Mitchell Humphrey

FMS III Phase 4 Enhancements

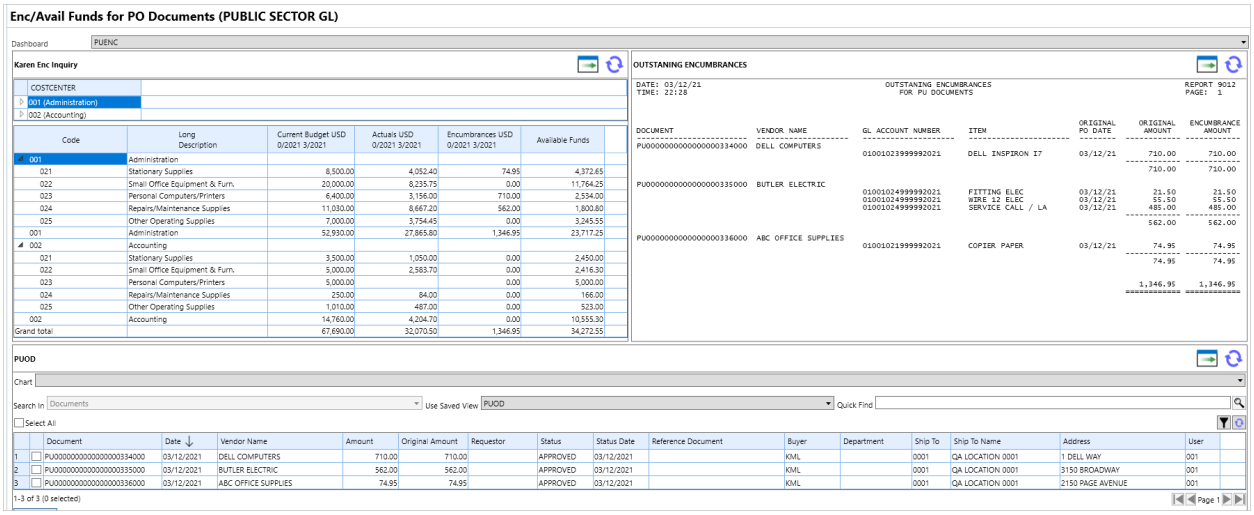
Quick Reference Guide

4-15-2021

Contents

FMS III Dashboards

Dashboards provide a way of viewing summaries of your operational data on a single screen.



Purpose and Availability

Dashboards allow online retrieval and display through a variety of FMS inquiry and reporting mechanisms and are available in all FMS Systems.

Security Capability

Listed below are the security capability numbers used for Dashboards and Charts.

- 706 — Maintain Dashboard
- 707 — Display Dashboard
- 708 — View Public Dashboards
- 709 — View Shared Dashboards
- 710 — Maintain Public Dashboards
- 711 — Use Personal Dashboard
- 712 — Share Personal Dashboard
- 713 — Set Own Default Dashboard
- 714 — Default Dashboard Assignment
- 715 — View Public Charts
- 716 — View Shared Charts
- 717 — Maintain Public Charts
- 718 — Use Personal Charts
- 719 — Share Personal Charts
- 721 — Dashboard OLI Module co-process (Always ON)

Scope

Each dashboard has a *scope* (sometimes called a *type*). The scope interacts with your security privileges to determine which dashboards you can view and/or modify. These are the scopes.

- **System**. System dashboards are defined and distributed by Mitchell Humphrey. Anyone who can view dashboards can view system dashboards. System dashboards can only be maintained by MH personnel.
- **Public**. Individual FMS customers may choose to define public dashboards. You can use public dashboards only if your security capabilities (below) allow it.
- **Personal (or Private)**. If your security capabilities allow it, you can define dashboards for your own repeated use. You may be able to share your personal dashboards with others. Unless shared, a personal dashboard is visible only to the person who created it.

Shared dashboards are a subset of personal dashboards. If your security capabilities permit it, you can optionally share any of your personal dashboards with others. Sharing for a given dashboard is all or nothing. If you share the dashboard, it is shared with everyone in the organization who can use shared dashboards.

Dashboard Concepts

You can define multiple dashboards, each focused on a particular type of data or organizational role.

Modules

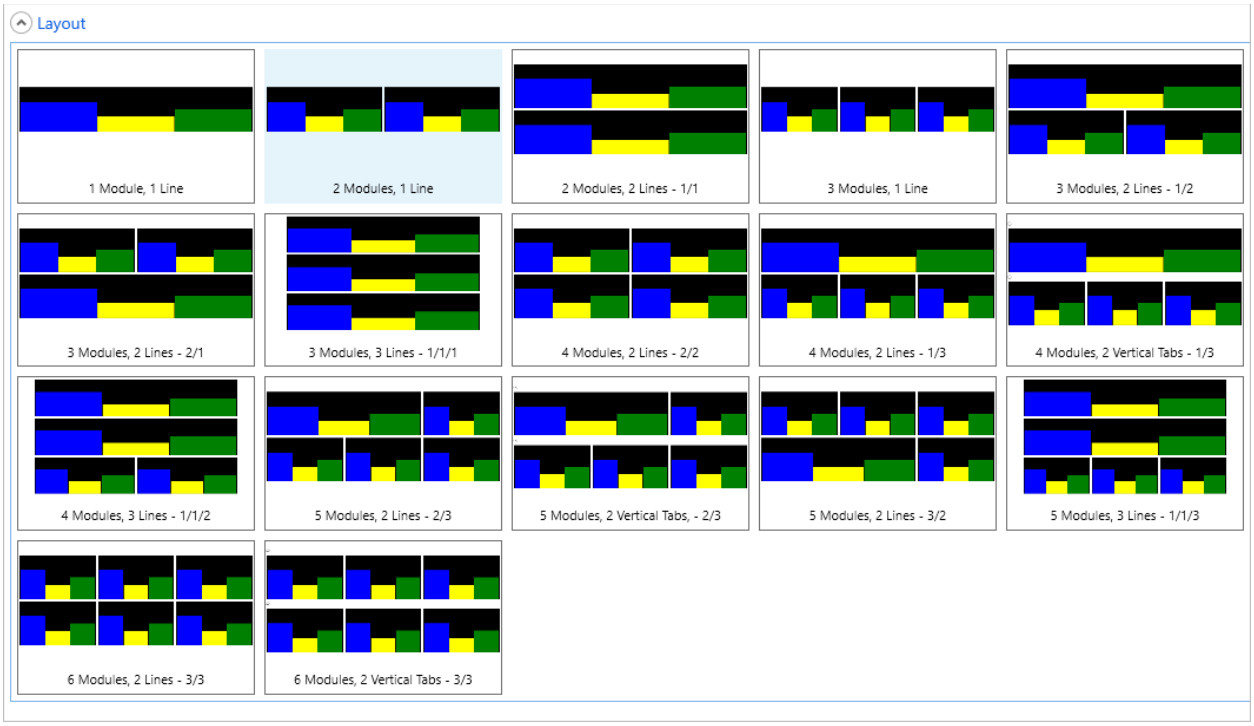
Each dashboard is composed of one or more *modules*. Currently, there are four different types of module. Each type is designed to display data using a particular inquiry or reporting tool.

- **Online Inquiry module**. Displays data from a single pre-defined online inquiry program.
- **List View module**. Displays data from a single saved list view.
- **Workflow action list module**. Displays your workflow action list.
- **Report Writer module**. Displays data from a single pre-defined reporter writer report.

The online inquiry and report writer programs used in those modules may have *prompts* and the dashboard framework provides a means for storing prompt values. There are special provisions for automatically changing prompt values related to fiscal period and year. Prompt values are always provided by the framework and cannot be changed interactively when the dashboard is displayed.

Layouts

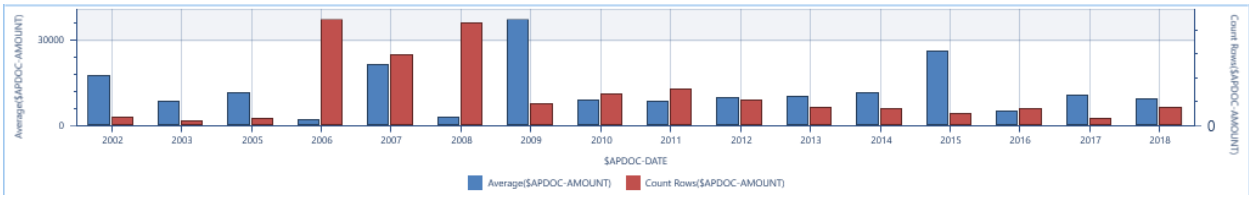
Each dashboard has one of several pre-defined *layouts*. The layout determines the maximum number of modules that the dashboard can hold. It also determines how the modules are arranged on the screen. Each layout provides for some combination of full width, half width, and one-third width modules on one or more rows. When you create a dashboard, you choose the layout, which is best suited to the set of modules you want to display.



When you place modules onto the dashboard, you specify the *contents* (for example, the online inquiry program or saved list view to display) of the module, values for any prompts required by the content, and a *title*. The title identifies the module in the dashboard display. The content and prompts determine the data which is displayed.

Charts

Dashboards also feature the ability to optionally *chart* the data displayed in a module. Dashboards provide a number of useful chart types, including bar, line, area and pie charts.



For detailed information on Dashboards, see the FMS III Dashboards manual on the Mitchell Humphrey web site.

FMS III InfoLink

The ability to selectively restrict access to individual attachments and optionally encrypt a secure attachment file has been added to FMS III Phase 4.

In addition, the following enhancements were implemented for attachments;

- Added the ability to drag and drop new attachments into FMS from file directories and other applications.
- Added ability to change the attachment name.
- Added the ability to double-click on an existing attachment in the list to open it.
- Include the attachment modify date on the attachment list.
- Added sorting for the columns on the existing attachments list.
- The record to which the attachment pertains to is now displayed on the attachment list.
- Added Application Event Logging for Attachments.
- The Add Attachments web service was updated for secure attachments.

Below is an introduction to secure attachments and the applied enhancements. For detailed information, see the FMS InfoLink manual on the Mitchell Humphrey web site.

Secure Attachments

This new feature allows your organization to selectively restrict access to individual attachments using FMS Selective Security.

Exempt from Selective Security Attachments

If Security Capability Number 699 is enabled for a role, then users assigned to that role are exempt from selective security and grant requirements are bypassed.

Exemption from Selective Security should be limited to only roles that truly have access to all the attachments in the respective system (A/P, A/R, etc.)

Secure Attachment Setup

Secure attachments are optional and will require additional setup to enable. When using this feature, an *attachment security class* is assigned to each attachment. Your security administrator grants various rights for the class to FMS security roles. Your role membership, along with rights granted to those roles, determine what you can do with attachments in that security class.

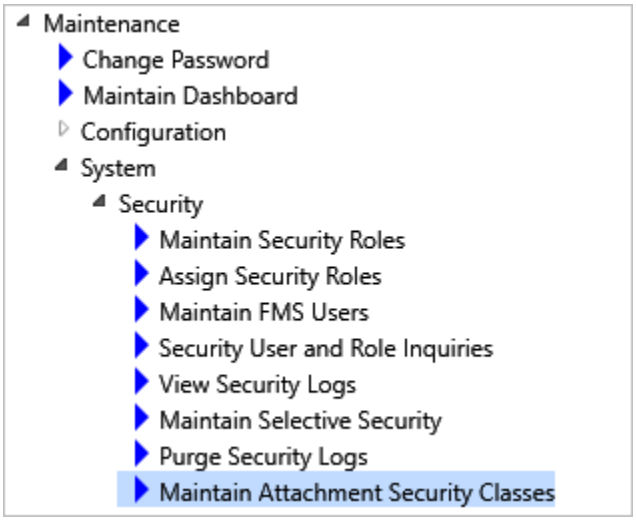
These are the rights associated with each attachment security class.

- View. Allows you to view existing attachments in this class.
- Edit (Modify). Allows you to modify existing attachments in this class.
- Delete. Allows you to delete existing attachments in this class.
- New (Add). Allows you to add new attachments in this class.
- Send-With. Allows you create an attachment of type SEND-WITH-DOC in this class.
- Execute (Run). This is a standard selective security right. It appears but does not apply to attachment security classes.

There is one standard security class, which is used for unsecured attachments. Typically, every user is granted all rights to this class. All other classes are specific to your organization.

Attachment Security Classes

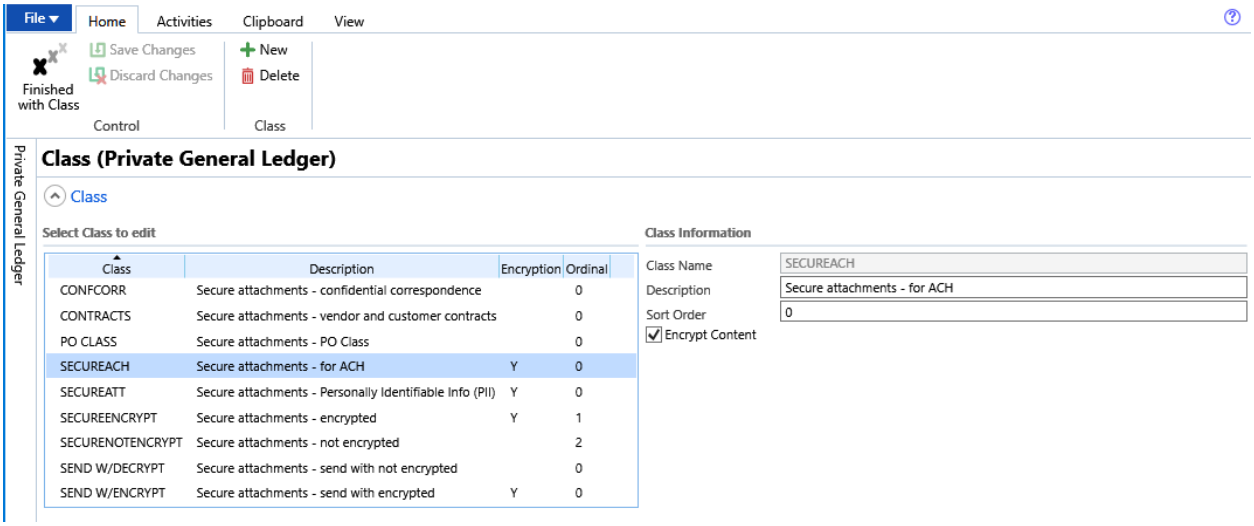
The new screen is accessible from the menu in any FMS system if Security Capability Number 720 is enabled. To open, select Maintenance > System > Security > Maintain Attachment Security Classes.



Attachment security classes are added, modified, and deleted from the **Attachment Security Class** screen. When you add or modify an existing class, the **Class Information** fields must be completed.

Encrypt Attachments

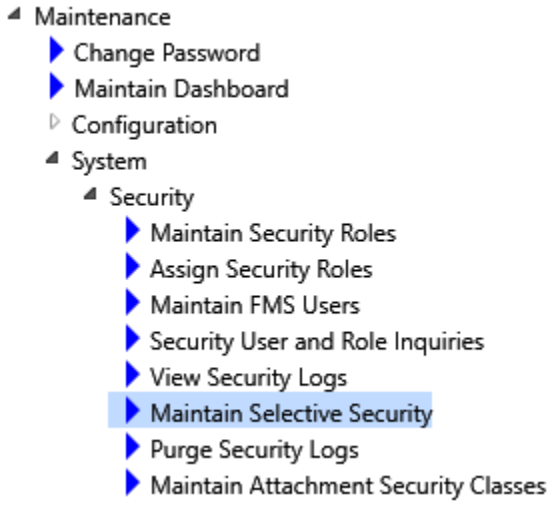
If attachments for the defined attachment security class are to be encrypted then the **Encrypt Content** checkbox should be checked.



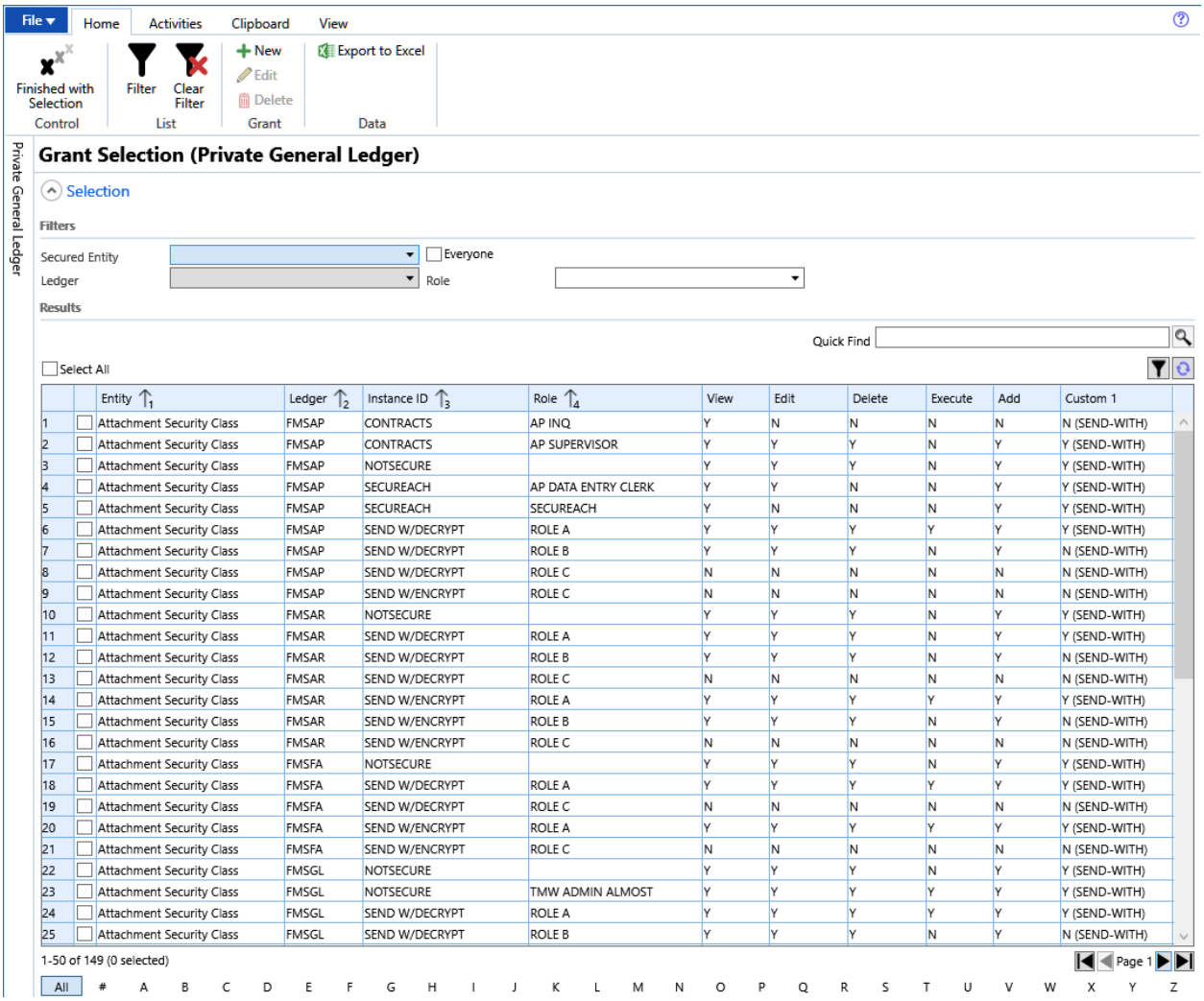
Assigning Rights for Classes

After creating attachment security classes, you must grant rights for those classes to FMS security roles or to everyone.

The rights assigned are configured in FMS Selective Security. To access Selective Security, select Maintenance > System > Security > Maintain Selective Security.

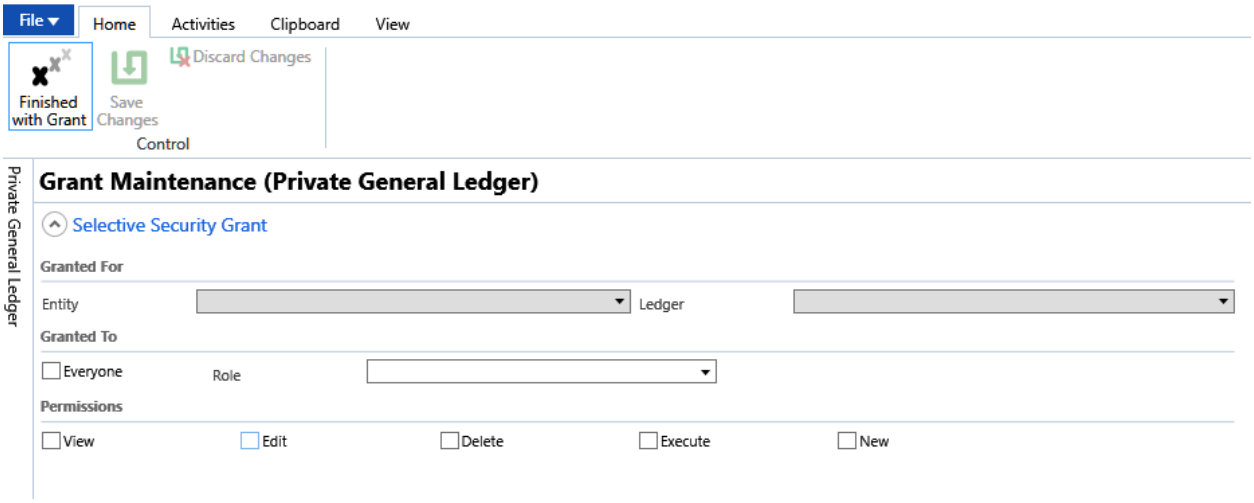


The Grant Selection screen will open with existing selective security records, if any, displayed.

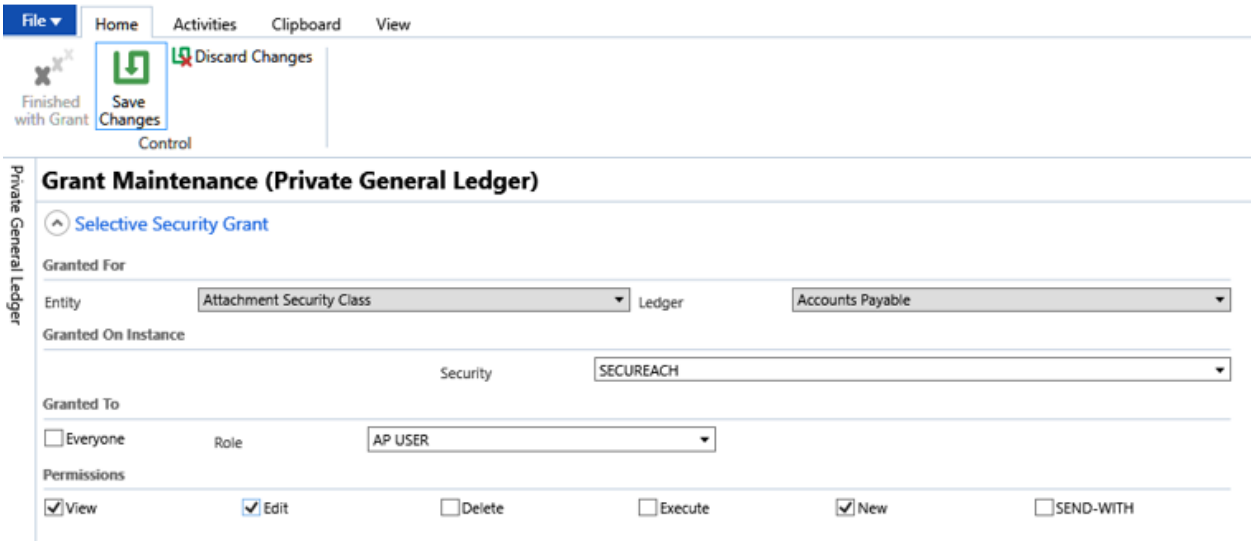


New Selective Security Grant

To create a new grant, click the "**New**" ribbon option. The Grant Maintenance screen will open.



Choose **Attachment Security Class** for the Entity and complete the fields for the Ledger, the Security Class, and the security Role in which the rights are granted. To grant rights to everyone, click the "Everyone" checkbox and leave the Role field blank, then check the Permissions box for each permission you want to grant.



Edit or Delete Selective Security Grant

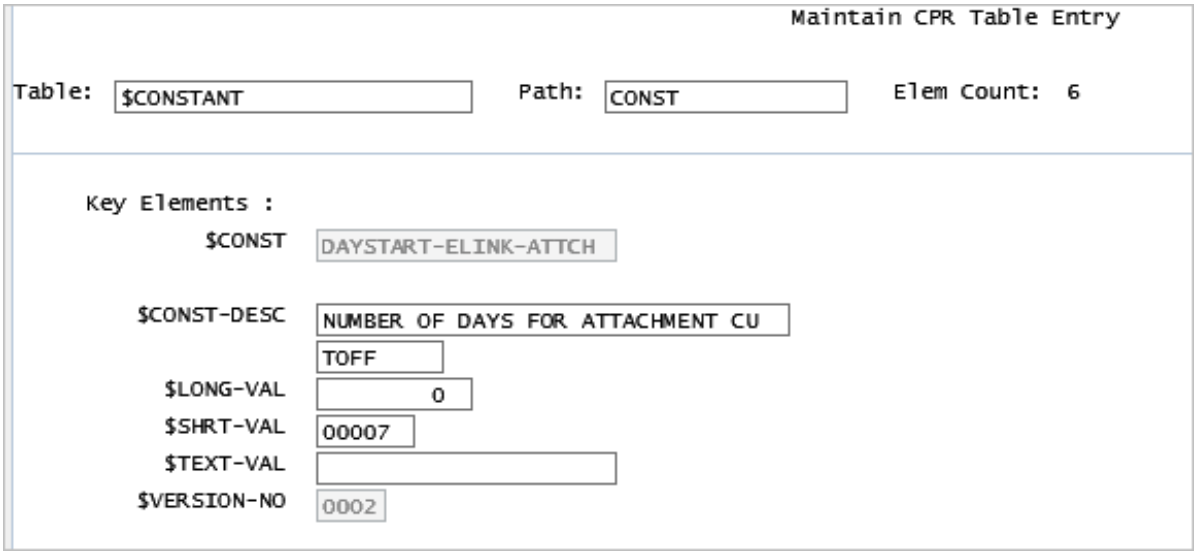
To modify an existing grant, select it in the list and click the **Edit** ribbon option. To delete one or more grants, select them in the list and click the **Delete** ribbon button.

Additional Configuration for Secure SEND-WITH Attachments

When a SEND-WITH attachment is added, the EDS file is retained in the EDS Email L->A and/or Print L->D folders on the account.

SEND-WITH attachments that are entered with a security class that is encrypted are not sent through FMS eLink as encrypted and therefore an unencrypted version of the file is placed in the eLink folder(s) mentioned above. To remove the unencrypted version of the file, Daystart was updated to include the deletion of these files, and the constant DAYSTART-ELINK-ATTCH was added.

The $SHRT-VAL setting on the DAYSTART-ELINK-ATTCH constant specifies the number of days that these EDS files are retained before Daystart deletes them. The default value is seven but it may be changed.



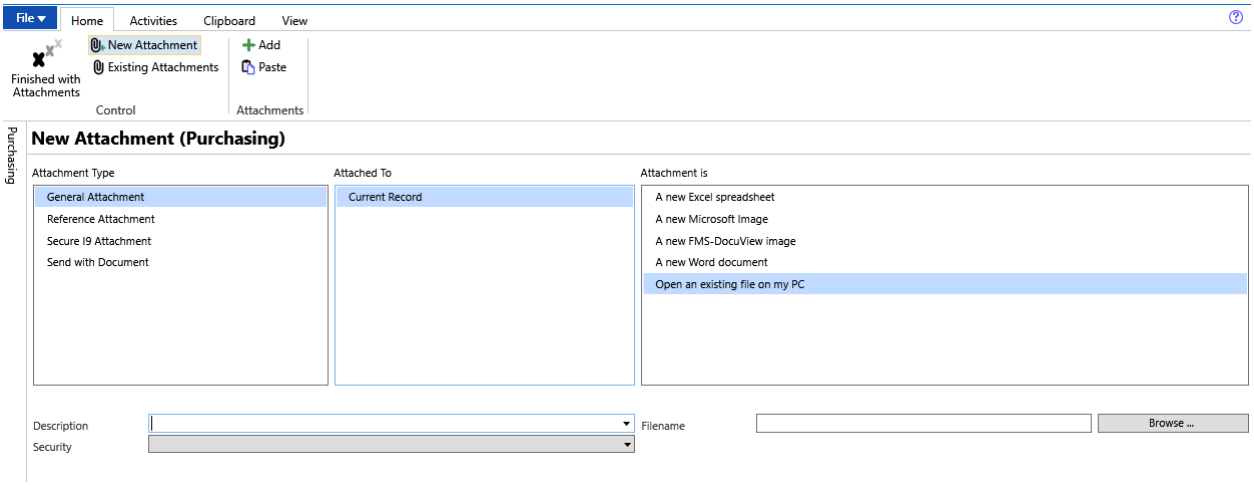
NOTE: After upgrading, attachments that were previously printed or emailed will be deleted from the noted EDS folders based on the constant setting when Daystart is run, so the first time Daystart is run, it may take a while to delete sufficiently old files.

Enhancements to the Attachment UI

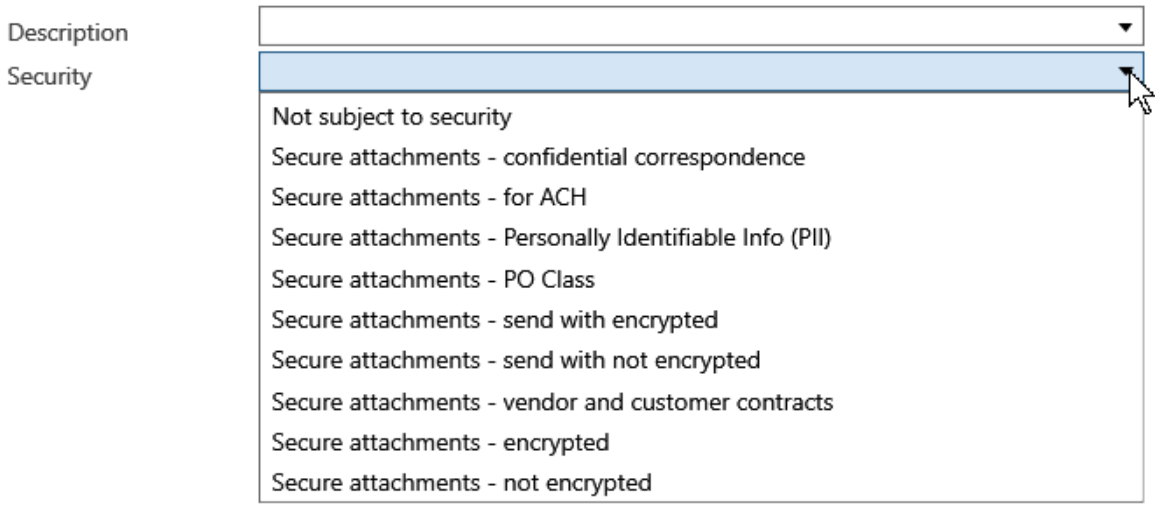
Both the New and Existing Attachments forms have been updated for "**Secure**" attachments. In addition, several enhancements were added to the Existing Attachments forms.

New Attachments

If attachment security is enabled at your site, the "Security" field will be displayed on both the **New Attachment** and **Existing Attachments** forms.

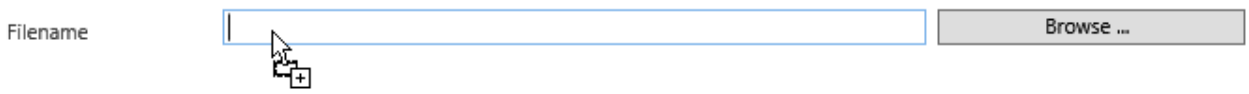


This Security drop down field contains the Attachment Security Classes for which you hold the rights to add an attachment.

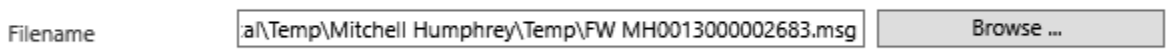


Drag and Drop Attachments

To Drag and Drop an existing file from another location (i.e., folder or from another application) to a new attachment, simply right click on the file and drag it to the **Filename** field on the New Attachments form and drop.

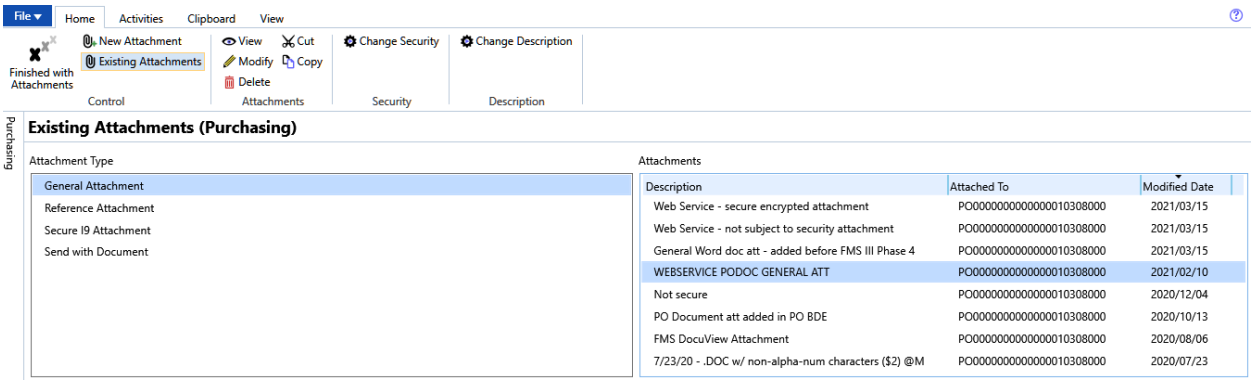


The path for the file will display in the field.



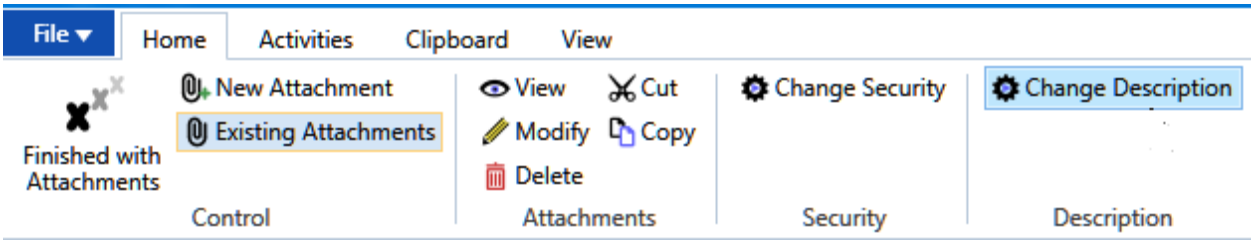
Existing Attachments

Several enhancements were implemented on the Existing Attachment form. Each of these are listed below.

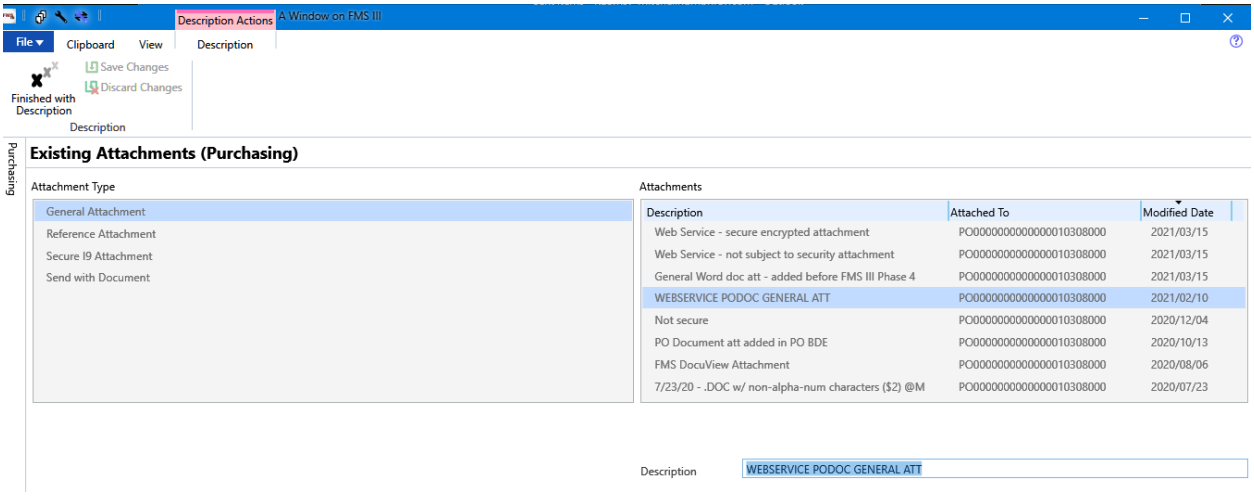


Change Description

To change the description for an existing attachment, a new ribbon option "**Change Description**" was added on the Existing Attachments form.



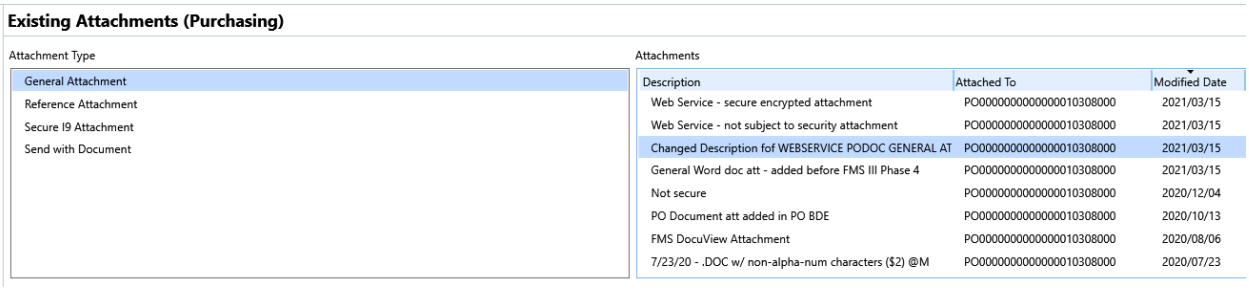
When an existing attachment is selected in the "Attachments" list and "Change Description" is selected, the "**Description Actions"** modal form below will open with the selected attachment description populated in the enabled Description field.



To change, simply type in the new description and click the "**Save Changes**" ribbon option, or click "Discard Changes" to revert to the original (or most recently saved) description.

Modified Date

The Modified Date column was added on the Attachments list. This is the date the attachment was added or the date the attachment was most recently modified.



Double-click on an existing attachment to open it.

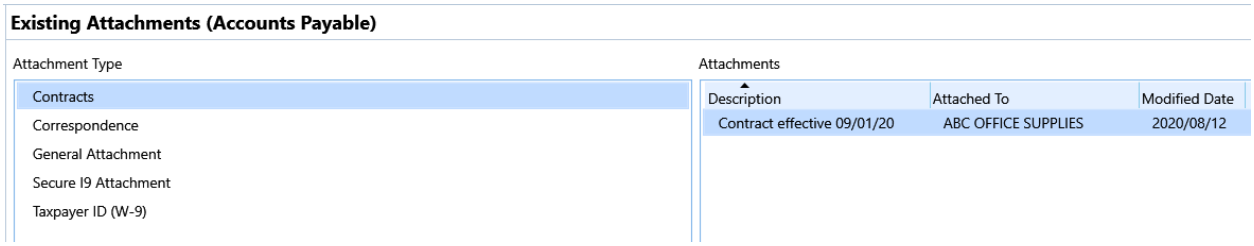
The ability to double-click on an existing attachment to open it has been added. When you double-click on an existing attachment, the attachment will open in View Mode.

Sorting on the Attachments in the list.

Added sorting on the Attachments list columns. To sort on any column, click the column Header.

Display the record for which the Attachment was added.

The "Attached To" column on the Attachments was updated to display the record for which the attachment was added. For example, the vendor name, document number, customer name, invoice…



Application Event Logging for Attachments

Event logging was added for attachments. Event logging for attachments will occur when;

- A new attachment is added in FMS.
- A new attachment is added via Web Services.
- A new attachment is added when copying and pasting from an existing attachment.
- When an existing attachment is modified.
- When the Description for an existing attachment is changed.
- When the Security Class on an existing attachment is changed.
- When an existing attachment is deleted.

Event Log Categories for Attachments are as follows.

1. ADD-ATTACH – Addition of new attachments. This includes Copied attachments, Drag and Drop attachments, and new attachments added via Web Services.

   Note: when a new Word document or Excel spreadsheet attachment is added (not via Browse to file), two event log entries are generated. They are;

   - ADD-ATTACH record with $MHC ATTACH-UI (Attachment User Interface)
   - MOD-ATTACH record with $MHC-ATTACH-COMP (Attachment Completion TX), which is generated when the added Word document or Excel spreadsheet is saved and closed.

2. MOD-ATTACH – Modification of attachments. This includes changing the attachment description.

3. DEL-ATTACH – Deletion of existing attachments.

4. CHNG-SEC-CLASS – Modification of the security class on an existing attachment.

Add Attachment Web Service

The Add Attachment web service was updated with the ability to add secure attachments.

The field "**AttSecClass**" was added to the Add Attachment SOAP Request to define the attachment security class to be applied to the new attachment, and the status return "**AttSecClass**" was added to the SOAP Response message.

The "AttSecClass" field is required in the Add Attachment SOAP request method if attachment security is enabled for the ledger specified in the web service request. When required, it must match an attachment security class that is configured in FMS. For a standard configuration, the element value would contain "NOTSECURE" for an unsecured attachment. Secured attachment classes are customized for your site.

If attachment security is enabled for the ledger then the following edits are performed on the attachment request for the specified security class;

- The security class entered in the SOAP request must be configured in FMS.
- The FMS User in the request must hold the security capability to add attachments in the specified ledger.
- The FMS User in the request must have *add permission* on the specified attachment security class in the specified ledger.
- If the attachment type being added is a "Send With" type, the FMS User in the request must have *send with permission* on the specified attachment security class in the specified ledger.

For more information on the changes to the Add Attachment Web Service, see the FMS III Web Services document on the Mitchell Humphrey web site.

Add Account Authorizations for Additional Data Files

This enhancement allows sites configured for encumbrance accounting to authorize accounts for actuals, encumbrances, and/or additional budget files when the original budget is posted, however it applies to any ledger batch regardless of the target data field. That is, it can be applied to budgets, actuals, or encumbrances.

This feature is optional and controlled at the batch type level. Following is an explanation of the $BATCH-TYPE-OBJ table elements used to enable this new feature.

- $BT-ADDL-AUTH, X1 – This new element was added to the $BATCH-TYPE-OBJ table for additional data file(s) authorization. “Y” enables this feature. “N” or blank disables this feature.

- $BT-HDR-4 - If the $BT-ADDL-AUTH = “Y,” then the additional data files must be entered in this field. It should contain one or more data files aligned on two-character boundaries. For example, if you would like to auto authorize an account for actuals, encumbrances, and budget file A, the value entered in this field would be “A ENBA” (where “A” is entered with a space before or after). If nothing is entered in this field, then additional authorization is ignored.

When the feature is enabled and a new authorization is added, the batch posting report will display a message for each additional authorization and data file.

```
Report: Ledger Posting                          BUDGET C BATCH ENTRIES          Batch ID: CM000130     Date: 04/12/21
System: FMSGL                                     BUDGET CONVERSION             Beg Pd: 03             Time: 17:59
User: KLEW                                                                      End Pd: 03
Device:                                                                         File: C                Page No: 1

Account Posted                          Key Code   Reference           Data Ending Year And Source Amount
Account Entered                         Desc       Reference Date      Type Pd     Batch Amount     Prior Amount     Posted Amount
----------------------------------------- ---------- -------------------- ---- -- ---------------- ----------------  ----------------

                                                Entered Amounts Represent Increments
                                                    Multiple Account Data Entry

01-011-0127-99999                       FMS Impl                        FFF  Yr: 21 Amount:         2400.00  Basis:     Spread:
                                                 04/12/21
                                                                              03         2400.00                            2400.00

*** Additional authorization succeeded for acct 01011012799999001 DF A  DT FFF.
*** Additional authorization via automatic account creation.
*** Additional authorization new authorization created.
*** Additional authorization succeeded for acct 01011012799999001 DF EN DT FFF.
*** Additional authorization via automatic account creation.
*** Additional authorization new authorization created.
*** Additional authorization succeeded for acct 01011012799999001 DF BA DT FFF.
*** Additional authorization via automatic account creation.
*** Additional authorization new authorization created.

                                    FINANCIAL TOTALS                                    STATISTIC TOTALS

                    ---NUMBER--- ------------------AMOUNT------------------  ---NUMBER--- ------------------AMOUNT------------------
                    DEBIT CREDIT        DEBIT                CREDIT         DEBIT CREDIT       DEBIT                CREDIT
                    ----- ------ -------------------- --------------------  ----- ------ -------------------- --------------------
NORMAL ENTRIES          1      0              2400.00                 0.00      0      0                 0.00                 0.00
SUSPENDED ENTRIES       0      0                 0.00                 0.00      0      0                 0.00                 0.00
REJECTED ENTRIES        0      0                 0.00                 0.00      0      0                 0.00                 0.00
                    ----- ------ -------------------- --------------------  ----- ------ -------------------- --------------------
     TOTALS             1      0              2400.00                 0.00      0      0                 0.00                 0.00

                                Batch messages: 0 Error, 0 Warning, 9 Informational


                                            *** End of Report ***
```

Event Logging for Account Maintenance

Event Logging for Account Authorization has been added to FMS III. This feature is optional and requires additional set up for logging to occur.

Some account authorization will create several Application Event Log entries so you will need to decide if you want to log entries for Add Account authorization, Modify Account authorization, or both, and for which ledger(s) you would like logging to occur.

When event logging is set up for Account Authorization, logging will occur when an account authorization is added/edited from Account Maintenance functions; New Accounts, Copy Accounts, Activate/Inactivate Accounts, and View/Edit Accounts. **NOTE:** Automatic account authorization generated through ledger batch posting will not be logged.

Setting up application event logging for Account Maintenance

Application event logging for Account Maintenance is optional so additional set up is required if you choose to log account authorizations. This set up is explained below.

Application Event Categories

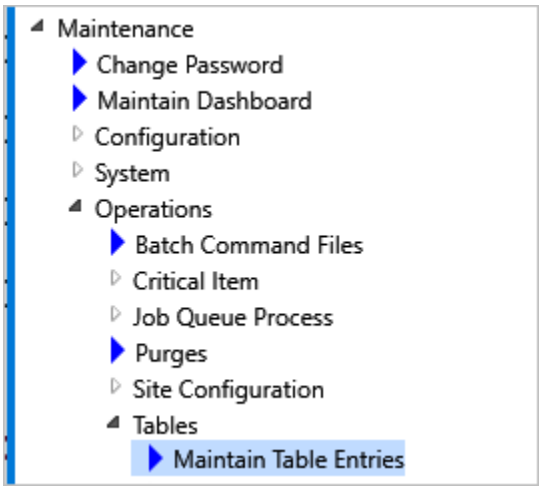
Event categories held in the table, **$APP-EVENT-CATEGORY**, represent the different types of events that are logged for Account Maintenance. The following $APP-EVENT-CATEGORY records are added by the upgrade and should not be changed.

- ADD-ACCOUNT
- MODIFY-ACCOUNT

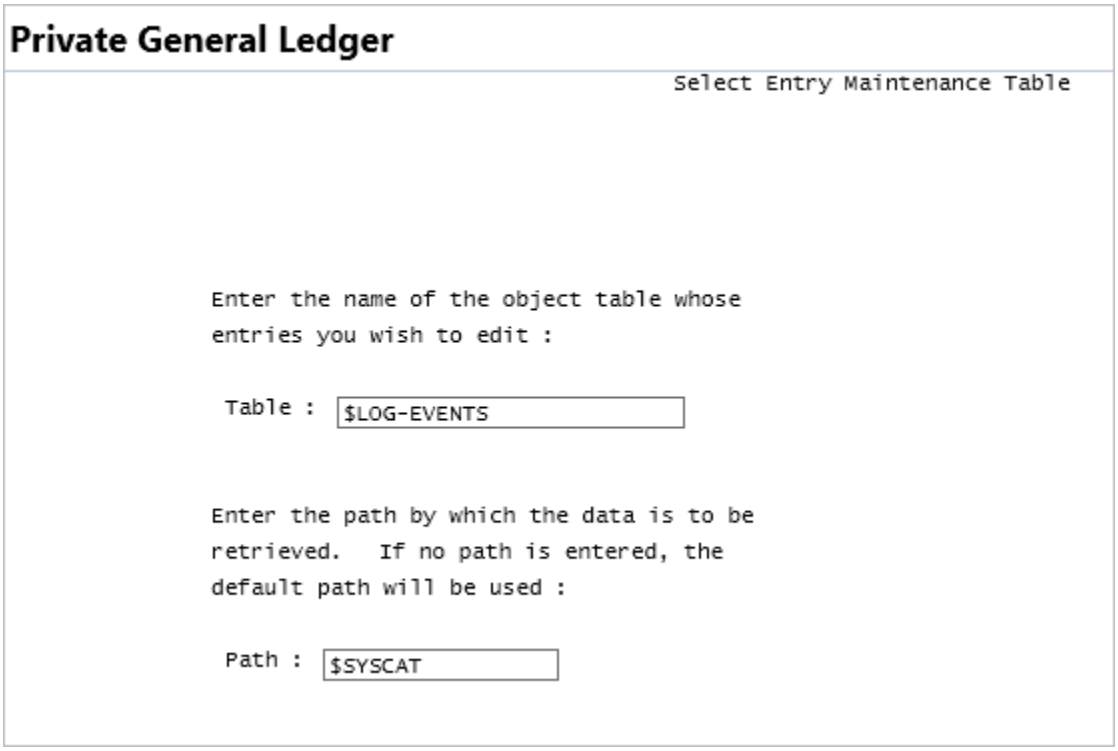
Log Events

$LOG-EVENTS entries are not added with the upgrade for ADD-ACCOUNT or MODIFY-ACCOUNT categories because logging account authorization information is optional, so $LOG-EVENT entries need to be added with the desired log values, if you choose to log this information.

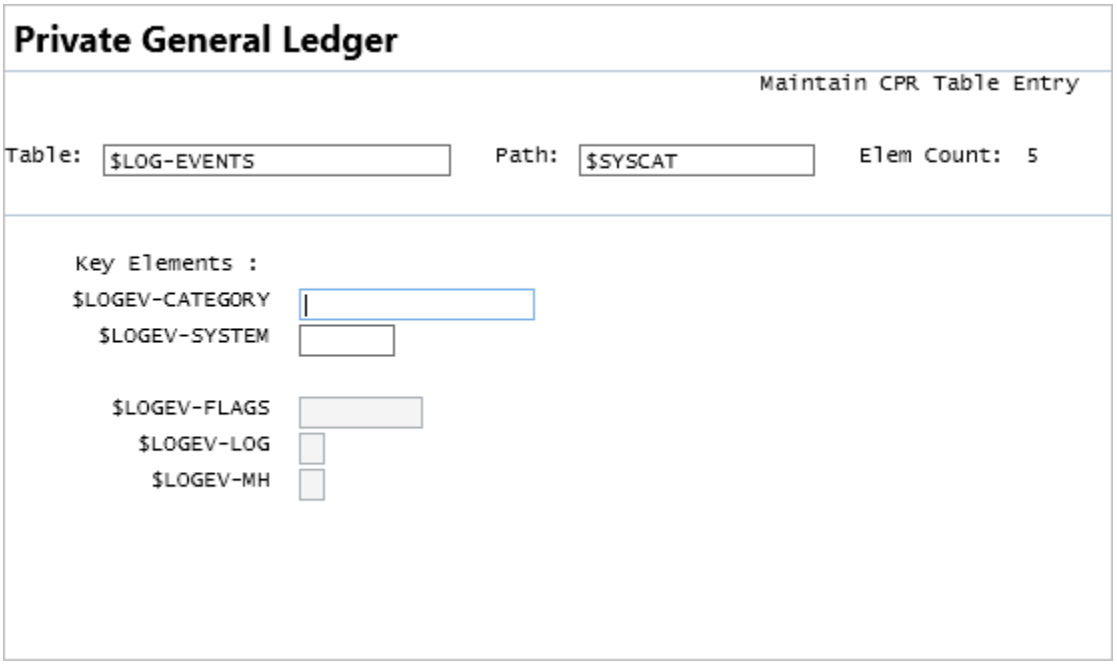
To access the $LOG-EVENTS table, select Maintenance > Operations > Tables > Maintain Table Entries from the menu tree or enter the command TEM.



Select or type the table name $LOG-EVENTS and Path $SYSCAT



Press Enter.



The elements in this table are described below.

$LOGEV-CATEGORY	The category to log. This should be set to ADD-ACCOUNT or MOD-ACCOUNT. If logging both add and modify events then a $LOG-EVENT record for each of them should be added.
$LOGEV-SYSTEM	This is the FMS system in which to log the event. If left blank, events for the category will be logged for all systems. To log data to a specific system, only enter the ledger name (I.E., FMSGL)
$LOGEV-FLAGS	This element should be blank.
$LOGEV-LOG	The log flag. **Y** to log the event for the System/Category, N do not log the event.
$LOGEV-MH	The Mitchell Humphrey record indicator. Set this to N. **Y** indicates that it is a MH record and will be removed during the next upgrade.

Logging Not Enabled

If there are no $LOG-EVENTS table entries for categories ADD-ACCOUNT and/or MODIFY-ACCOUNT then account authorization logging will not occur.

Logging Turned On

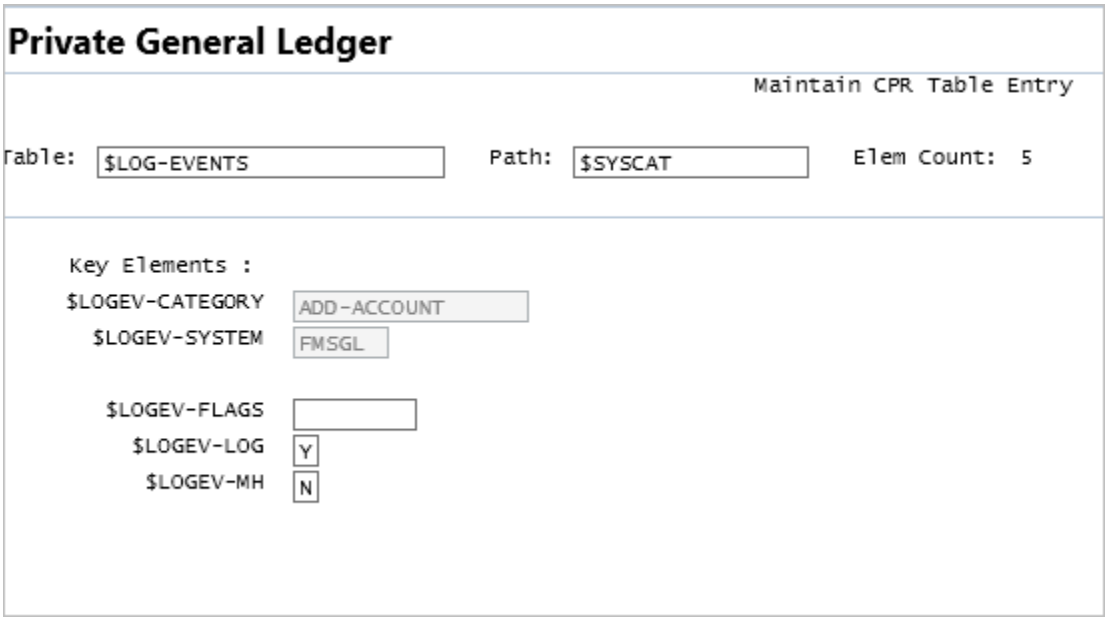
Open the $LOG-EVENTS table with path $SYSCAT.

To log new account authorization records, enter “ADD-ACCOUNT” in the $LOGEV-CATEGORY field and the desired system in the $LOGEV-SYSTEM field then press <Enter> and the F2 key to Add.

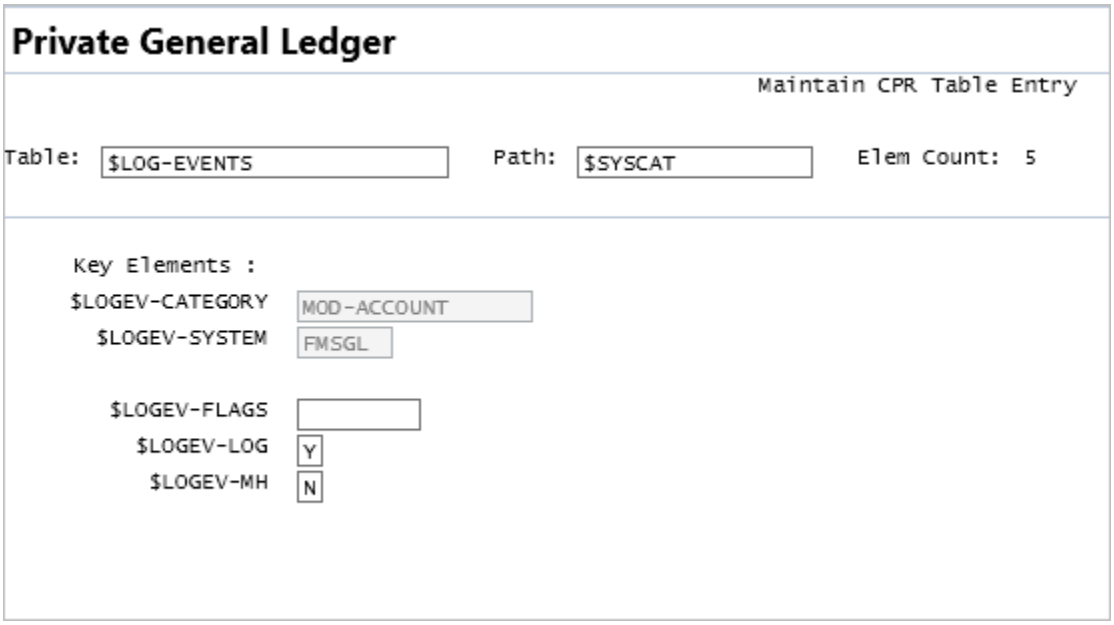
The remaining fields will open, enter “Y” in the $LOGEV-LOG field, and “N” in the $LOGEV-MH field. Press <ENTER> then click the F5 key to Finish.

In the example below, account authorizations that are added in FMSGL will be logged in the app_event_log table.

Note: Separate entries may be created for other systems, or the $LOGEV-SYSTEM may be set to blank for all systems.

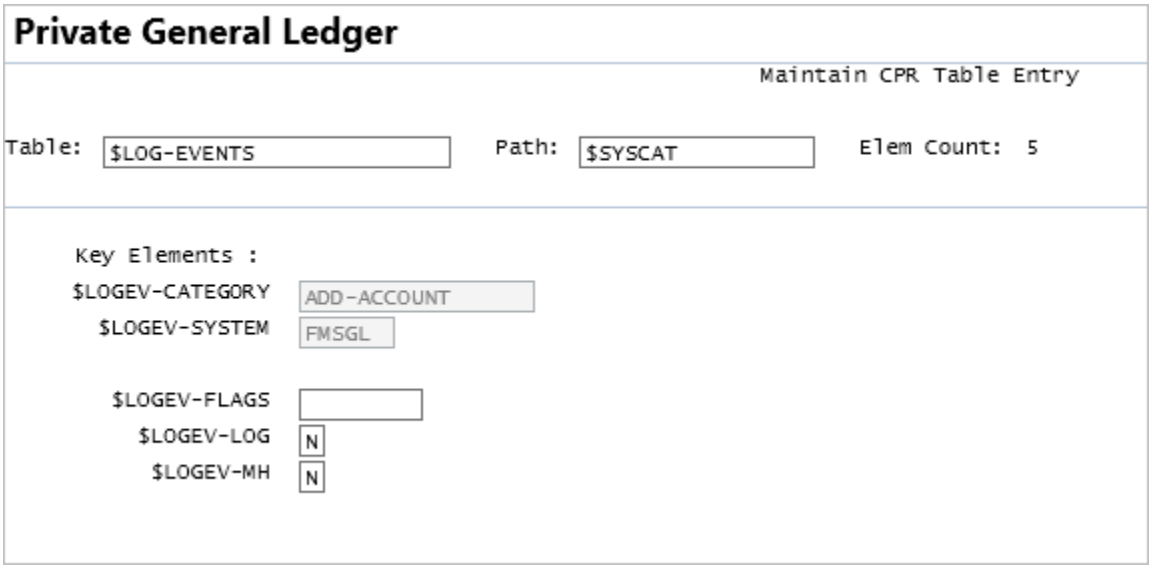


To log modified account authorization records to the application event log, add a $LOG-EVENT table entry for the MOD-ACCOUNT category with the desired ledger.



Logging Turned Off

To turn off logging for account authorizations, the $LOGEV-LOG value should be set to “N” in the $LOG-EVENT table for ADD-ACCOUNT and/or MOD-ACCOUNT categories.



FMS Purges

Several ledger purges were updated, and two new purges were added in FMS III Phase 4.

Updated Purges

The following Ledger detail transaction purges were updated to include the removal of detail transaction records that qualify from the tx_detail table, which was added in FMS III Phase 1. Note that a detail transaction record will only be purged if it is not associated with any other detail transaction(s).

- 0200 – DETAIL TRANSACTIONS – ACTUALS
- 0201 - DETAIL TRANSACTIONS – ENC/FC
- 0202 - DETAIL TRANSACTIONS – ALL BUDS
- 0203 - DETAIL TXS – SINGLE BUDGET
- 0204 - DETAIL TXS – ALL DETAILS

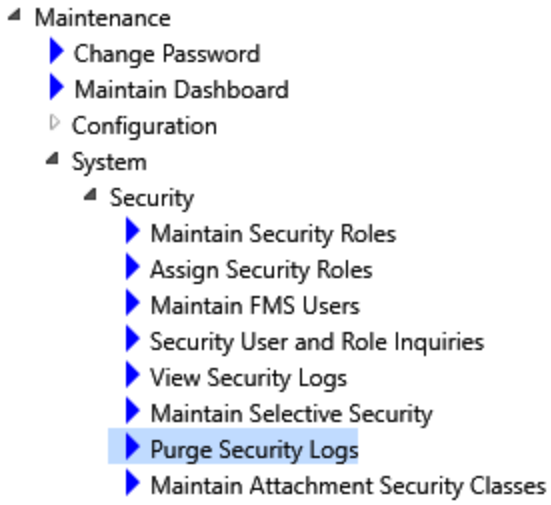
New Purges

The following purges were added.

Purge Security Log

A new purge “Purge Security Logs” was developed to remove historical Security Log data from the FMS database.

Purge Security Logs is not accessed from the Purges menu. It is only accessible from the Security menu in any FMS system if Security Capability Number 617 is enabled.



Absent User Purge

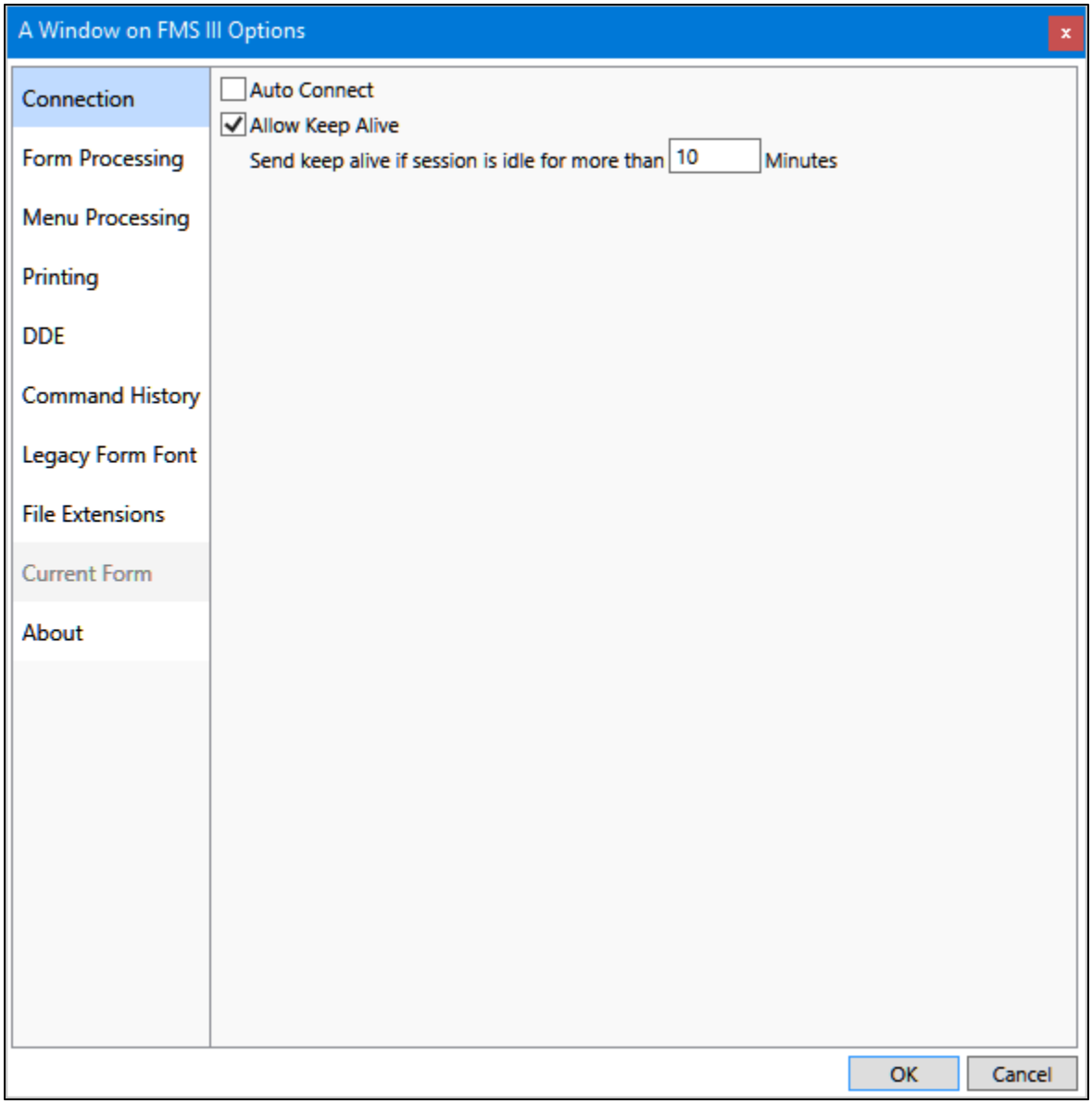
Purge 0400 "**Absent User"** was developed to remove historical Workflow Absent User records from the FMS database. This purge is accessed from the Purges menu.

For more information on Purges, see the FMS Operations manual.

WinUI "Allow Keep Alive" Feature

To prohibit FMS from shutting down when a WinUI connection is idle too long, a keep-alive feature has been added along with a "no-op" message that will periodically send to the server for idle connections.

To enable this optional feature a check box has been added on the "A Window on FMS III Options" form, which is accessed from the File tab on the ribbon. The keep-alive feature is enabled when the "Allow Keep Alive" check box is checked and disabled when unchecked.



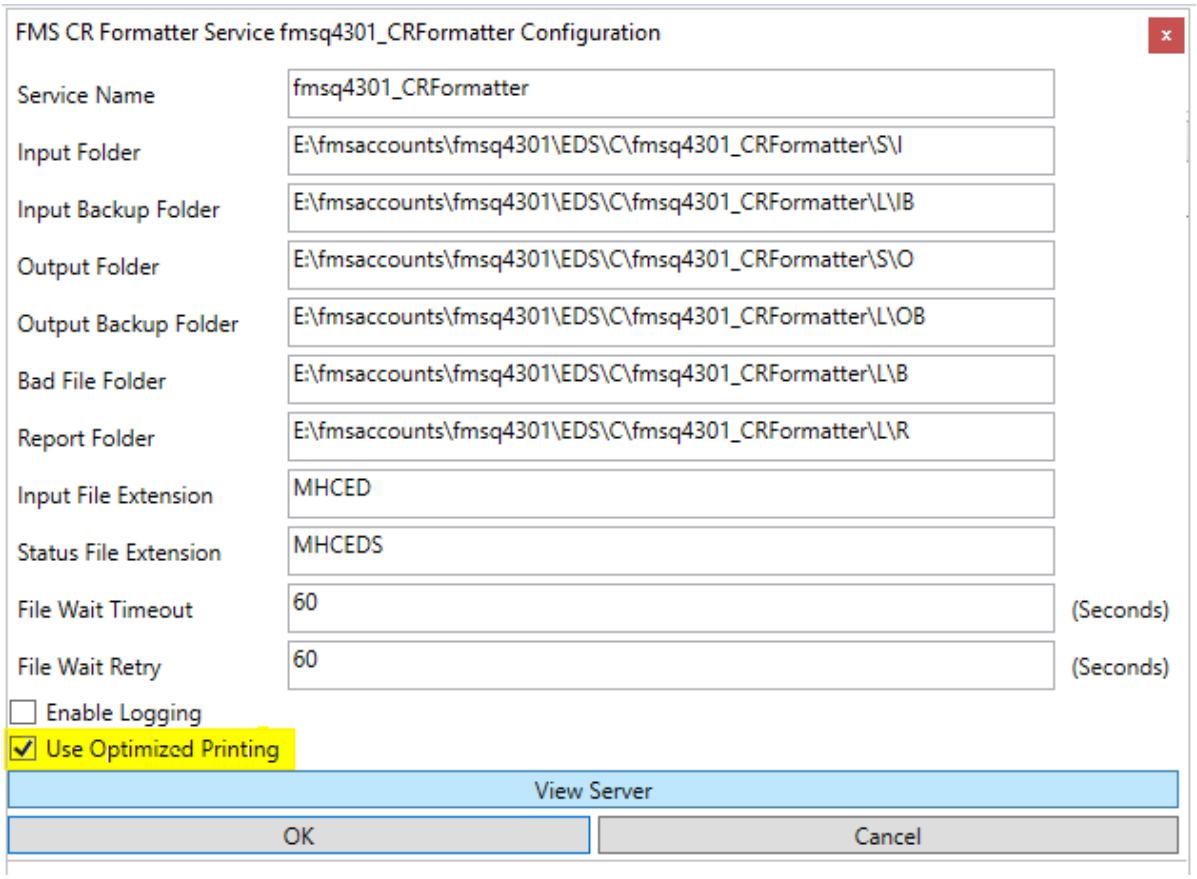
FMS eLink

Optimized Printing

In FMS eLink version 3.42.025, a supplementary print routine was implemented for CRFormatter. This optional print method was added to speed up the printing of Crystal reports from FMS eLink.

The original print method uses the printer-shared name on the device to determine which printer to print. The Optimized print method cannot use the printer share name, it must have the “real” printer name, and therefore a new destinations entry must be created.

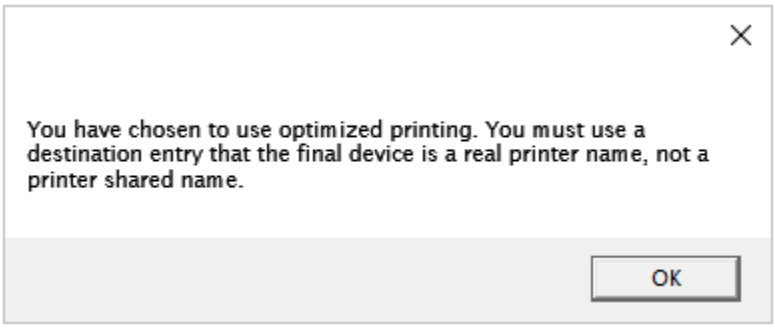
To configure optimized printing, open FMS III eLink Configuration Manager then select the CRFormatter Service to open the Properties dialog.



When you initially access the form, the “Use Optimized Printing” checkbox is unchecked, which is the default print method.

- The original print method is used when “Use Optimized Printing” check box is unchecked.
- Optimized Printing is used when the “Use Optimized Printing” check box is checked.

When “Use Optimized Printing” is checked, the message below is displayed reminding you that an output device must be set up in FMS ($DESTINATIONS-OBJECT table) with the “real” printer name entered as the final device.



Duplex Printing

Duplex printing capability was added to CRFormatter.

To use this feature at your site for existing eLink Crystal Reports, e.g. AR Statements, Purchase Orders, Invoices…, the custom rule or ProGen for the print job will require changes.