
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 activity on member data by your credit union employees, as well as activity initiated by a member of the CU*Answers client support teams, referred to as your “Data Center” employees.

CONTENTS

<u>DATA CENTER EMPLOYEE SECURITY</u>	<u>2</u>
OVERVIEW	2
DATA CENTER STAFF ID RULES	3
TOOLS FOR OUR SELF PROCESSING CREDIT UNION PARTNERS	5
<u>AUDITING EMPLOYEE ACTIVITY</u>	<u>6</u>
TRACKING WHICH EMPLOYEES ACCESS WHICH CU*BASE FEATURES	6
TRACKING WHICH DATA CENTER EMPLOYEES SIGNED ON TO YOUR ISERIES (SELF PROCESSORS ONLY)	8
<u>VIEWING A LIST OF EMPLOYEE IDS</u>	<u>9</u>
<u>DATA CENTER STAFF ID SETUP</u>	<u>10</u>

Revision date: October 10, 2011

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

DATA CENTER EMPLOYEE SECURITY

OVERVIEW

In order for CU*Answers to assist its online 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 CU*Answers employees. Previously there were primarily two IDs used by all CU*Answers 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, CU*Answers introduced a system to allow us to separate Data Center (CU*Answers) Staff from credit union employees, and give each individual CU*Answers 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 CU*Answers' employ, it is not necessary to change the generic 89 password manually on every credit union library; that employee's ID is simply suspended.
- ◆ Any activity performed by a CU*Answers employee on credit union files is logged using that individual person's ID, not the generic 89.

*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 CU*Answers, 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 CU*Answers employees, and the use of "alias" IDs on credit union Employee Security master files (such as the existing ID 89).

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

Additionally, a specific alias (93) has been created for use by the Xtend call center employees, which restricts access even further than the 89 alias. This alias is also managed by a security officer, ensuring an even higher level of security for your credit union.

NOTE: Data Center security is handled differently for our **Self Processing clients** that have their own iSeries systems. Please refer to Page 5.

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 Staff IDs requires a Data Center Staff ID that has administrator privileges. (This administrator can adjust Data Center Staff 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 Staff ID password. See Page 10 for additional information.
- Data Center Staff 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 “Change Employee Password” on 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 to change it.
- Each Data Center Staff 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 and speed sequences can be used by data center staff. For example:

<i>CU*Answers 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 Xtend 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, CU*Answers 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	Xtend

*NOTE: Alias IDs (89, 90, 91, 93, etc.) still must be set up in each individual CU's employee security master. Currently CU*Answers reserves employee IDs 89-99 for our use.*

- Any password assigned to an alias ID on the CU's employee security master will be ignored and not used. For example, CSR access can no longer 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; CU*Answers 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 Staff 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.

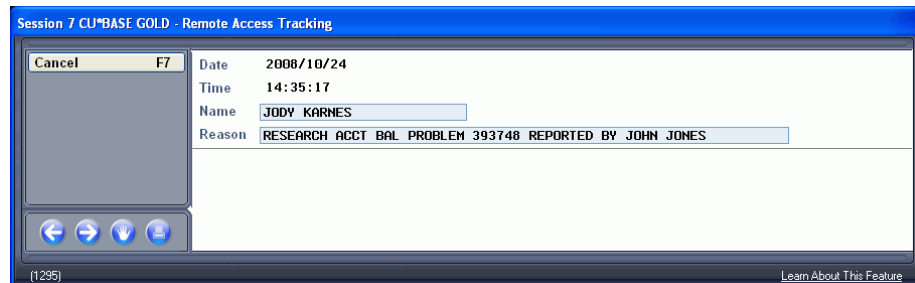
TOOLS FOR OUR SELF PROCESSING CREDIT UNION PARTNERS

Because the data center employee ID file resides only on the CU*Answers iSeries 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 CU*Answers employee accesses your credit union’s system, there is a special file that will log information about the person logging in to your iSeries.

The following window will appear every time a CU*Answers employee logs in to your iSeries:



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 8 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 monitor access to CU*BASE programs by any employee ID, whether CU*Answers or credit union employee. Every time a CU*BASE program is accessed, the system records who accessed the command and when. For CU*Answers employees, the file records the individual ID for the staff member (not the alias) so you will be able to tell who from CU*Answers 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.

*NOTE: If your credit union does not currently require an employee ID and password to access Member Inquiry, now may be the time to revisit this policy. After all, CU*BASE can only record an ID if one is entered in the first place! Contact a CSR if you wish to change this setting.*

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 Management Functions menu:

MNAUDT #16 "Audit Insider/Employee Audit"

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:

General

Session 0 CU*BASE GOLD - Display Report

Display Report : CUBASEQ/MNQRY28 Report Builder

Position to line: [] Shift to column: [] Report width: 113

Line	DATE	Emp ID	Employee Name	Account Number	Access Granted	Program	User ID	Work Station	Time (HHMMSS)	CU#
000001	07/22/2009	+D		0	Y	TSBNTB	DARRELLS	QPRDEV000F	12:50:47	133
000002										
000003	07/22/2009	+R	ROGER	0	Y	TSBNTB	ROGERH	ROGERD21	10:47:40	114
000004	07/22/2009	+R	ROGER	0	Y	TSBNTB	ROGERH	ROGERD21	10:47:20	114
000005	07/22/2009	+R	ROGER	0	Y	TSBNTB	ROGERH	ROGERD21	10:39:39	114
000006	07/23/2009	+R	ROGER	0	Y	TSBNTB	ROGERH	ROGERD21	15:22:20	114
000007	07/23/2009	+R	ROGER	0	Y	TSBNTB	ROGERH	ROGERD21	12:06:29	114
000008	07/23/2009	+R	ROGER	1	Y	TSBNTB	ROGERH	ROGERD21	16:02:57	114
000009	07/24/2009	+R	ROGER	0	Y	TSBNTB	ROGERH	ROGERD21	9:22:55	114
000010										
000011	07/20/2009	+7	CU*NW BONNIE HANSON	300	Y	TSBNTB	BONNIEH	QPRDEV000F	13:15:26	740
000012										
000013	07/20/2009	-3	MARIBETH	1	Y	TSBNTB	MARIBETHH	MH...D1	13:59:47	740
000014	07/20/2009	-3	MARIBETH	300	Y	TSBNTB	MARIBETHH	MH...D1	15:01:20	740
000015	07/20/2009	-3	MARIBETH	300	Y	TSBNTB	MARIBETHH	MH...D1	15:02:52	740
000016	07/20/2009	-3	MARIBETH	300	Y	TSBNTB	MARIBETHH	MH...D1	15:03:04	740
000017	07/20/2009	-3	MARIBETH	300	Y	TSBNTB	MARIBETHH	MH...D1	15:04:17	740
000018	07/20/2009	-3	MARIBETH	0	Y	TSBNTB	MARIBETHH	MH...D1	15:05:36	740

FR QRYRPT32

Your report may contain more columns than are currently visible. First use the scroll bar to view more columns. Then use the "Move Left" and "Move Right" buttons to adjust the display further.

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.
- ◆ The final column (not visible above) 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.
- ◆ 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 invalid ID was entered when attempting to access the command, or the assigned alias ID does not exist.
- ◆ If your credit union does not require an Employee ID and password to access Member Inquiry, a record will still be written to this file but the Emp. ID and name will be blank.
- ◆ 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 CU*Answers Operator. As usual, there is a nominal charge if this service is required.)
- ◆ 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.

Security Question and Code Word Access

Line	DATE	Emp ID	Employee Name	Account Number	Access Granted	Program	User ID	Work Station	Time (HHMMSS)	CU#
000019	09/16/2010	Y	MEYERS	2002	Y	CNFIRM	OST	A M	14:31:23	112
000020	09/21/2010	Y	MEYERS	1075	N	CNFIRM	OST	A M	11:10:49	112
000021	09/21/2010	Y	MEYERS	2002	N	CNFIRM	OST	F M	11:22:25	112
000022	08/03/2010	Y	MEYERS	2002	Y	CODE WORD	A M	G0	12:01:52	112
000023	08/03/2010	Y	MEYERS	2002	Y	CODE WORD	A M	G2	14:28:02	112
000024	08/09/2010	Y	MEYERS	2002	Y	CODE WORD	A M	G0	11:47:34	112

- ◆ The example above shows how correct and incorrect answers to code words and security questions (configured via Privacy Controls) appears in the SECAUD report.

TRACKING WHICH DATA CENTER EMPLOYEES SIGNED ON TO YOUR ISERIES (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 iSeries (see Page 5). 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, then 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 DATE (CCYYMMDD)	ACCESS TIME (HHMMSS)	REMOTE USER NAME	REASON FOR REMOTE ACCESS
000001	2006/11/20	16:20:00	JODY KARNES	RUN MONTH-END BILLING QUERIES
000002	2006/11/20	15:47:53	DAWN M SMITH	TESTING THIS SYSTEM
000003	2006/11/20	15:47:25	JODY KARNES	RESEARCH ACCT BAL PROBLEM 393748 REPORTED BY JOHN JONES

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

VIEWING A LIST OF 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 CU*Answers employee.

MNMGMT #1 "CU*BASE Employee Security"

Click F10-DC Employee to see a list of IDs and names for CU*Answers 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 F10-Data Center Empl to view the list of CU*Answers staff IDs.

Use option #6 to view the list of credit union employee 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.

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 iSeries system.

MNOP09 #13 "Define Data Center Employees"
Screen 1

Click F9-Toggle ID Name to switch from sorting by ID to sorting by Employee Name.

ID	CU	Employee Name	ID	CU	Employee Name
.K	89	KEEGAN	+E	92	ERIC
.1	89	HOPE	+F	92	DENNIS
.2	89	CARLA	+G	92	LORA
.3	89	RICK	+H	92	HUGO
.4	89	CONSTANCE	+I	92	MATT
.5	89	CARI	+J	92	JIM
.6	89	CAROLYN	+K	92	BARBARA
.7	89	MATTHEW	+L	92	LORIE
.8	89	MARTHA	+M	92	MIKE
.9	89	CINDY	+N	92	TON
+A	92	JACK	+O	92	DEB DE
+B	92	BOB	+P	92	CARRIE
+C	92	CU*NORTHWEST	+Q	92	SETH
+D	92	DARRELL	+R	92	ROGER
			+S	92	SCOTT
			+T	92	CHRISTINA

This is the first of two screens used to define IDs for Data Center (CU*Answers) 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 CU*Answers staff members will be allowed to add, delete, or change these IDs for online credit unions.*

Screen 2

Backup	F3
Suspend	F4
Cancel	F7
Delete	F16

This screen allows an administrator to create a new ID, suspend or delete an existing ID (when someone leaves CU*Answers' 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.