
Auditing Employee Access to CU*BASE Tools

Understanding CU*BASE Employee Activity Tracking Features & Data Center Employee Security

INTRODUCTION

This booklet describes special features your credit union can use to monitor and audit access to your files and activity on member data by your credit union employees, as well as activity initiated by a member of the client support teams from CU*Answers, CU*NorthWest, CU*South, etc., referred to as your “data center” employees.

CONTENTS

<u>OVERVIEW OF AVAILABLE TOOLS</u>	<u>2</u>
OTHER AUDITING TOOLS YOU SHOULD USE	3
USER IDS VS. EMPLOYEE IDS	3
<u>UNDERSTANDING DATA CENTER EMPLOYEE SECURITY</u>	<u>4</u>
OVERVIEW	4
DATA CENTER STAFF ID RULES	5
VIEWING A LIST OF DATA CENTER EMPLOYEE IDS	7
TOOLS FOR OUR SELF PROCESSING CREDIT UNION PARTNERS	8
<u>AUDITING EMPLOYEE ACTIVITY</u>	<u>9</u>
TRACKING WHICH EMPLOYEES ACCESS WHICH CU*BASE FEATURES	9
TRACKING ACTIVITY ON EMPLOYEE ACCOUNTS	11
TRACKING ACTIVITY PERFORMED BY DATA CENTER EMPLOYEES	12
TRACKING USER IDS THAT CAN LOG IN TO YOUR CREDIT UNION’S DATA	13
TRACKING WHICH DATA CENTER EMPLOYEES SIGNED ON (SELF-PROCESSORS ONLY)	14
<u>APPENDIX: DATA CENTER STAFF ID SETUP</u>	<u>16</u>

Revision date: July 30, 2015

For an updated copy of this booklet, check out the Reference Materials page of our website:
http://www.cuanswers.com/client_reference.php
CU*BASE® is a registered trademark of CU*Answers, Inc

OVERVIEW OF AVAILABLE TOOLS

<i>Tools Introduced In This Book</i>	<i>Tool & Location</i>	<i>Uses</i>	<i>See page</i>
<p>Tracking Which Employees Access Which CU*BASE Features</p> <ul style="list-style-type: none"> What CU*BASE menu commands are being accessed by CU employees and data center staff? What accounts are people viewing via Member Inquiry or Phone Operator? What accounts are being accessed via teller posting? 	<p>Audit Insider/Employee Activity on the Auditing Functions (MNAUDT) menu</p>	<p>Use this to watch for patterns of employees attempting to access commands to which they are not authorized, or surfing accounts in Inquiry or Phone Op.</p> <p>Useful in conjunction with other forensic research to detect patterns on accidental, unauthorized, or suspicious activity uncovered during other routine audits.</p>	9
<p>Tracking Activity on Employee Accounts</p> <ul style="list-style-type: none"> What activity is being performed on “special” memberships like employee and board member accounts? Are any employee accounts showing signs of potential fraudulent activity or other areas of concern? Who is performing transactions on accounts owned by members who are also data center employees? 	<p>Insider Audit/Due Diligence Rpt on the Auditing Functions (MNAUDT) menu</p>	<p>Use this to track all activity on memberships flagged with an insider code, performed either by a CU employee or Data Center staff.</p> <p>CU*TIP: Insider codes can be used to flag any accounts requiring special monitoring. If you have members who happen to be data center employees, you will receive an annual notification of these names by your data center. These accounts should be flagged and monitored the same as accounts owned by your own employees and board members.</p>	11
<p>Tracking Activity Performed by Data Center Employees</p> <ul style="list-style-type: none"> What transactions are being posted by CSRs and other data center staff? What file maintenance is being performed on by CSRs and other data center staff? Which CSRs and other data center employees are accessing member accounts? 	<p>Audit Data Ctr Employee Activity on the Auditing Functions (MNAUDT) menu</p>	<p>Use this to track all activity performed by data center employees, on any credit union memberships.</p>	12
<p>Tracking User IDs That Can Log In to Your Credit Union’s Data</p> <ul style="list-style-type: none"> Are User IDs being deleted promptly when employees leave the CU? Are there any User IDs that are not being used regularly? Are login passwords being changed periodically? 	<p>User ID Information & History on the Auditing Functions (MNAUDT) menu</p>	<p>Use this to perform regular audits of the User IDs that employees use to log in to CU*BASE. Ensure that there are no User IDs sitting idle and unused for an extended period, and make sure your credit union’s policies regarding who can log in to your data are being followed.</p>	13
<p>Tracking Which Data Center Employees Signed On <i>(for self-processing credit unions only)</i></p> <ul style="list-style-type: none"> What data center employees have been logging in to my system? 	<p>MNOP17 #18 Remote Access Tracking Query (OPER 17 > 18)</p>	<p>Our self-processing partners should use this to track data center staff who need to log in for any reason.</p> <p>Useful in conjunction with other forensic research to detect patterns on accidental, unauthorized, or suspicious activity uncovered during other routine audits.</p>	14

OTHER AUDITING TOOLS YOU SHOULD USE

- ◆ Credit union security officers should also be familiar with the set of **Employee Security Reports** available on the Auditing Functions menu (MNAUDT). These reports help you verify that your Employee Security settings are configured according to your credit union's policies. The reports should be reviewed regularly, especially immediately before and after any software release in which changes are made to CU*BASE menu commands.
- ◆ In addition to the reports described in this booklet (Pages 11&12), the **Audit File Maintenance** feature on the Auditing Functions menu, MNAUDT, can be helpful if researching changes made to various configurations and other settings (as well as maintenance performed on member accounts).
- ◆ Watch for possible fraud by watching the **Abnormal Activity Monitoring** tool (also available on the Auditing Functions (MNAUDT) menu) for unusual activity levels in high-risk categories (like EFT traffic), or for activity by member accounts flagged for special due diligence. Learn more in the [Abnormal Activity Monitoring](#) booklet (available on our Reference Materials page).
- ◆ Monitor entries posted to your general ledger by printing the **General Journal Report**, accessed via **Print GL History (daily)** on the CU*BASE General Ledger (MNGELE) menu. The report can be set up to display entries made with the J/E IDs of "WE" and "CU" used by CU*Answers and "XT" used by Xtend SRS.
- ◆ Keep an eye on how your products and services are set up in CU*BASE via the options on the **Management Review of Key Configurations** (MNMGMC) menu.
- ◆ For more details on policies to which our client support teams must adhere when working with your data, please refer to the Security section of the Special Interest Docs page of our website:

<http://www.cuanswers.com/resources/doc/special-interest-publications/>

USER IDS VS. EMPLOYEE IDS

Remember that User IDs are used to log in to CU*BASE, whereas Employee IDs are the 2-digit ID used to access various menu commands after logging in.

For online credit unions, User IDs can be added or deleted only by an authorized data center employee after proper paperwork has been submitted by a credit union security administrator. Self-processing credit unions control the User IDs for their own system. If data center staff need to remotely access the credit union's system, such as to install software upgrades or assist with a problem, a designated user profile will be used (see Pages 8 and 14 for more details on auditing this access).

Employee IDs are controlled by your credit union's internal security administrator using the CU*BASE Employee Security feature on the Management Processing/Active Beta Tests (MNMGMT) menu.

UNDERSTANDING DATA CENTER EMPLOYEE SECURITY

OVERVIEW

In order for us to assist our clients with day-to-day CU*BASE support issues and perform various daily and monthly processing tasks on their behalf, special employee IDs have been set up in all credit union libraries and are used by all data center employees.

In the past there were primarily two IDs used by all data center staff: 89 used by Client Service and other support personnel, and OP used by Operations staff when performing daily/monthly processing tasks. Starting in November, 2004, a new system was introduced that allows us to separate data center staff from credit union employees, and give each individual employee his or her own ID to use when performing tasks on credit union data in CU*BASE. This change had several obvious benefits:

- ◆ When someone leaves the data center's employ, it is not necessary to change a password manually on every credit union library; that individual employee's ID is simply suspended.
- ◆ Any activity performed by a data center employee on credit union files is logged using that individual person's ID, not a generic one used by others.

*As always, file maintenance or member transactions are performed only upon written request by an authorized credit union employee. Refer to the separate [CU*BASE Client Support Security Policy](#) for details.*

The "Alias" Solution

This system gives each online credit union complete control over what data center staff is allowed to do on their files, without adding additional maintenance chores for the CU or for the data center, and without using up more credit union employee ID numbers. This was accomplished by the use of a central, single file that stores IDs for data center employees, and the use of "alias" IDs on credit union Employee Security master files (such as the existing ID 89, or 93 for call center employees, etc., as outlined on Page 6).

The alias ID controls what menu commands can be accessed by any data center employee that is tied to that alias. So if employee 89 can do something, any data center employee ID that uses 89 as an alias can do it, too. If 89 is restricted, so are the corresponding data center employees. So all the CU security officer is responsible for is controlling the credit union's settings for 89.

NOTE: Data Center security is handled differently for our **Self Processing clients** that have their own IBM i systems. Please refer to Page 8.

DATA CENTER STAFF ID RULES

- Data center staff IDs will be stored in one central location (file name DCEMPSEC in library CUBASEFILE) and used by all online credit union libraries, so if a password needs to be changed or an employee added/deleted, it only has to be done once from any CU. This also means that if an employee leaves, the ID simply needs to be suspended; it is not necessary to access all individual credit union libraries and change the alias password. (The ID is suspended rather than deleted so that any previous activity by that employee would still be able to tie out to that employee's name.)
- Adjusting settings or resetting passwords for data center employee IDs requires a data center employee ID that has administrator privileges. (This administrator can adjust data center employee ID settings and passwords, but the CU is still responsible for the alias ID.) Online credit union security officers will NOT be able to reset a data center employee ID password. See Page 16 for additional information.
- Data center employee IDs will use separate expiration settings (regardless of the CU's normal settings):
 - ⇒ Staff ID passwords will require a minimum of 4 characters (alphanumeric)
 - ⇒ Password expires every 30 days
 - ⇒ One warning each day for 7 days prior to expiration
 - ⇒ Can't use the same password used the last 13 times
 - ⇒ The ID and password cannot be the same (this is also true for credit union Employee IDs); if they match, the system will treat like an expired password
- When an Employee ID password expires (or if the password is reset), the employee security window will note "password has expired." The option **Change Employee Password on the Main Menu (MNMAST) will be available to both CU and data center employees to change an expired password.** As always, an employee must know his or her password in order to change it.
- Each data center employee ID will be tied to an alias Employee ID on the credit union's employee security master. The alias Employee ID controls what menu options can be used by data center staff. For example:

<i>Data Center Employee</i>	<i>Data Center Staff ID</i>	<i>Alias on CU security master:</i>	
Mary Service	#S	89	Means that Mary, Fred, Sarah, and Tom can only do what 89 is authorized to do in the CU's employee security
Fred O'Perator	@O		
Sarah Programmer	*P		
Tom Systems	+T		
Sally Xtend	;X	93	Means that Sally can only do what 93 is authorized to do, meaning what the call center is authorized to do.

- Employee IDs used as aliases will be disabled in the Employee Security window (where an ID and password is entered) so that an individual staff ID must be entered to use any CU*BASE program. The same restriction will apply to miscellaneous programs such as Inquiry, Phone, Teller, etc., that do not use the Employee Security window.

- This system allows us to set up alias IDs with different degrees of access (such as an employee ID without access to OPER or other sensitive menu options). To start, data center IDs will use the following aliases for all online credit unions:

89	Client Services and other client support staff
90	Operations (replaces OP)
91	Systems
92	Programming and Quality Control
93	Xtension Call Center
9x	Various, used by Xtend, Lender*VP, etc.

NOTE: Alias IDs (89, 90, 91, 93, etc.) still must be set up in each individual CU's employee security master. Currently we reserve employee IDs 89-99 for data center use, including 9x where x equals a character A-Z.

- Any password assigned to an alias ID on the CU's employee security master will be ignored and not used. For example, CSR access cannot be controlled by simply changing the 89 password. Refer to the separate [CU*BASE Client Support Security Policy](#).
- The credit union is responsible for maintaining the alias; the data center is responsible for maintaining data center staff IDs.

When Data Center Staff IDs are Used vs. the Alias

When a CU*BASE screen requires an employee ID to be recorded, such as a loan interviewer ID, etc., CU*BASE will require a *credit union* employee ID to be entered. In these cases the alias ID would be used instead of the data center employee ID.

Whenever a program writes out an employee ID to a file behind the scenes (such as if a transaction is being posted, or when the system records a "last maintained by" ID, etc.), CU*BASE will use the actual ID being used, not the alias.

Situation	ID To Be Used	
	<i>Alias ID from CU Employee Security Master</i>	<i>Data Center Staff ID</i>
Accessing a menu command		✓
Accessing Member Inquiry, Phone Operator, or Teller Posting (or similar programs where there is no employee security window)		✓
Entering an Employee ID into an input field	✓	
Recording an ID behind the scenes (posting transactions, file maintenance, etc.)		✓

If it is necessary for a data center employee to access Teller Posting screens (typically for testing purposes only), the program will be accessed using the data center staff ID, but the system will use the *alias* teller drawer number (for example, if staff ID "&A" was alias 89, &A would be used to access Teller

Drawer Control and Teller Posting, but employee ID 89 would be activated as the drawer). Again, this applies primarily to test libraries and other testing situations.

VIEWING A LIST OF DATA CENTER EMPLOYEE IDS

There are several ways you will be able to see a list of data center staff IDs and names. Remember that for online credit unions, maintenance of these IDs can be done only by an authorized data center employee.

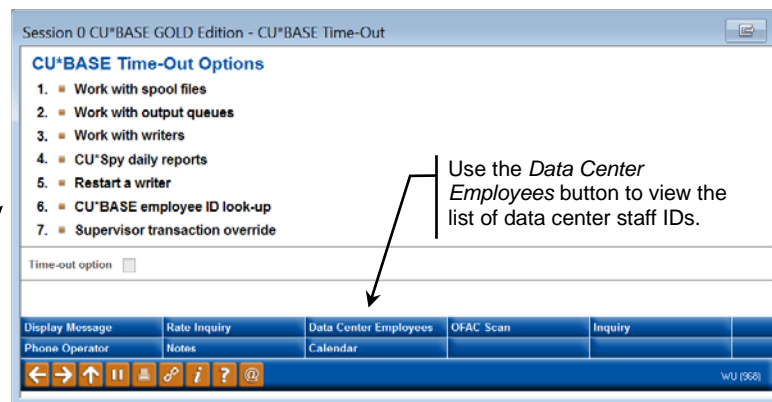
“CU*BASE Employee Security” on the Management Processing (MNMGMT) menu



Use the DC Employees button to see a list of IDs and names for data center employees.

When working in other programs, if you need to look up the name for a particular employee ID (whether CU or data center staff), access the CU*BASE Timeout window:

Timeout Window



Use CU*BASE Employee ID lookup (#6) to view a list of credit union employee IDs.

Use the Data Center Employees button to view the list of data center staff IDs.

On miscellaneous CU*BASE screens where an Employee ID must be entered manually (such as recording an Interviewer or Underwriter ID when opening a loan account), the lookup feature will NOT show data center employees, since those IDs cannot be entered in those cases.

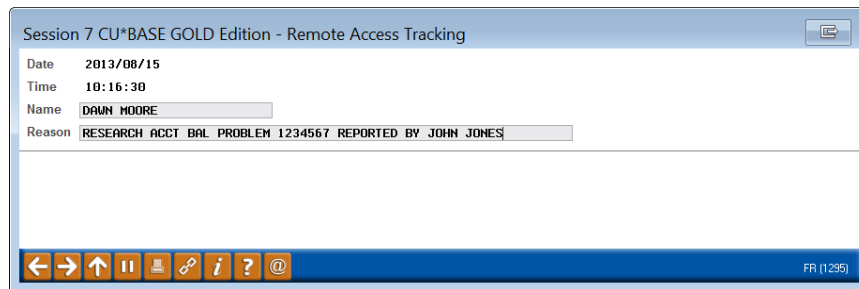
TOOLS FOR OUR SELF PROCESSING CREDIT UNION PARTNERS

Because the data center employee ID file resides only on our system, we will still use the generic employee ID 89 whenever it is necessary for us to work on a self processing credit union's system.

*As always, file maintenance or member transactions are performed only upon written request by an authorized credit union employee. Refer to the separate [CU*BASE Client Support Security Policy](#) for details.*

To allow you to control and audit situations where a data center employee accesses your credit union's system, there is a special file that will log information about the person logging in to your IBM i.

The following window will appear every time a data center employee logs in to your system:



Both fields must be completed before the user will be allowed to log in. For the name, at least two words must be entered (i.e., cannot be a first name only or initials), and the name entered cannot match the User ID used to log in.

See Page 14 for instructions on how to view the data gathered by this feature.

Once logged in the data center employee will use Employee ID 89 for any activity performed in CU*BASE.

AUDITING EMPLOYEE ACTIVITY

TRACKING WHICH EMPLOYEES ACCESS WHICH CU*BASE FEATURES

Employee Security features allow you to control and monitor access to CU*BASE programs by any employee ID, whether data center or credit union employee. Every time a program is launched from a CU*BASE menu, the system records who selected the command and when, as well as whether they were actually granted access to the application or not. For data center employees, the file records the individual ID for the staff member (not the alias) so you will be able to tell who from data center was doing the work.

The file was designed to let you see what commands an employee accessed, *not what they did while they were in there*. The Employee Security window where you enter your ID and password automatically records which program you accessed and when (even if you use Auto Security). Miscellaneous programs such as Member Inquiry, Phone Operator, Teller Posting, etc., that do not use the Employee Security window, will also record access details to the audit file.

This audit trail was not designed to replace the existing CU File Maintenance (CUFMNT) tool or other tracking tools such as recording last maintained date and ID for a specific program. Instead, it is an additional resource for detective work in cases where there is a question about some employee activity. An inquiry of this file will be available from the Auditing Functions menu:

“Audit Insider/Employee Activity” on the Auditing Functions (MNAUDT) menu

This is a “canned” Query of file **SECAUD** using the CU*BASE Report Builder. On the initial screen you can enter selection criteria such as Employee ID #, date, or program name. (Refer to online help for instructions on entering selection criteria.) Following is an example of the inquiry that will display:

Line	DATE	Emp ID	Employee Name	Account Number	Access Granted	Program	User	Work Station	Time (HHMMSS)	CU#
000001	08/08/2013	-N	NANCY	0	Y	MNOPER	NANCYB	#OCUANKBG1	10:32:39	113
000002	08/08/2013	-N	NANCY	0	Y	RRCNETCL	NANCYB	#OCUANKBG1	10:32:43	113
000003										
000004	08/08/2013	HW	KERI	266660	Y	CNFIRM QST	KERIC135	A613560	11:14:00	113
000005	08/08/2013	HW	KERI	266660	Y	CODE WORD	KERIC135	A613560	11:13:37	113
000006	08/08/2013	HW	KERI	0	Y	TSBMTB	KERIC135	A613560	11:13:16	135
000007	08/08/2013	HW	KERI	266660	Y	TSBMTB	KERIC135	A613560	11:13:22	135
000008	08/08/2013	HW	KERI	266660	Y	TSBMTB	KERIC135	A613560	11:14:00	113
000009	08/08/2013	HW	KERI	266660	Y	TSBMTB	KERIC135	A613560	11:14:00	113
000010	08/08/2013	HW	KERI	266660	Y	TSBMTB	KERIC135	A613560	11:14:00	113
000011	08/08/2013	HW	KERI	266660	Y	TSBMTB	KERIC135	A613560	11:14:00	113
000012	08/08/2013	HW	KERI	266660	Y	TSBMTB	KERIC135	A613560	11:14:00	113
000013										
000014	08/08/2013	MK	MICHELLE	90840	Y	IPHACT	MICHELK113	C211360	11:56:42	113
000015	08/08/2013	MK	MICHELLE	1051368	Y	IPHACT	MICHELK113	C211360	10:31:47	113
000016	08/08/2013	MK	MICHELLE	1051368	Y	IPHACT	MICHELK113	C211360	10:32:11	113
000017	08/08/2013	MK	MICHELLE	1051368	Y	IPHACT	MICHELK113	C211360	10:32:45	113
000018	08/08/2013	MK	MICHELLE	1051368	Y	IPHACT	MICHELK113	C211360	10:37:51	113

CU*TIPS:

- ♦ All Data Center Staff ID numbers are *less than* AA - which means they start with any special character except an asterisk (*) and end with a letter, number, or other special character. Credit Union Employee IDs start with numbers or letters and would therefore be *greater than* AA (because of how the iSeries sorts special characters before letters and numbers). This will make it easier to display just the employees you want to see on the inquiry.

To see only data center employee activity:

Combine (And/Or)	Field Name	Comparison	Criteria (Field, #, 'Text', etc.)
	SAEMPID	Less Than	'AA'

To see only credit union employee activity:

Combine (And/Or)	Field Name	Comparison	Criteria (Field, #, 'Text', etc.)
	SAEMPID	Greater Than or Equal To	'AA'

- ◆ The column labeled **Access Granted?** shows whether the employee was granted access to this option or not. If N, the employee attempted to gain access (whether accidentally or on purpose) but was stopped by the employee security program.

NOTE: A blank in the Access Granted column means that this record represents just one step in the access process (such as if your Privacy Controls require a code word and security questions to be entered); a separate record will show whether access was ultimately granted or not.

- ◆ If the employee name reads “**UNKNOWN**” the ID could not be found in either the credit union or the data center employee security files. This could mean an incorrect ID was entered when attempting to access the command, or the assigned alias ID does not exist.
- ◆ If an employee accesses Inquiry, Phone Operator, or Teller Processing, the system **will record an audit record for each member account that was accessed** during the session, even if the employee did not exit back to the menu between each account.
- ◆ The SECAUD file is a monthly file. To view data from previous months use file name **ESECmmyy**. (You may need to request a tape be loaded by a data center Operator. As usual, there is a nominal charge if this service is required.)

NOTE: If in the past your credit union did not require an Employee ID and password to access Member Inquiry, the Emp. ID and name will be blank. But effective in 2012, this feature is no longer optional, so all records should have at least an ID.

- ◆ When a Shared Branching employee assists your member, a record of the transaction will be recorded in the SECAUD file of both the member’s (home credit union) and teller’s credit union database.

TRACKING ACTIVITY ON EMPLOYEE ACCOUNTS

“Insider Audit/Due Diligence Report” on the Auditing Functions (MNAUDT) menu

This tool helps you monitor activity on memberships that you have flagged as “special,” including employee accounts, board member accounts, and even accounts that data center employees have with your credit union. There are four reports, each monitoring different types of activity, such as teller activity, transactions, and file maintenance. By using the *Data type* option, the same reports can also be used to monitor accounts you have flagged for special due diligence monitoring.

*TIP: Due Diligence Monitoring flags are configured by your credit union (via **Configure Due Diligence Codes** on the **General Configuration 1 (MNCNFC)** menu) and added to member accounts via **Update Membership Information** on the **Update Functions 1 (MNUPDT)** menu. Also see the “Abnormal Activity Monitoring” booklet for more tips on monitoring these special accounts.*

Refer to online help for complete details and report samples.

Here are some tips on using this tool from our Audit Link compliance experts:



“We recommend you monitor employee accounts by reviewing the Insider Audit reports once a week, looking for suspicious activity and to ensure internal procedures are being followed.

“Watch for large transactions, delinquent and negative balances, unauthorized overrides and loan changes, credits to employee accounts via G/L transfer, and inappropriate teller postings.

“The BSA requires that any employee living above their means should be reviewed. Use large transactions as a starting point when reviewing employee accounts.”

TRACKING ACTIVITY PERFORMED BY DATA CENTER EMPLOYEES

“Audit Data Ctr Employee Activity” on the Auditing Functions (MNAUDT) menu

The screenshot shows a software window titled "Session 0 CU*BASE GOLD Edition - TEST CREDIT UNION". The main heading is "Print Data Center Employee Audits". Below this, there are two columns: "Report Options" and "Response".

Report Options	Response
Report for period	From: 00000000 [MMDDYYYY] To: 00000000 [MMDDYYYY]
Reports to print:	<input checked="" type="checkbox"/> Job queue Copies: 1 Printer: P1
<input checked="" type="checkbox"/> Transaction activity review	
<input checked="" type="checkbox"/> File maintenance review	
<input checked="" type="checkbox"/> Account access/security audit	
<input type="checkbox"/> List only if access not granted	

i Are you printing the file maintenance review or account audit monthly? You must pick a range of one month spanning only one calendar month. Printing only the transaction review? In this case only, you may select any range of dates.

At the bottom, there is a navigation bar with icons for back, forward, up, down, search, help, and refresh. The version number "v11 (4544) 01/15/13" is visible in the bottom right corner.

This tool helps you monitor activity performed by data center employees on your credit union’s accounts. This includes shared-resource employees such as Xtend or Lender*VP.

NOTE: These reports are similar to the Insider Audit/Due Diligence Report already described. However, where those reports look at all employees but only for activity on special memberships, these reports look at all memberships but only for activity performed by data center employees.

Refer to online help for complete details and report samples.

TRACKING USER IDS THAT CAN LOG IN TO YOUR CREDIT UNION'S DATA

“User ID Information & History” on the Auditing Functions (MNAUDT) menu

User ID	User Name	Last Logged In Date	Last Password Change Date	Created Date
SIBARON		Jul 25, 2013	Jul 25, 2013	Jun 12, 2013
MONTICA		Jul 03, 2013	Jul 25, 2013	Jun 12, 2013
MARKESSA		Jul 22, 2013	Jul 15, 2013	Jun 12, 2013
BETHANN		Jul 27, 2013	Jul 27, 2013	Jun 12, 2013
BRANDON		Aug 07, 2013	Jul 30, 2013	Jul 24, 2013
JEFF		Aug 07, 2013	Aug 07, 2013	Aug 07, 2013
MIKE		Aug 09, 2013	Jul 30, 2013	Jun 12, 2013
STACY		Aug 12, 2013	Jul 26, 2013	Jun 12, 2013
EMILY		Aug 13, 2013	Jul 26, 2013	Jun 12, 2013
KATHRYN		Aug 16, 2013	Jul 26, 2013	Jun 12, 2013
LARREN		Aug 16, 2013	Jul 26, 2013	Jun 12, 2013
MARALIA		Aug 16, 2013	Jul 29, 2013	Jun 12, 2013
ROBIN		Aug 16, 2013	Aug 16, 2013	Jun 12, 2013
KAYLEE		Aug 19, 2013	Jul 30, 2013	Jul 24, 2013
SARAH		Aug 19, 2013	Aug 05, 2013	Jun 12, 2013
AMBERLE		Aug 20, 2013	Aug 12, 2013	Jun 12, 2013
CHRISTINA		Aug 20, 2013	Jul 26, 2013	Jun 12, 2013
DARCY		Aug 20, 2013	Jul 25, 2013	Jun 12, 2013
ELLEN		Aug 20, 2013	Aug 01, 2013	Jun 12, 2013

Use the **History** button to see a history of User IDs added, changed, and deleted

Use the **Print Report** button to generate a list of current User IDs (same as what's shown on this screen – just remember to keep this report secure!)

This tool is used to monitor the employees who are allowed to log in to CU*BASE and work with your credit union's member data. This tool shows User IDs authorized to your files, and the last time they logged in or changed their password.

To protect your data, whenever someone leaves your employ, their User ID should immediately be deleted. This tool helps you monitor to make sure that's being done properly. You can also see a history of password resets and other changes being made to your User IDs, either by data center employees (who are responsible for following your instructions to add or delete IDs) or your internal security officers (responsible for resetting passwords).

CU*TIPS:

- ◆ Inactive User IDs (where the last logged-in date is over 90 days ago) will be purged by an automated daily routine. Use the History button to view these IDs; purged records will show a “Performed by” name of SYSTEM.

For self-processing credit unions: The purge routine can be run manually but we recommend you automate it via ROBOT or IBM Job Scheduler. It can be set to any interval of days (90 is recommended). Contact a Production Center representative if you need assistance.

- ◆ User IDs that do not distinguish a credit union employee (such as AUDITOR, TEMP, TELLER, CREDITCOMM, etc.) are not allowed. To ensure the integrity of your data, only a credit union *employee* should be granted access to your credit union's files. Once a session has been established, a separate CU*BASE Employee ID can be created to give third parties access to your files as you see fit.
- ◆ Use the **Print Report** button to generate a report showing the data from this screen. BE CAREFUL! Since this report contains a list of user

names and IDs, if it is printed the output should be carefully secured to prevent its being used for social engineering security attacks.

- ◆ Click the **History** button to show a history of IDs added and deleted, as well as changes such as correcting a misspelled name or logging a name change after marriage or divorce. This history, shown below, also lists password resets done by a Client Service Representative on your behalf, including whether or not a fee was charged to your credit union for that service.

Purged records are user IDs that were deleted by the system automatically during the daily routine. User IDs are purged when the last logged-in date is more than 90 days ago.

User ID	User Name	Action	Action Date	Performed By	Fee
MACKENNA		Added	5/06/2013	HELENP	N
KATHRYN		Deleted	4/28/2013	HELENP	N
KAREY		Deleted	4/28/2013	HELENP	N
DONNIE		Deleted	4/26/2013	MRODNET	N
LITIA		Deleted	4/17/2013	KRISTAND	N
MARLYS		Purged	4/10/2013	SYSTEM	N
MARLI		Purged	4/10/2013	SYSTEM	N
JEFF		Purged	4/10/2013	SYSTEM	N
CHARLOTTE		Purged	4/10/2013	SYSTEM	N
ERIC		Purged	4/10/2013	SYSTEM	N
CHELSEA		Added	4/04/2013	HEATHERH	N
CHARLEY		Added	4/03/2013	HELENP	N
CHRIS		Deleted	4/03/2013	HELENP	N
SANDY		Deleted	4/02/2013	MRODNET	N
TRAVIS		Deleted	4/01/2013	NICOLEHA	N
JOHN		Added	3/22/2013	HELENP	N
CINDY		Deleted	3/19/2013	HELENP	N
CHRIS		Added	3/06/2013	MATTHEURGN	N
KATHRYN		Added	3/05/2013	KRISTAND	N

- ◆ Remember that your credit union’s Security Officer is responsible for resetting employee passwords using **Reset User Password/Device** on the Back Office (MNBACK) menu. Our CSRs have been instructed to refer reset requests to the credit union’s security officer. If an emergency reset needs to be done and there is no one at the credit union who can handle it, Client Services may charge a fee for this service.
- ◆ As of the 13.1 release (implemented for online CUs in July 2013, and for self-processors in October 2013), whenever a new CU*BASE server is installed, profiles must be rebuilt and will show a creation date that reflects that rebuild date.

TRACKING WHICH DATA CENTER EMPLOYEES SIGNED ON (SELF-PROCESSORS ONLY)

In addition to the audit feature described above, self-processors can monitor access to their iSeries system by data center staff by reviewing the file that logs a name and purpose each time a data center employee signs on to the IBM i (see Page 8). Then this data can be correlated to the history of activity performed by employee ID 89, as described above.

The remote access login data is stored in a file called **RMTACCESS** in your **CUBASEFILE** library. To review this database, use the following “canned” Query (or create your own using this file):

MNOP17 #18 "Remote Access Tracking Query"
 (OPER 17 > 18)

On the initial screen you can enter selection criteria (such as the date). Refer to online help for instructions on entering selection criteria. Following is an example of the inquiry that will display:

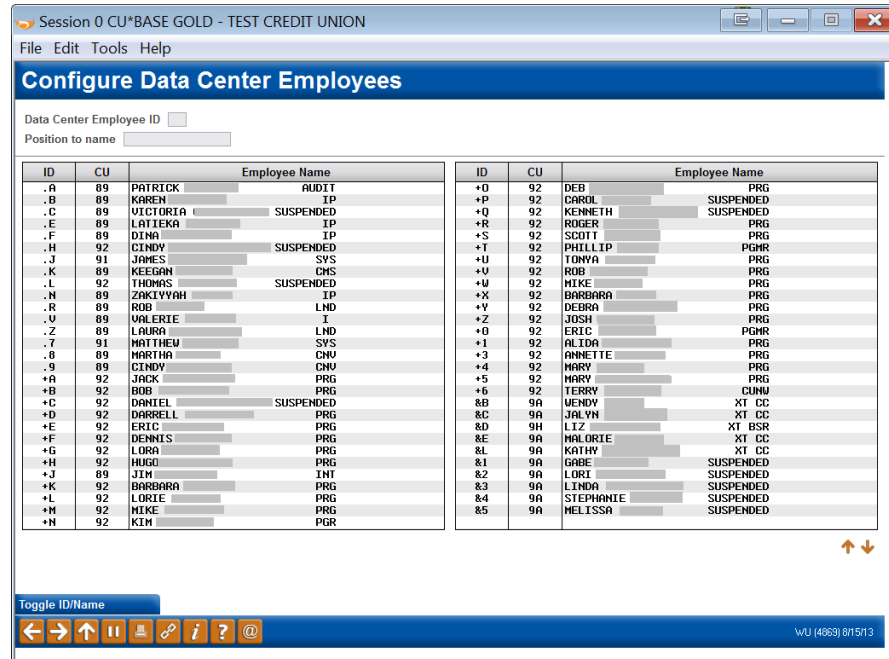
Line	ACCESS	ACCESS	REMOTE	REASON FOR
	DATE	TIME	USER NAME	REMOTE ACCESS
	(CCYYMMDD)	(HHMMSS)		
000001	2013/08/14	17:50:42	JACK CARPENTER	LOOK AT SETUP OF SENDING STMTS TO EDOC SERVER
000002	2013/08/14	17:21:57	JACK CARPENTER	LOOK AT SETUP OF SENDING STMTS TO EDOC SERVER
000003	2013/08/12	9:42:40	DAVE SCHEPERS	SEND BATCH MAINTENENCE FOR 8/10/13
000004	2013/08/09	12:18:17	DEB FINKBEINER	RESEARCH ERROR QSVSOPR
000005	2013/08/09	12:17:12	DAVE SCHEPERS	RESEARCH ERROR QSVSOPR

Remember that all of these users will use Employee ID 89 when performing CU*BASE activity.

APPENDIX: DATA CENTER STAFF ID SETUP

NOTE: Online credit unions do NOT have access to the following screens. They are shown here only to explain how these special employee IDs are being handled behind the scenes. Also remember that self-processors do not have this file on their system.

MNOP09 #13 "Define Data Center Employees" (OPER > 10 > 13)
Screen 1



This is the first of two screens used to define IDs for data center employees. Notice that all IDs must begin with a special character (anything except an asterisk *).

This screen will allow changes ONLY if accessed with a Staff ID that has Administrator privileges. Therefore only certain designated data center staff members will be allowed to add, delete, or change these IDs for online credit unions.

Screen 2

Session 0 CU*BASE GOLD - TEST CREDIT UNION

File Edit Tools Help

Configure Data Center Employee

Data Center Employee ID .X

Employee Name TEST EMPLOYEE

Employee Password *****

Administrator

CU Emp ID for authority 89

Suspend

Delete

WU (4068) @11513

This screen allows an administrator to create a new ID, suspend or delete an existing ID (when someone leaves the data center's employ), or reset a password for an employee. The *CU employee ID for authority* represents the alias ID that must be set up on the credit union's own employee security master.

Remember that any employee can reset his or her own expired employee password using the command on MNMAST. However, you must know your old password to enter a new one. Therefore, this screen would be the last resort should an employee forget his or her password.

CU*TIP: This screen will not let you continue without entering a password. Therefore, any change to the name, administrator setting, or alias ID will require that the password also be reset by entering a temporary new one here. The user will be required to change that password before they will be able to access any other commands.