issued to stop all active
- KISC01      11/09/23 10:46:37 AD Admin  iEventMonitor Purge bypassed, no
- KISC01      11/09/23 10:46:44 AD Admin  STRIEM issued to start all active
- KISC01      11/09/23 10:52:08 AD Admin  ENDIEM issued to stop all active
- KISC01      11/09/23 10:57:59 AD Admin  iEventMonitor Purge bypassed, no
- KISC01      11/09/23 10:58:06 AD Admin  STRIEM issued to start all active
- KISC01      11/09/23 13:36:32 AD Admin  ENDIEM issued to stop all active
More...
F3=Exit      F5=Refresh      F6=Print List      F9=Purge
MA C 03/015
10.2.2.3:23

```

To select a different system, enter that name in the System Name field at the top of the display and press ENTER. To view the details for any entry, use option 5 next to the entry. Here is a typical display:

```

DSPDOC Display History Log DSPLOG
Time Stamp: 11/09/23 10:41:54 System Name: KISC01
Sent to: rich@kisco.com
iEventAlert detected 1 event(s)-Audit Code:CP - User Profiles Changed
This email was sent by iEventMonitor.

```

From the list of activity log entries, you can also choose the following function keys:

- F6 Will create a listing of selected log information. See the following section for more details on how the listing selection works.
- F9 Will run a purge of the central activity log. Details on how the purge works are in the following section of this documentation.

Listing Central Activity Log

When you select the F6 function key from the central activity log display, the following prompt screen will be shown:

```

List Central Log File (DSPLOGCLST)

Type choices, press Enter.

Select System Name . . . . . > *ALL          System Name, *ALL
Selection . . . . .                *ALL          *ALL, *TODAY, *PRVDAY, *RANGE
From Date . . . . .                _____      YYYYMMDD
To Date . . . . .                  _____      YYYYMMDD
  
```

Note: You can also start this process using the DSPLOGCLST command from library IEMLIB.

Enter the parameters as follows:

- | | |
|--------------------|---|
| Select System Name | Enter the system name for the records that you want included in the list. Use the special value *ALL to list records for all systems on file. |
| Selection | Choose one of the following date select settings:
*ALL All records for all dates will be listed
*TODAY Just records for the current date will be listed
*PRVDAY Only records for the previous date will be listed
*RANGE A specific date range will be use to select records to be listed. |
| From Date | This parameter can only be used when the selection parameter is set to *RANGE. Enter the starting date for your selection in the format YYYYMMDD. |
| To Date | This parameter can only be used when the selection parameter is set to *RANGE. Enter the ending date for your selection in the format YYYYMMDD. |

When you press ENTER, the listing will be generated.

Purging Central Activity Log

When you select menu option 5 on the LOGS menu or you press the F9 function key from the central activity log display, a purge of the central activity log will be accessed. The purge will run the same way the purge has always run. Please see the purge documentation in the Installation and Configuration section of this documentation. When you run the purge on the central logging server, the central log and the local log will both be purged.

Reclaim Remote Log Entries

On a system with a logging role of *RMT (Remote), a communications failure could result in activity log information not getting sent to the central logging server. When this happens, the activity log records are held in suspense until the communications issue is resolved. You can use option #2 on the LOGS menu to check for records to be reclaimed. It should normally show as 'None'.

If there are records to be reclaimed and the communications issue has been resolved, you can reclaim the records by running option #8 on the LOGS menu. The records that have been held in suspense will then get sent to the central logging server.

Remote Configuration Sync Feature

For customers with multiple locations running iEventMonitor, a Remote Configuration Sync feature is included in the software. The Remote Configuration Sync is only available to customers who have upgraded to the Enterprise version of iEventMonitor. If you have the basic license and would like to try out the Enterprise features, please contact sales@kisco.com for more information.

To access the Remote Configuration Sync features, you need to go to the SYNC menu in library IEMLIB. You can use the following command:

```
GO MENU(IEMLIB/SYNC)
```

The following will be displayed:

```

C - 2:5250 Display
File Edit View Communication Actions Window Help
QSEC0FR SYNC Menu KISC01
iEventMonitor Configuration Sync Menu

1. Work With Sync Locations WRKSYNCLOC
2. Check Sync Location SYNCCHK
3. Sync To Location SYNCIEM

10. To MASTER Menu

(c) 2015-2024 Kisco Systems LLC

Selection or command
===>
  
```

The menu options are:

- | | |
|-----------------------------|--|
| 1. Work With Sync Locations | Lets you work with locations where you want to synchronize your iEventMonitor configuration. |
| 2. Check Sync Location | Tests a remote location to see if it can be used. This option is not normally used from the menu but is accessed using menu option #1. |
| 3. Sync To Location | Runs a configuration sync process. This option is not normally used from the menu but is accessed using menu option #1. |

Getting Started with Remote Configuration Sync

When you have multiple systems in your network that are using iEventMonitor, Remote Configuration Sync lets you transfer the iEventMonitor configuration from one system to another. Typically, one system is chosen as the central server where a standard configuration is created and kept. This configuration can then be “pushed” to remote systems to enforce those settings.

The Remote Configuration Sync feature works using IBM’s Distributed Data Management (DDM) feature. This is the same requirement as for central logging. If that has already been done, skip the next paragraph.

Before you start configuring remote sync, we recommend that each of your systems be enrolled by system name in the IBM i OS Host Name Table. This is done using option 10 on the IBM menu named CFGTCP. On each remote server, the system name of the central server must be enrolled with the associated IP address of the central server.

Remote Configuration Sync also uses the IBM i Relational Database Directory for each remote location to be synced. You can access this feature using the IBM command WRKRDBDIRE. When you enter this command, the following display will be shown:

```

Work with Relational Database Directory Entries

Position to . . . . . _____
Type options, press Enter.
  1=Add  2=Change  4=Remove  5=Display details  6=Print details

Option  Entry                Remote Location      Text
-----  -----                -
  1      *MSC01                    *LOCAL
  2      *MPDEV                    mpdev
  3      *MPA1                     mpa1
  
```

Each location that will be synced must appear in this table. To create a new entry, enter a ‘1’ on the first option line, fill in the location name and press ENTER. The following display will be shown:

```

Add RDB Directory Entry (ADDRDBDIRE)

Type choices, press Enter.

Entry:
  Relational database . . . . . > TESTLOC
  Relational database alias . . . *NONE
Remote location:
  Name or address . . . . . _____

Type . . . . . *SNA          *SNA, *IP
  
```

The following fields will need to be set:

Name or address Enter the location name from the IBM i Host Name Table

Type Be use to change this to the special valid '*IP'

Press ENTER to store the RDB Directory Entry in the table. This must be repeated for each remote location while configurations will be synchronized.

The Remote Configuration Sync feature also depends on customers having the same release level of iEventMonitor installed at each participating system. This will be checked each time the logging function runs. You can check this by using option 5 on the INSTALL menu on each system.

To define the roll of a server for the Central Logging feature, select option 3 from the LOGS menu. Note that this option cannot be used while iEventMonitor is active on the server. If you just want to see what the current settings are, use menu option #2. You can shut down all iEventMonitor tasks using the ENDIEM command and then restart once configuration changes have been made using the STRIEM command.

Working With Sync Locations

To work with sync locations, select option #1 on the SYNC menu or use the WRKSYNCLOC command. The following display will be shown:

```

C - 2:5250 Display
File Edit View Communication Actions Window Help
Sync Location Maintenance                               SYNCMN

Type options, press Enter.
  2=Change      4=Delete      5=Display      7=Test      9=Sync

Opt Location    Location Desc    Last Status
  1 DR Remote Partition    Synced

F3=Exit      F5=Refresh      F6=Create

Bottom
MA C 09/003
10.2.2.3:23
  
```

On this display, any remote locations already configured will be shown along with their current status.

To create a new location, use the F6 function key and the following display will be shown:

```

ADD                               Sync Location Maintenance          SYNCMN

Type information, press Enter.
Location . . . . .                _____
Location Desc . . . . .           _____
-----
Last Status . . . . .             Synced
Location Added . . . . .
Last Task Sync . . . . .
Last Exceptions Sync . . . . .
Last Override Sync . . . . .
Last Alert Routings Sync . . . .
Last Devices Watched Sync . . . .
Last Network Locations Sync . . .
Last Connection Addresses Sync . .
Last Authorized Users Sync . . . .

```

Enter the location name you are adding and a text location description. Press ENTER to record the new location. The other fields on this display are just for information purposes.

Once a location has been entered, then it must be tested to make sure that a stable communications path is available. To do a test, place a '7' next to the location to be tested and press ENTER. If there are any errors, they will be returned on at the bottom of the display panel.

In order for a test to be successful, iEventManager must be stopped on both the local system and on the remote system being tested. If either of these are active, then the test will not complete successfully. When the test is successful, the status will show as "Passed".

To synchronize to the location, place a '9' next to the location name and press ENTER. The following display will be shown:

```

Synchronize IEM With Remote (SYNCIEM)

Type choices, press Enter.

Remote Location Name . . . . . > MD          Character value
Sync Tasks? . . . . .                *NO          *NO, *YES
Message Exceptions? . . . . .        *NO          *NO, *YES
Monitor Overrides? . . . . .         *NO          *NO, *YES
Alert Routings? . . . . .            *NO          *NO, *YES
Devices Watched? . . . . .           *NO          *NO, *YES
Network Locations? . . . . .         *NO          *NO, *YES
Connection Addresses? . . . . .      *NO          *NO, *YES
Authorized Users? . . . . .          *NO          *NO, *YES

```

You can synchronize selective configurations from this point. The first time you run this, check the following options carefully to make sure that you understand what each sync will do. Keep in mind that this will **replace** the current configuration at the remote location. The default setting of *NO means that the selected configuration will not be sent to the remote location. Changing a value to

*YES will include the configuration in the remote synchronization process.

The options are:

Sync Tasks	All tasks existing on the local system will be sent to the remote location. You can review the list of tasks using option #1 on the MASTER menu.
Message Exceptions	All message ID exceptions on the local system will be sent to the remote location. You can review the list of exceptions using option #5 on the MASTER menu.
Monitor Overrides	All message overrides on the local system will be sent to the remote location. You can review the list of overrides using option #6 on the MASTER menu.
Alert Routings	All message routings on the local system will be sent to the remote location. You can review the list of routings using option #4 on the MASTER menu.
Devices Watched	The list of devices to be watched on the local system will be sent to the remote location. You can review the list of devices using option #1 on the WATCH2 menu.
Network Locations	All network locations on the local system will be sent to the remote location. You can review the list of network locations using option #1 on the NETWATCH menu.
Connection Addresses	All connection IP addresses on the local system will be sent to the remote location. You can review the list of connection addresses using option #6 on the NETWATCH menu.
Authorized Users	Warning - it is the customer's responsibility to make sure that the user profiles included in the authorized user list already exist at the remote locations. All users authorized to iEventMonitor on the local system will be sent to the remote location. You can review the list of authorized users using option #8 on the INSTALL menu.

Once the options have been selected on this display, press ENTER and the selected options will be sent to the remote location and replace those (if any) that are currently in place there. When the sync has completed, the selected items will be updated with the current date and time information and the status will be updated to show "Synced".

After a successful sync, iEventMonitor can then be started at both locations.

Installation and Configuration

Before any iEventManager functions will work, the initial install procedure must be run. iEventManager can be installed from a download file obtained from the Kisco Systems website.

This installation procedure will install the base support for iEventManager when used with a standard terminal-based interface. To use the web-enabled features of iEventManager from your web browser, some additional installation and configuration steps will be needed. Please see the separate documentation that arrived with your software for these instructions.

Installation from Download

Use the install instructions from the iEventManager Download web page.

<https://www.kisco.com/iem/iemdload.html>

After you download the ISO CD image install file and documentation from the website, print the Download page and use it for reference while completing the installation.

Release Upgrade Installation

When Kisco Systems completes work on a new Release of iEventManager, you will be notified of the availability for the new release. New releases are available via download from the Kisco website for iEventManager.

To install an upgrade, follow the above link. Be sure to get the most recent copies of the updated documentation as well.

iEventManager Removal

Removing iEventManager may happen when doing a license transfer to a different system or when you have decided not to go ahead with a purchase following a free trial.

Before you remove iEventManager from your system you must first run option #15 on the INSTALL menu (Remove Message Handling Exit Program). Once this has been done, then the application library name IEMLIB can be safely deleted and the software will be removed.

SMTP Port# Variable

iEventMonitor allows you to specify a non-standard port number for SMTP when sending alerts by email. If your system uses port 25 (which is a standard industry practice and applies to most installations), then you do not need to do anything.

If you want to use a different SMTP port number, it is stored in the data area named IEMCONTROL in the IEMLIB library. The value is in positions 796-800 and is expressed in hexadecimal. You can use the following command to make changes:

```
CHGDTAARA DTAARA(IEMLIB/IEMCONTROL (796 5)) VALUE(X'0000000019')
```

Note: the above command sets the SMTP port# to 25, the default value.

This only applies when you are using the internal email delivery protocol in iEventMonitor. If your system is using the IBM i OS SNDSMTPEMM protocol, then check with IBM support if you want to use a different port number.

IEM Respond Configuration

For the IEM Respond feature of iEventManager 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 IEVENTMON
- Step 3: Install the HTTP Server objects for iEventManager
- Step 4: Start the new IEventManager server instance
- Step 5: Set IEMSET Parameters for IEM Respond

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, the Web Administration wizard that comes with your OS will be displayed.

Step 2: Create a new HTTP server instance named IEventManager

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 “IEVENTMON”. The server description of “Kisco iEventManager 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 iEventManager

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 IEMLIB/INSTALL
```

Run option #11 (Install HTTP Server Instance Objects) from this menu. This will install the HTTP server objects needed by iEventManager.

Step 4: Start the new IEventMonitor 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(IEVENTMON)
```

The server instance will now be active. You can now test the server instance by going to your browser and entering the following URL to bring up the test page:

```
http://yoursystemi.com:8077
```

A test page like this will be displayed:



iEventMonitor Configuration Test

WELCOME & CONGRATULATIONS!

Your iEventMonitor Respond server instance is working.

At this point, the server instance is ready for use.

Step 5: Set IEMSET Parameters for IEM Respond

Before you can use the IEM Respond feature, several settings must be updated in the IEMSET command (option #9 on the INSTALL menu) as follows:

- | | |
|--------------------------|---|
| IEM Respond Active? | This must be set to *YES. |
| IEM Respond Page Heading | This allows you to customize the browser display heading for your installation. |
| IEM Browser Respond IP | Sets the HTTP address used for your browser session. |

Refer to the documentation for option #9 (IEMSET) on the INSTALL menu contained in the following section of this user's guide.

The Install Menu

When you select item 30 from the MASTER menu, the installation menu is displayed as follows:

```

C - 2:5250 Display
File Edit View Communication Actions Window Help
INSTALL
INSTALL Menu

 1. Run initial install procedure
 2. Display installation status
 3. Change installation status
 4. Print documentation
 5. Check Version Information
 6. Purge iEventMonitor Activity Log           DSPLOGPRG
 7. Process Kisco PTF Package
 8. Work With Authorized Users               WRKIEMUSR
 9. Set iEventMonitor Default Values         IEMSET
10. Send Test Email Message                  SNDALERTT
11. Install HTTP Server Instance Objects    WWWINST
12. Test Error for IEM Respond

15. Remove Message Handling Exit Program
16. Generate SIEM Feed                       IEMLOGEX
17. Send Diagnostic Info to Kisco           SNDIAGF
18. To LOGS Menu
20. To Master Menu

(c) 2015-2024 Kisco Systems LLC

===>
  
```

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

- | | |
|-------------------------------------|---|
| 1. Run initial install procedure - | Do not use this option unless directed to do so by Kisco Support staff. This option is automatically run during normal install processing. |
| 2. Display installation status | Displays a screen showing the current installation status for the software. |
| 3. Change installation status | Displays the current software installation status and allows for changes to be made. |
| 4. Print documentation | Prints the documentation changes since this manual was last updated. |
| 5. Check Version Information | Displays information about the specific version of iEventMonitor that is installed on your system. |
| 6. Purge iEventMonitor Activity Log | Lets you purge the activity log using the DSPLOGPRG command. |
| 7. Install Kisco PTF package | Allows you to process a corrective PTF package received from Kisco for program fixes. |

- | | |
|--|---|
| 8. Work With Authorized Users | Allows you to maintain which user profiles are allowed to use the iEventMonitor product features. |
| 9. Set iEventMonitor Values | Lets you set up global default settings for iEventMonitor. |
| 10. Send Test Email Message | Sends a test email message to the email address that you provide. Used when getting email notification configured. |
| 11. Install HTTP Server Instance Objects | Installs the IEM Respond feature server objects on your system. Only needs to be run once. |
| 12. Test Error for IEM Respond | Submits a job to QBATCH which will force an error message that requires a response. This can be used when setting up the IEM Respond feature for your testing process. |
| 15. Remove Message Handling Exit Program | Only used when removing iEventMonitor from your system. DO NOT USE at any other time. This option makes sure that the exit program used for message queue reminders is not registered in the IBM i OS exit registration. |
| 16. Generate SIEM Feed | Used to generate the optional SIEM Feed file for SIEM integration. |
| 17. Send Diagnostic Info to Kisco | Collects diagnostic information about iEventMonitor on your system and emails it to Kisco Systems for analysis purpose. You should only use this option as directed by Kisco support staff. |
| 18. To LOGS Menu | Displays the LOGS menu for access to the Central Logging options. This is only available to customers who have upgraded to the Enterprise version of iEventMonitor. |
| 20. To MASTER Menu - | Will display the iEventMonitor MASTER menu. |

Details on each of these menu options are covered in the following sections of this documentation.

Display installation status

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

```

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

Installation for      IEMLIB      Developer ID code  KISCO
Machine serial number 785D4C0    Current Library    IEMLIB
Sec.serial number     785D4C0    Sec.install date.. 211221
Machine run date.... 220217      Sec.expire date..  999999
Sec.partition....    002

Security Status PERMANENTLY INSTALLED...Z-003

Please enter:
Type of install ....  T for trial, or P for permanent
Install password .... Blank for trial, or permanent password
New expire date..... Blank for trial, or 999999 for permanent

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

M&  C  17/031
10.2.2.3:23

```

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

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

<u>Message</u>	<u>Explanation</u>
Z-001 NOT INSTALLED	Trial installation not started
Z-002 TRIAL EXPIRED	Trial period has ended
Z-003 PERMANENTLY INSTALLED	Software is permanently installed
Z-004 INSTALLED ON TRIAL	Software is installed on trial
Z-005 PASSWORD NOT ACCEPTED	Password keyed is not valid
Z-006 WRONG LIBRARY	Programs must run from our library
Z-007 PLEASE RUN TRIAL INSTALL	Must have trial install before perm.
Z-008 INVALID INSTALL REQUEST	Must be P or T
Z-009 INVALID SECURITY (REC#6)	Call Kisco
Z-010 INVALID SECURITY (NO ZZ)	Call Kisco
Z-011 INVALID SECURITY (HASH.)	Call Kisco

Change installation status

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

```

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

Installation for      IEMLIB      Developer ID code  KISCO
Machine serial number 785D4C0    Current Library    IEMLIB
Sec.serial number     785D4C0    Sec.install date.. 211221
Machine run date.... 220217      Sec.expire date.. 999999
Sec.partition....    002

Security Status PERMANENTLY INSTALLED...Z-003

Please enter:

Type of install ..... █      T for trial, or P for permanent

Install password .... :..... Blank for trial, or permanent password
New expire date..... :..... Blank for trial, or 999999 for permanent

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

M  C 17/031
10.2.2.3:23

```

Trial extension

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

Type of install	Enter 'T' for trial
Install password	Enter all six digits of the extension password provided, including any leading zeros
New expire date	Enter the new expiration date in the format YYMMDD (ie: Jan 12, 2021 would be 210112)
User count	Enter the number of users that you are authorized for from Kisco

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

Permanent installation

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

Type of install	Enter 'P' for permanent
Install password	Enter all six digits of the extension password provided, including any leading zeros
New expire date	Enter all 9's (ie: 999999)
User count	Enter the number of users that you are authorized for from Kisco

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

Print additional documentation

At any time, you can reproduce the Additional Documentation Topics by using this menu option. A full copy will be printed.

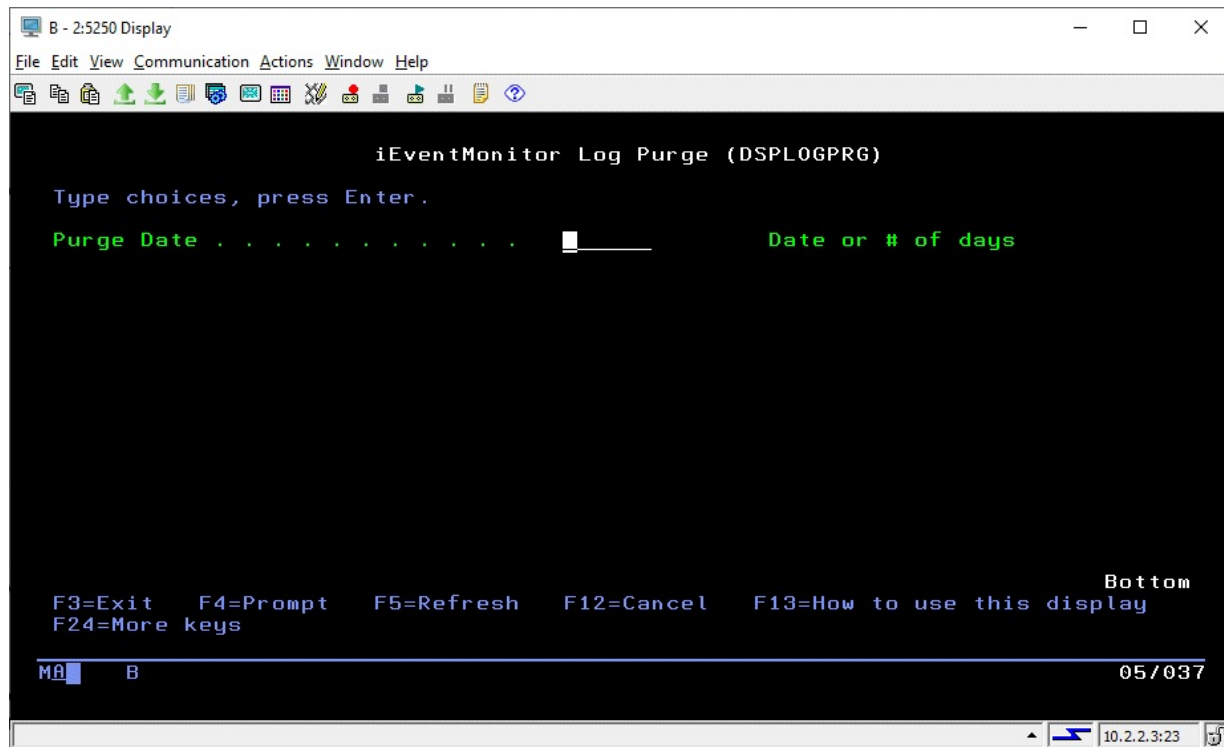
Check Version Information

This menu option will display the current release level and PTF information for your version of iEventMonitor. Kisco may need to verify this when working with you on a support issue.

Purge Activity Log

Option 6 on the INSTALL menu will prompt the DSPLOGPRG command to let you remove records from the iEventMonitor Activity Log. If your system is configured as the central logging server in your network of servers running iEventMonitor, the log purge on the LOGS menu should be used, not this one.

When select the option, the following screen prompt will be displayed:



Enter the date that you want to purge up to. The date format should agree with the way your system is configured for date presentation. All records prior to the date entered will be purged.

If you don't want to specify a date, you can enter up to three digits in this field to indicate the number of days that you want to keep on file in the log. All older entries will be purged.

The purged records will be removed from the Activity Log. If you want a listing of them before you run the purge, you can do that from the Activity Log display, option #9 on the MASTER menu.

Install Kisco PTF Package

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

The current instructions for PTF installation can be found at the Kisco Systems website using the following link:

<https://www.kisco.com/iem/support/ieptfupd.html>

Work With Authorized Users

When iEventManager is initially installed, it can only be used by a user profile with *ALLOBJ authority (such as QSECOFR). To grant access to use iEventManager to users who do not have *ALLOBJ authority, use option #8 on the INSTALL menu or use the WRKIEMUSR command:

```

Session F - [24 x 80]
File Edit View Communication Actions Window Help
Maintain End-User Table          USRMT1

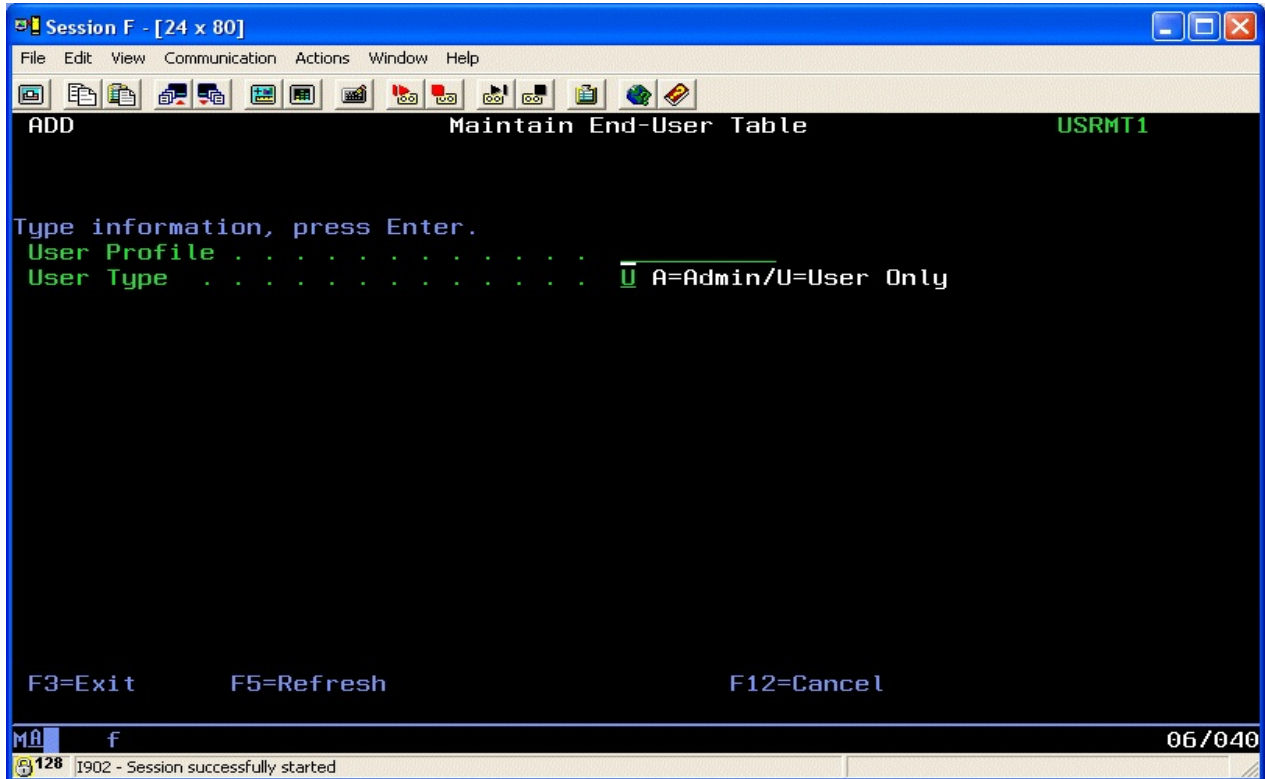
Type options, press Enter.
  2=Change      4=Delete      5=Display
  User          User
Opt Profile    Type User Description
- IEMONITOR    A   iEventManager Application Profile
- QSECOFR      A   Security Officer

F3=Exit      F5=Refresh      F6=Create          Bottom
M1 f 03/006
128 | I902 - Session successfully started

```

As shipped from Kisco Systems, the user profiles QSECOFR and IEMONITOR are automatically granted access to use iEventManager. Do not remove either of these entries.

To add a new user to the list of those who can use the software, select the F6 function key:



To authorize your additional user profile, enter the profile here. You must also then specify the type of user you want them to be as follows:

- | | |
|-------------|--|
| User Type A | Is an administrative user. An admin user can use all functions and features of the iEventManager software product. |
| User Type U | Is a user. All functions of iEventManager are available to them except for option #8 on the INSTALL menu. |
- For the Bluescape web browser interface for iEventManager administration, a user type can only look at settings and active tasks, they cannot change them, set up new monitors or start and stop monitors.

This allows you to let specific users use iEventManager, but restricts granting and removing this permission to just those user who are categorized as administrative users.

iEventMonitor Default Values

Choose menu option #9 from the INSTALL menu to set default values. The following prompt will be displayed:

```

C - 2:5250 Display
File Edit View Communication Actions Window Help
Type choices, press Enter.
Message Que Read Delay . . . . . > 02           Seconds (01-30)
Prime Shift Start Time . . . . . > 730         0000-2400
Prime Shift End Time . . . . . > 1600        0000-2400
Include Job Info in Alert? . . . . > *YES       *YES, *NO
IEM Bluescape Active? . . . . . > *YES       *YES, *NO
IEM Respond Active? . . . . . > *YES       *YES, *NO
Text Friendly Alerts? . . . . . > *YES       *YES, *NO
Duplicate Alert Suppression . . . > 001        Minutes - 000-060
Use SNDSMTPPEMM? . . . . . > *YES       *YES, *NO
Email Format . . . . . > *PLAIN     *HTML, *PLAIN
Use kConnect SMS? . . . . . > *YES       *NO, *YES
kConnect ACCT ID . . . . . > *DEFAULT   Character value
Default Notification Address . . > 'support@mycompany.com;18885551212'

More...
F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys

MA C 17/072
10.2.2.3:23

```

Set these parameters as follows:

Message Que Read Delay	This value is no longer used by iEventMonitor.
Prime Shift Start Time	Defines your primary shift starting time expressed in 24 hour clock format (hhmm).
Prime Shift End Time	Defines your primary shift ending time expressed in 24 hour clock format (hhmm).
Include Job Info in Alert?	This option can add more information to each message queue monitor alert notification. With this option activated, the job name, job number and user profile for the job issuing the message to the message queue will be included in the notification.

Choose one of the following values:

***NO** No additional logging will be done.

- *YES** The additional logging information will be posted to the joblog and to the system history log.
- IEM Bluescape Active? Tells iEventMonitor whether or not the Bluescape web browser interface is installed and configured. This is initially set to ***NO**. After the additional configuration work has been completed, this can be set to ***YES**. **DO NOT set this to *YES until you are sure that you are ready.**
- IEM Respond Active? Tells iEventMonitor whether or not the IEM Respond feature has been activated on your system. When initially installed, this defaults to ***NO**. Once you have completed the additional configuration steps as outlined in this user's guide, you can set this to ***YES** to enable the feature. **DO NOT set this to *YES until you are sure that you are ready.**
- Text Friendly Alerts? Choose one of the following values:
- *NO** If you are not using the IEM Respond feature, leave this set to ***NO**.
 - *YES** If you are using the IEM Respond feature and you are issuing alerts to text destination addresses, this option will cause the alerts that require a response to be formatted better for those receiving the alert by text.
- Duplicate Alert Suppression This option controls suppression of duplicate message queue monitor alerts issued within a short period of time. It can be used to make sure that your email stream issued from your IBM i systems does not get clogged if an application error gets into a looping condition.
- This setting is in minutes and the default value is set to 5. If an identical message is issued by the same user profile within the given period of time, only the first instance will result in an alert being issued.
- Changing this value to zero will turn this feature off for your system.
- Use SNDSMTPEMM? Controls which email transport mechanism is used by iEventMonitor to send email from your system. If you make a change to this setting, it will not take effect until the next time you end and restart iEventMonitor.
- Choose one of the following values:
- *YES** When an alert is sent, the IBM i SNDSMTPEMM protocol will be used. Note: This is only valid on system running IBM i OS 7.3 or later.
 - *NO** The legacy protocol will be used to send email. This is required on systems running IBM i OS 7.2 or earlier.

If you make a change to the SNDSMTPEMM setting while iEventMonitor is active, you must then stop and restart your monitors using the ENDIEM and STRIEM commands.

Email Format

Controls how your alert notification emails are formatted when you are using the SNDSMTPEMM protocol.

Choose one of the following values:

***HTML** The email body will be encoded using HTML formatting. This option is not available when the previous option is set to ***NO**.

***PLAIN** The email body will be encoded using plain text formatting.

If you make a change to the format setting while iEventMonitor is active, you must then stop and restart your monitors using the ENDIEM and STRIEM commands.

Use kConnect SMS?

If you have Kisco Connect installed on your system, then changing this value to ***YES** will integrate iEventMonitor with Kisco Connect for text notifications.

kConnect ACCT ID

If Kisco Connect is activated, a valid Account ID must be specified here.

Default Notification Address

This is the email address field that will be used by iEventMonitor whenever the special value ***DFTID** is used for an alert.

See the Notification Address(s) section of this manual on page 5.

In the example above, an email address is specified and is stacked with a cell phone number. This is for an installation that has Kisco Connect installed.

Press the roll-up key once to access additional parameters on the next screen panel as follows:

Alternate Notification Address

Enter the email address information that you want to use for off-shift notifications locations.

See the Notification Address(s) section of this manual on page 5.

If you do not want to use the off-shift notification process, enter the special value ***NONE** here.

Support Email Address

Enter a single email address. This address will be used with all alert emails as the “from” email and the “reply-to” address.

Support Name Description

Enter a name description that you want to show up on the

email as the sender of your alert notices.

Default Alert Subject Enter the standard email Subject text that you want used for all alert notices. If you are using iEventManager on multiple systems or partitions, you might want to have each install use a Subject that identifies the system that it is coming from.

Note: If you use either the header or trailer option, additional text will be included in all alerts. If you are routing alert messages by text, this could result in incomplete alert information when text size is limited by a cell carrier.

Optional Alert Header Text Enter up to 80 characters that you want added as the first line header of every alert message that is issued. If you use the special value of *NONE, no first line header will be included in the alert.

Optional Alert Trailer Text Enter up to 80 characters that you want added as the last line trailer of every alert message that is issued. If you use the special value of *NONE, no last line trailer will be included in the alert.

IEM Respond Page Heading This is used as a web page heading when the IEM Respond feature is active for your installation.

IEM Browser Respond IP This is your system web address to be used for the IEM Respond feature.

An example might look like this:

`http://yoursystemi.com:8077`

Note that the port reference of 8077 must be included. You can also specify a numeric IP address like the following example:

`http://10.1.2.3:8077`

Escalation Notification Addr Some features in iEventManager provide for reminder alerts to be sent when a situation has not been resolved yet. If you want to send an alert to any additional addresses, you can enter those here. Do not repeat any addresses that are already included in the primary notification.

See the Notification Address(s) section of this manual on page 5.

Off-Shift Days If you are using the off-shift alternate notification feature and you want to define certain days of the week as off shift all day (such as Saturday and Sunday), enter those days here. You can enter up to 5 values. Use the standard system values for the days of the week (*MON *TUE *WEB *THU *FRI *SAT

*SUN). If you do not want any days to be considered as off-shift all day, use the special value *NON for none.

Purge Days Range

Enter the number of days to be used when an automatic purge is run. The automatic purge runs whenever the STRIEM command is issued. If this is set to 000, then the purge will be bypassed during startup processing. To use the automatic purge, a number of days within the range of 007-365 must be specified. All activity log entries older than the number of days specified will be purged.

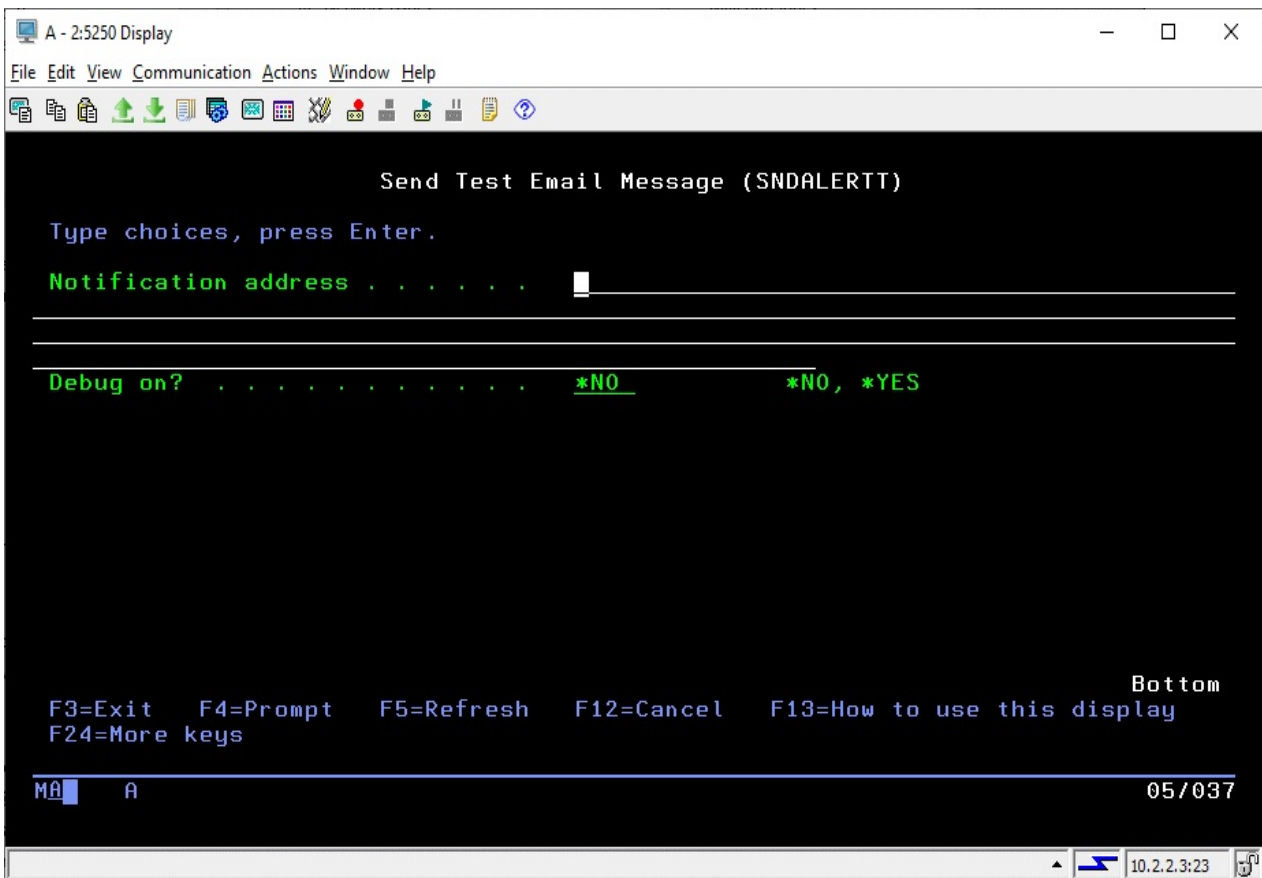
List Purged Records?

If you are using the automatic purge feature, this setting will control whether a listing of the purged activity log entries will be created during the purge. Changing this setting to *YES, will cause the listing to be created.

Note: Before you can use email alerts in iEventMonitor, a test email must be successfully sent from your system using option #10 on the INSTALL menu.

Send Test Email Message

iEventManager can send alerts via email. To check to make sure that the email transport mechanism is working on your system, an option is available on the INSTALL menu to send a test message by email. To send a test email using iEventManager, select option #10 on the INSTALL menu. The following prompt field will be shown:



Enter a valid email address where you want to send the test and press ENTER. During the initial processing of the request, several system configuration tests will be run to make sure that the basic email environment needed for iEventManager is valid. Watch for these initial error messages. Once those tests are completed, then the test email transmission will be done.

If you have Kisco Connect installed on your system, you can also specify a cell number for an SMS text test. This test does not support stacking multiple addresses together.

If the email gets delivered, then you know that the process is configured correctly and will work. If no email arrives or if you get an error message, enter the following command:

DSPJOBLOG

When the display comes up, press F10 and then F18. This will display details from your session joblog that should contain diagnostic information about what may have failed. If you need help

with this, contact Kisco Systems. Kisco may want to see the detailed joblog at this point. You can generate a detailed joblog using the following command:

DSPJOBLOG OUTPUT(*PRINT)

This will place the joblog in the output queue named QEZJOBLOG. Kisco will want you to email this to them for review.

There is also a debug option. If the joblog does not reveal the source of the issue and you are NOT using the IBM i OS SNDSMTPEMM protocol, try repeating the test with the debug option set to *YES. This will generate a short 2-3 page listing to you session output queue. Review that listing for clues as to what might be causing your email delivery to fail.

If you are having problems with email processing, check the following web page at our website for tips and suggestions:

<http://www.kisco.com/emailconfig.htm>

SIEM Feed Option

iEventMonitor includes an optional feature that lets you generate a feed to an external Security Information and Event Management (SIEM) system. The feed is formatted using the IBM LEEF 2.0 standard. This update for SIEM will process all messages from any monitored message queue.

To generate the feed file, a new option has been added to the INSTALL menu. Option #15 (or using the IEMLOGEX command) will create a new feed file with all new events since the last time it was run. The first time it is run, it will pick up events logged since the PTF (or version update) was installed.

When the option runs, it will create a new file each time. The file will be named "iem_siem_nnnnn.txt" and will be located in the "/tmp" path in the IFS. The nnnnn in the file name will be a sequential number starting with "00001". If you prefer to have the file generated with a different name or in a different IFS path, contact Kisco Systems for instructions on how to make this change.

Each SIEM feed record will include standard LEEF 2.0 header fields along with standard src, usrName, devTime and devTimeFormat fields. Two custom event keys have been added which are msgID and msgText.

Optional Activity Trace

iEventMonitor includes an option that will let you trace successful alerts created by iEventMonitor. With the trace active, every successful alert issued by iEventMonitor will be noted in the joblog for the respective alert task with a copy of the trace being recorded in the system history log. You can view entries in the system history log using the DSPLOG command from IBM.

To activate this option, just run the following command:

CHGDTAARA DTAARA(IEMLIB/IEMCONTROL (627 1)) VALUE('X')

To deactivate it once it has been started, run the following:

```
CHGDTAARA DTAARA(IEMLIB/IEMCONTROL (627 1)) VALUE('')
```

SETALT Command

iEventMonitor includes a command, SETALT (Set Alternate Address On/Off). This command can be used to temporarily switch all alert notifications from iEventMonitor to use the Alternate Notification Address for alerts. When you first install the software, it will be set to *OFF status.

You can use this command to switch alerts to your alternate addresses for special circumstances that fall outside of the range of shift times and off-shift days. For example, if your support staff has a meeting during the day and you want backup staff to handle any alerts.

To use the command, simply prompt the SETALT command in library IEMLIB. There is a single parameter of either *OFF or *ON. If you turn the feature *ON, it is the customer's responsibility to turn it back *OFF when your circumstances return to normal.

Task-Specific END commands

Prior to iEventMonitor Release 7.10, each of the task functions appearing on the menus included both a starting and an ending command. When release 7.10 was published, most of the the ending commands were removed from the menus in favor of the new ENDIEMTSK command (see the section titled Controlling iEventMonitor Tasks above).

For compatibility reasons, the task ending commands are still included with the software and can be used by customers. Keep in mind that when tasks are ended using this method, they are removed from the list of tasks implemented in iEventMonitor.

- End Watch (ENDIEMWAT)
- End Watch ASP (ENDWCHASP)
- End A Job Watch (IEMJOBWEND)
- End JobQ Watch (ENDWCHJQ)
- End Utilization Monitor (ENDIEMUTIL)
- End User Watch (ENDUSRWCH)
- End A Job MTXW Watch (IEMMTXWEND)
- End A Job LCKW Watch (IEMLCKWEND)
- End A Job THDW Watch (IETHDWWEND)
- End Output Queue Watch (ENDWCHOQ)
- End Device Watch (IEMDEWEND)
- End Certificate Watch (ENDDCMW)
- End User Expiration Watch (ENDUXW)
- End A Network Watch (ENDNETW)
- End Connection Watch (ENDCNNW)
- End Message Que Monitor (ENDIEMON)
- End Audit Scan (ENDSCAN)