

eMARS NEWSLETTER

SEPTEMBER 13, 2018



Issue 2

POST GO-LIVE

It's September and we are moving right along. There have been some hurdles, however. This issue of our newsletter will address some of those.

Topics include; vendors, reporting, procurement and just understanding how things have changed, including password resets.

"If everyone is moving forward, then success takes care of itself."

Henry Ford

CUSTOMER RESOURCE CENTER

THANK YOU FOR YOUR PATIENCE

With the implementation of eMARS 3.11 the Customer Resource Center (CRC) has been inundated with calls and emails. In addition, we are working with limited staff. As a result, users may experience wait times. This has not occurred since 2006. Your patience and understanding is very much appreciated.

OUR eMARS COMMUNITY

Come join our eMARS community within MyPURPOSE. We are just getting started, but we hope this can be a place for users to collaborate with each other and with the eMARS team members. We also plan to post our manuals and other eMARS related documents. Let's see what we can do! Locate your MyPURPOSE icon on your desktop, then select the MyCOMMUNITY icon. Our eMARS Community is called **eMARS Elements**. Let's get talking and sharing!



eMARS Elements



PASSWORD RESETS

Now that we have two environments for eMARS and eMARS Reporting (3.10 and 3.11), password resets need to be clarified when coming into CRC. Here are some helpful tips to help us serve you better:

1. Send all requests **to our group email** box: Finance.CRCGroup@ky.gov
2. In your **subject line** please state: **Password Reset AND 3.11 eMARS OR the older 3.10 eMARS OR if it is for Reporting**
3. In the email body **please provide** your **User ID** and your name or at least have an email signature please. Your ID is required for the Reporting reset requests

You can save yourself time in the future by setting up for a future password reset by doing this below.

Once into eMARS successfully, do this below to do your own password reset in the future.



You must use the following criteria when changing your password:

8-16 characters (must contain letters, numbers and special character combination)

Must have at least one lower case and one upper case character

Must contain one of the following special characters: . @ # \$ % - (period, at sign, pound sign, dollar sign, percent sign, dash) Can't be similar to your previous 12 passwords.

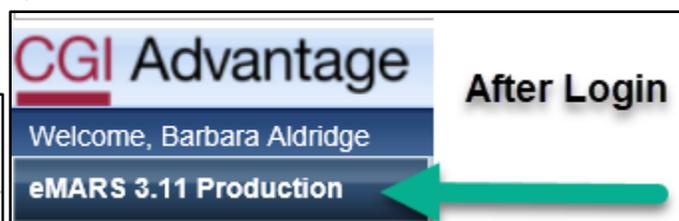
Set up your password hint by clicking on Administration. This will allow you to reset your own password next time. However after 3 bad login attempts your account will be locked and must be unlocked/reset by us.

Keep in mind eMARS 3.10, eMARS 3.11, eMARS Reporting 3.10 & eMARS Reporting 3.11 all have different logon credentials.

NEED A GPS?

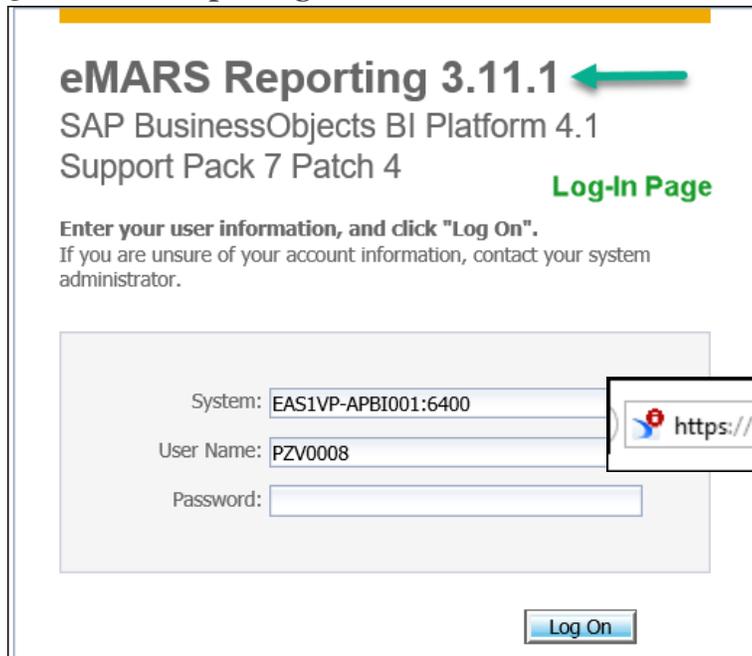
With two environments of eMARS and two of eMARS Reporting, users sometimes find themselves lost in the environments. Here are some identifiers to help you along the way.

eMARS 3.11

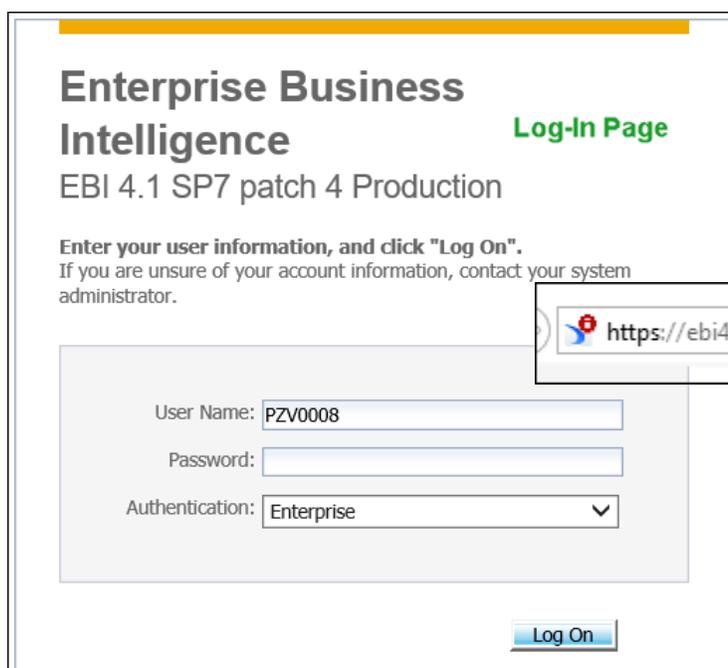




3.11 eMARS Reporting



3.10 eMARS Reporting



VENDORS

EMPLOYEE VENDORS RECORDS



During the pre go-live phase, the Office of the Controller stated that ALL employee vendors would not be included on the VCUST table. We loaded employees that had traveled in the year prior to soft go-live. Then later found out about a few atypical scenarios that were not accounted for, therefore, several more employee records were added around mid-July. If an employee is not on the Vendor Customer Table (VCUST) at this point, agencies will need to add them using a VCC document or use the spreadsheet upload process. **Employees CANNOT register through Vendor Self Service (VSS).** When adding employee vendors, please pay attention to the following:

- Employee ID must be used as the vendor number
- EZ Vendor Registration Form can be used to gather all information for VCC documents
 - <https://finance.ky.gov/services/statewideacct/Pages/UpgradeInfor.aspx> //
- Spreadsheet upload process may be used if you have several to enter
 - Contact Finance.CRCGroup@ky.gov for assistance

The Office of the Controller takes special measures to ensure all sensitive information is safeguarded. Please make sure that you store all sensitive employee data securely and destroy hardcopies if they are not needed.

UPDATING VENDOR ADDRESSES

When updating vendor addresses it is important to communicate with the vendor and ask the following questions:

- Is this a NEW address or and CHANGE to a current address?
- Is this a Payment Address or Ordering/Procurement Address or both?
- Do I have proper documentation from the vendor to make these changes?

Vendor records were consolidated from 3.10 and multiple addresses were added. Therefore, it is important to discuss any changes to the record with the vendor to ensure they are accurate before submitting your VCM.

PAY ATTENTION

With the upgrade to 3.11, CRC has received several calls from vendors who have received checks sent to wrong addresses and EFT's sent to incorrect bank accounts. In some cases, the data on the vendor record was incorrect and has been corrected. But in most cases, the agency simply selected the wrong vendor or address. Some vendors are marked in the Alias/DBA field to be used specifically by a particular agency or program.

Vendor/Customer	Legal Name	Alias/DBA	Vendor Active Status
✓ KY0033804	FRANKLIN COUNTY ✓		Active
KY0033847	FRANKLIN COUNTY FISCAL COURT	Homeland Security Use ONLY	Active
KY0040383	FRANKLIN COUNTY	JAIL COMMISSARY	Active

From 1 to 3 of 3 First Prev Next Last [Attachments](#)

Vendor/Customer	Legal Name	Alias/DBA	Vendor Active Status
KY0028918	KENTUCKY UTILITIES CO		Active
✓ KY0032446	KENTUCKY UTILITIES	CEMCS use Only	Active

From 1 to 2 of 2 First Prev Next Last [Attachments](#)

Unless you belong to the identified agency or your payment regards the identified program, DO NOT use that vendor. There will be another vendor number for use by all agencies.

Vendors have also reported receiving checks when they have valid EFT information on file. It appears users have been changing the Disbursement Format field. The Office of the Controller recommends letting the Disbursement Format field infer from the vendor record and not changing it. Below you will find the valid Disbursement Formats for EFT vendors. Please leave these as they infer from the vendor record.

<p>General Information Disbursement Options Invoice Information</p> <p>Disbursement Type: EFT</p> <p>Disbursement Format: CCD</p> <p>Scheduled Payment Date: 09/17/2018</p> <p>Disbursement Priority: 99</p>	<p>General Information Disbursement Options Invoice Information Agreement Reference</p> <p>Disbursement Type: EFT</p> <p>Disbursement Format: CTX</p> <p>Scheduled Payment Date: 09/10/2018</p> <p>Disbursement Priority: 99</p>
---	---

If you have a valid reason and require a paper check, you may change the Disbursement Format to **REG**, but only when necessary. There would never be a circumstance to change the Disbursement Format to anything other than REG.

COMMUNICATE PAYMENT INFORMATION

CRC gets several calls a day from vendors, receiving both ACH (EFT) and paper checks, who cannot properly apply their payments. The identifying information was not included on the payment document or was not included in the proper location on the payment document. Two fields are available to communicate to your vendors: **Vendor Invoice Number** (32 characters) and **Check Description** (first 24 characters). Both fields print on the check stub or in the email that goes out to ACH (EFT) vendors. In the case of ACH (EFT) vendors who are set up with a Disbursement Format of CTX, it is imperative that the proper information be included in the **Vendor Invoice Number** field.

Be sure to include the necessary identifying information, Invoice Number, Account Number, Case Number, Date of service, etc., in these two fields of your documents. Do not use the Document Description, Line Description, Extended Description or Commodity Description. These are not provided to the vendor.

<p>32 characters</p> <p>Vendor Invoice Number: 69201617</p>	<p>Attention</p> <p>Please Use Caution and do not enter confidential information in these fields such as Social Security Numbers, Credit Card Numbers or Bank Account Numbers, etc.</p>
<p>first 24 characters</p> <p>Check Description: Acct 5785987</p>	

Procurement News



EMARSCONVERSION2018

The cited authority, EMARSCONVERSION2018, used for payments against 3.10 contracts expired on August 31st. If you still have final payments remaining against 3.10 contracts, you may use Cited Authority FAP111-09-00-12 and attach a copy of the Assembled PDF from the 3.10 contract. Please be aware, this will go to the Office of Procurement Services (OPS) for approval.

COMMODITY CODES

When the commodity codes were last updated, you needed a DVD player to watch a movie, you needed a computer to surf the internet and a tweet was the sound a bird made. It was time for a refresh!

Some highlights:

- Modernized codes for products and services that didn't exist in 2006 when the codes were last updated
- Codes ending in "PS". Use the PS codes for professional services contracts (PON2's and MOA's)
- The previous commodity code for Freight/Delivery (59920) is now Transportation of Goods and Other Freight Services (96286)

Contact OPS if you need help locating a code.

WHERE'S MY PO2?

There is nothing left to say but good-bye PO2...

Use the following documents where the PO2 may have previously been used:

- The PO for goods and non-professional services
- The SC for university agreements, professional services and grants exempt from Governmental Contract Review Committee
- The PON2 for professional services subject to review by the Governmental Contract Review Committee
- The CTRP1 for Real Property

Here is a reminder of the Cited Authorities for the newer Award documents, the SC and CTRP1.

CTRP1 – Real Property Contract

Cited Authority	Agency
KRS56.800 – Property Rental	Various
KRS45A.300(4) – Interagency Real Property Lease	Various
FAP220-15-00 Acquisition of Real Property	Various

SC – Service Contract

Cited Authority	Agency
KRS177.035 - Cost of relocation of publicly-owned equipment	Department Of Highways
KRS177.280 - Agreements of local government units	Department Of Highways
KRS277.065 - Railway grade crossing maintenance payments	Department Of Highways
KRS39A.030 - Grant activity-Div of Emergency Mgmt	Department Of Military Affairs
EMW-2017-SS-00016 - FFY 2017 Homeland Security Grant Program	Office Of Homeland Security
KRS 65.7631(2) - CMRS Grant Funds	Office Of Homeland Security
KRS177.280 - Agreements of local government units	Various
KRS45A.690(1)(D)11 - Other Agreements-Not MOA	Various
KRS45A.690(1)(D)4 - University Agreements-Not MOA	Various
KRS45A.690(1)(D)7 - Nonfinancial Agreements	Various

From the Treasurer’s Office

REMINDERS FOR CRS & CACRS

When creating CRs and CACRs, please remember that the **Payment Type** drop down is now located in the Vendor section of the document on the General Information Tab. Be sure and select the correct **Payment Type** for your document. If you select Cash, Check, Money Order or Cashier’s Check do NOT check the **Suppress Pend Print** check box.



Payment Type:

- Cash
- Check
- EFT
- Wire Transfer
- Money Order
- Cashier's Check
- Payroll Deduction

Payment Type: ▼

Suppress Pend Print:

A MESSAGE FROM OUR BANK

JPMorgan Chase provided some beneficial information to remind us stay vigilant and avoid falling victim to cybercrime.

BE VIGILANT: Cybercriminals Are Using More Complex BEC Schemes

Cybercriminals are increasing the complexity of business email compromise (BEC) attacks, using the telephone as an additional method to increase the effectiveness of their campaigns, the FBI reports.

In a recent announcement, the FBI indicated that companies suffered more than \$3.6 billion in fraud losses over the last five years. Many of these losses are the result of BEC attacks, where criminals pose as executives or known third-party suppliers or vendors who send fraudulent payment instructions to a company's payments employee to induce them to send payments to a bank account controlled by the criminals. Often criminals compromise an email account or use lookalike or forged domains that are very similar to a legitimate address.

As organizations implement tighter security, criminals are modifying their own approach after launching a BEC attack by calling potential fraud victims to obtain employee names and contact information, and then attempting to gather additional personal data. For example, criminals are calling company help lines or using social media engineering to trick employees to provide information.

And as payments teams prepare for the final wave of summer vacations, it's also important to keep in mind precautions to help stop email, phishing and malware attacks. Cybercriminals will hack company email systems and actively monitor social media to learn when regular payments employees—and others with designated transaction authority—are away and temporary or less experienced staff are filling in.

Don't be fooled by these BEC schemes or by seemingly frantic calls that insist transactions must be done immediately. Always follow procedures and escalate anything unusual. Here are some tips organizations can keep in mind:

- Provide basic training and advanced education for employees to recognize BEC and phishing schemes.
- Monitor information that is available on the company's recorded phone lines, public-facing websites and social media accounts.
- Make sure temporary staff covering for your payments employees understand that criminals may pose as clients and vendors to try and manipulate them.
- Ask employees to refrain from posting summer travel plans and other personal information on social media.
- Do not provide payment information over the phone.
- Follow your established account payable internal control procedures to verify the identity of approved vendors and the propriety of their invoices.
- Validate payment requests and invoices—even if they appear to be from an internal employee—either in person or by telephone using a known telephone number.
- If you become suspicious before or after sending a payment, contact us immediately.
- Do not open emails from strangers, click links or download files that could be loaded with malware.
- Avoid using public USB charging stations and Wi-Fi in hotels and airports, which may be convenient but are an easy way for others to access your data and account information. Never log in to sensitive accounts while on public Wi-Fi.
- Run anti-virus and anti-malware on your devices once you return.

“Phishing” emails are messages containing links to fake web sites which are meant to deceive unsuspecting readers into clicking the links and entering private information. Remember if you feel you have received a “phishing” email, do not open it. Report it to COT at COTPhishingNotifications@ky.gov

REPORTING NEWS

SOURCE REPORTING – SPREADSHEET UPLOADS TO COMBINE DATA



One option available to Report Developers for combining FY19 data with earlier data is to upload a spreadsheet to EBI and use it as a Data Provider for reporting. Once Java RTE is up to date, uploading a spreadsheet is easy: just click the “New” button at the top of the Documents panel, select Local Document, browse for the spreadsheet, and click “OK”. The spreadsheet will be uploaded to your “My Favorites” folder.

Using the spreadsheet as a Data Provider also requires Java RTE. When you create your report (or “Modify” and “Add Query”), choose “Excel” instead of “Universe” then select the uploaded spreadsheet. The query that appears is very similar to what you normally see, except that it includes all data in the spreadsheet – all columns and all rows.

The screenshot shows the 'Query Panel' window. On the left, there are sections for 'Object Properties', 'Query Properties', and 'Query Definition'. The 'Object Properties' section shows 'Name: Date', 'Qualification: Dimension', and 'Type: Date'. The 'Query Properties' section shows 'Name: Query 1', 'Source Path: /2018 Holb...', and a checked 'Refreshable' box. The 'Query Definition' section has an 'Edit settings...' button. The main area is divided into 'Result Objects' and 'Data Samples'. 'Result Objects' contains buttons for Date, Start, End, Hrs, Type, REG (R), 6ADL (+), Lunch (L), ANNL (A), SICK (S), COMP (C), FMLA (F), LNPA (-), AWOL (X), TOTAL, Net, _2, Extra Bal, ANNL Bal, SICK Bal, COMP Bal, FMLA Bal, and Note. The 'Data Samples' table has columns: Date, Start, End, Hrs, Type, REG (R), and 6AD. The table contains several rows of data, including a row for '1/2/2018 12:...' with values for Start, End, Hrs, Type (R), REG (R) (3.49999999...), and 6AD.

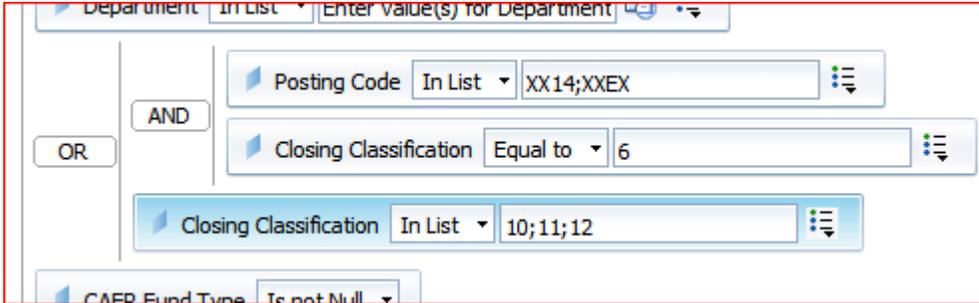
Date	Start	End	Hrs	Type	REG (R)	6AD
1/2/2018 12:...	12/31/1899 ...	12/31/1899 ...	12/31/1899 ...	R	3.49999999...	
	12/31/1899 ...	12/31/1899 ...	12/31/1899 ...	L		
	12/31/1899 ...	12/31/1899 ...	12/31/1899 ...	C		
	12/31/1899 ...	12/31/1899 ...	12/31/1899 ...	R	3	
	12/31/1899 ...	12/31/1899 ...	12/31/1899 ...	+	1	0
			12/31/1899 ...		7.49999999...	0

You cannot use query filters on the uploaded data, but you can remove columns from the report after you run the query and use table filters (or report filters) to narrow down the data displayed.

UPDATING REPORTS TO REFLECT CONVERTED AMOUNTS

Do your budget reports still show inaccurate balances for grants or capital projects? The problem may be missing converted amounts for expenditures, revenues, program income or charges.

For expenditures on Capital Projects, if your report filters based on Closing Classification, to include converted expenditure amounts you should update those filters as follows:



The screenshot shows a report filter interface with the following filters:

- Department: In List (with a search box for "Enter value(s) for Department")
- Posting Code: In List (with values "XX14;XXEX")
- Closing Classification: Equal to (with value "6")
- Closing Classification: In List (with values "10;11;12")
- CAER Fund Type: Is not Null

The filters are connected by "AND" and "OR" operators.

(The Posting Code for eMARS 3.11.1 converted expenditures is "XXEX". "XX14" is not required; it may already be in your filters since it was the conversion Posting Code for eMARS 3.10. There's no harm in leaving it there.)

Similarly, Capital Projects reports for revenue may need filters updated to include Posting Code = "XXRV". Capital Projects converted amounts are posted in Fiscal Year 2019, Accounting Period 1 on JVA documents with Document IDs beginning with "CONV" (e.g., JVA 660 CONV00000120).

For Federal Grant reports, the conversion posting codes are "XXEX" (for expenditures), "XXRV" (for drawdown revenue), "XXGI" (for program income revenue), and "XXPC" (for non-reimbursable charges).

Converted amounts for grants are posted in Fiscal Year 2019, Accounting Period 1 on JVC documents beginning with "C" followed by the Department code, the Program code, and the Program Period code (e.g., JVC 721 C721010500OL16 for Department 721, Program 010500OL, Program Period 16).

The Statewide Reports for grants and capital projects are updated to reflect these amounts in balance calculations. Should you find balances that still do not tie to the inquiry pages in eMARS, please contact Diana Holberg (diana.holberg@ky.gov) in Statewide Accounting Services.



Customer Resource Center

502-564-9641

877-973-4357

Finance.CRCGroup@ky.gov

<https://finance.ky.gov/services/statewideacct/Pages>

