
Defense MD

Backup Tape Encryption for Our Self Processing Credit Union Partners

INTRODUCTION

This document describes how to use the various controls and menu options related to encryption of backup tapes via the Defense MD system.

CONTENTS

INTRODUCTION	2
DEFENSE MD: ENCRYPTED TAPE BACKUPS FOR SELF-PROCESSORS	2
SYSTEM BACKUP AND BUSINESS RECOVERY STRATEGIES	2
COSTS	3
GETTING STARTED	3
CHANGES TO YOUR POLICIES AND PROCEDURES	4
HANDLING BACKUP TAPES	4
GENERATING ENCRYPTION KEYS	4
NEW PROCEDURE FOR FULL SYSTEM SAVES	4
CHANGES TO YOUR ANNUAL DISASTER PLAN TESTING	5
THE DEFENSE MD MENU	6
ENCRYPTING YOUR DAILY/MONTHLY BACKUPS	8
YOUR FULL SYSTEM BACKUP	9
WORKING WITH ENCRYPTED FILE TAPES	11
COMMANDS FOR SAVING & RESTORING INDIVIDUAL ENCRYPTED FILES	11
CONFIGURATION OPTIONS	13
SPECIAL NOTE TO CUS USING HIGH AVAILABILITY (HA)	15
OTHER DEFENSE MD FEATURES	16
DAILY/MONTHLY BACKUPS FOR SERVICE BUREAUS	16
AES ENCRYPTION BACKUP MENU	18
APPENDIX	19
SAMPLE DATA ENCRYPTION POLICY	19

Revision date: December 8, 2010

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

INTRODUCTION

DEFENSE MD: ENCRYPTED TAPE BACKUPS FOR SELF-PROCESSORS

Do you cringe when you read news articles about a company that misplaces a data tape and now must notify their entire customer base of the potential security risk because their personal data has landed in unknown hands? Can your business afford either the risk or the expense of a similar exposure happening in your data center? How secure are your end-of-day backup tapes when they leave your building?

As self-processors, these are questions that we must continually ask ourselves, and most certainly be ready to answer when they are asked of us by members, examiners, or vendors. As a diligent CUSO partner, you have implemented secure and practical solutions to protect member data, but to what degree will they hold up? Can they go so far as protection against a disgruntled employee walking off with an unencrypted backup tape?

Member data is the lifeblood of your business, and today's marketplace requires all of us to step up to the challenge of preserving its security. As a data processor, this same challenge is magnified to the point where it became prudent to invest CUSO financial and staff resources to develop a even higher degree of data security—tape encryption with **Defense MD**.

Defense MD allows you to securely encrypt data that you are currently putting on magnetic tape.

CU*Answers has partnered with Patrick Townsend & Associates to offer their Alliance AES/400 product to our self-processing community. The heart and soul of the Alliance AES/400 solution is its use of AES (Advanced Encryption Standard). AES is an encryption method that has been selected by the National Institute of Standards and Technology (NIST) of the US government for use in private and public applications to protect sensitive information.

During our internal deployment, CU*Answers added a user-friendly wrapper around the AES/400 product to create an easy-to-use menu system, configuration options, and invaluable assistance with key management. Defense MD can even notify you when a new library has been added to your system so that its proper disposition can be defined.

Defense MD is the solution to safely and securely protecting your valuable member data and to satisfy the scrutinizing eye of auditors and examiners.

SYSTEM BACKUP AND BUSINESS RECOVERY STRATEGIES

Several credit unions have approached us recently about the possibility of transmitting daily backup files to CU*Answers in order to eliminate the daily tape cycle. While we are working toward a solution to meet these requests, there are still valid reasons for all in-house clients to strongly consider tape encryption:

- ◆ Even if you are already using or considering a high availability/data replication solution, you will always have a need for tape backups for local restore purposes.
- ◆ And what about your full system backups?

- ◆ Or your month-end CU*BASE file backups (you should have two sets – one onsite and one offsite)?

An examiner will certainly remind you that it is critical to retain a hard copy of these backup tapes for seven (7) years. Since moving data to tape is not going away totally any time soon (even after you deploy a data replication strategy), your member data will continue to be exposed to risk without a comprehensive encryption strategy like Defense MD.

COSTS

Fees for Defense MD include a one-time software and implementation services fee of \$9,000 (plus applicable T&E). This cost covers a member of our iSeries team coming on-site to configure, document, and train your staff on AES/400. The second cost is a 20% Annual Maintenance Fee. This \$1,800 fee will be invoiced upon installation and each subsequent anniversary.

If your credit union has High Availability, there may be an additional cost to purchase a second copy of the AES/400 software for your HA backup iSeries.

All fees are subject to change. Refer to the current year's Self Processor Pricing Guide (sent to your credit union CEO annually) for updated pricing.

GETTING STARTED

For more information or to get signed up for Defense MD services, contact **Lora Goodin (lgoodin@cuanswers.com)** or **Scott Collins (scollins@cuanswers.com)**. Following is a summary of the process:

1. A contract will be drawn up to be signed by your credit union and CU*Answers.
2. Your credit union should develop a policy and procedure for handling encryption keys and secure transport and storage of encrypted materials. **(See the Appendix for a sample policy to consider.)**
3. We will order the Alliance AES/400 software from Patrick Townsend & Associates for you.
4. A pre-site contact will be set up to discuss the timing and process for implementation for your credit union.
5. Based on your pre-site, a CU*Answers representative will take care of loading and configuring the software on your iSeries.
6. A CU*Answers representative will provide training to your staff, either in person or over the phone as desired.
7. Your Operations staff will begin following your newly established procedures for handling daily/monthly backup tapes.

CHANGES TO YOUR POLICIES AND PROCEDURES

See the Appendix on Page 19 for a sample data encryption policy. This policy can be copied and adapted for your credit union's use, with changes and additions as appropriate.

HANDLING BACKUP TAPES

The actual steps for daily and monthly processing (see Page 8) will not change much for your Operators, but the procedures for handling the backup tapes will. This is necessary to ensure that the encryption keys are kept safe and easily accessible, but NOT stored in the same location as the backup tapes themselves. After all, the data isn't secure if someone could easily steal the tapes and the secret password codes at the same time!

NOTE: Data is never stored encrypted on the iSeries itself; encryption occurs at the point when files are copied from disk to tape using the command on the MNOP04 Daily Processing or MNOP03 Monthly Processing menus.

GENERATING ENCRYPTION KEYS

In a nutshell, an **encryption key** is basically a randomly-generated password that uses a complex set of characters in a long string. Each key has a **key name** that helps to identify which backup tapes were encrypted using that particular password.

You will need to have policies and procedures in place to routinely generate new encryption keys, such as on an annual basis, according to your credit union's security policies and risk assessment. Keys must be retained for as long as the backup tapes that use those keys (old tapes continue to use the old key that was in place when the tape was generated).

The procedure for generating keys is part of the instructions you will receive separately with the Alliance AES/400 software. You will then use a command on the Defense MD menu (page 6) to save a backup copy of the keys to be stored in a separate off-site location.

NEW PROCEDURE FOR FULL SYSTEM SAVES

Although the menu options your Operators will use for daily and monthly backup tapes will not change with Defense MD, in order to encrypt member data as part of your periodic full system backup, a new menu option must be used on the Defense MD menu. See Page 9 for instructions.

CHANGES TO YOUR ANNUAL DISASTER PLAN TESTING

To make sure your backup tapes will be available when you need them, we recommend you set an annual schedule to test restoring data from backup tapes using the encryption keys. This can be done as part of your annual disaster recovery testing.

In addition, be sure to make a note in your disaster plan to include the AES key file in the list of data tapes you will need in the event of a disaster. In the event that a full system restore is needed, for a DR test or after an actual disaster, the following tapes will be needed:

1. Most recent full system save (includes encrypted and unencrypted tapes)
2. AES Key file
3. Most recent EOD or BOD (depending on when disaster occurred)
4. Latest EOM
5. Most recent version of any daily backups (if done)

THE DEFENSE MD MENU

When Defense MD is installed and configured on your iSeries, a new menu will be added. **This menu will only be used in a few situations:**

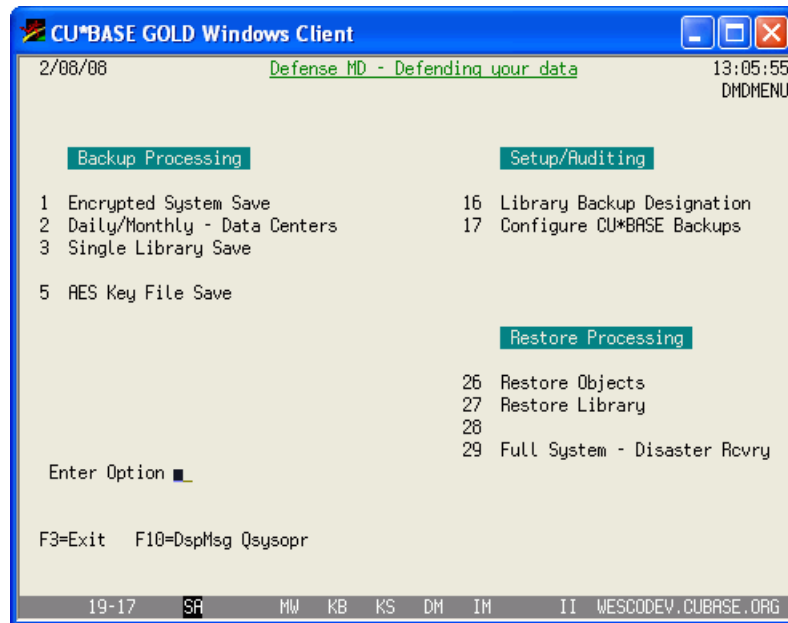
- ◆ If you need to change the configuration from what is initially set up for you by a CU*Answers representative, or
- ◆ To run your periodic full system backup (instead of using the “GO SAVE” command).
- ◆ To save or restore an individual encrypted library or file.

To access the Defense MD menu, your user profile will need to include the DEFMD library in your library list. (You may need to adjust the USERID profile for select employees who will need this library.)

From the main Operations menu MNOP01, choose option 18 “Defense MD Tools” (or type command DEFMD on a command line) to display the following menu:

The Defense MD Main Menu

MNOP01 #18 “Defense MD Tools”



Menu Options

Option	What it does
<i>Backup Processing</i>	
1 Encrypted System Save	This is the option you will use from now on to process your full system backup. See Page 9.
2 Daily/Monthly – Data Centers	Calls DLYMOBKCL to display the Defense MD Daily/Monthly Backups menu (Page 16). Not used by self processing credit unions. See Page 8 for instructions.

<i>Option</i>	<i>What it does</i>
3 Single Library Save	<p>Calls the DMDSAVLIB command. See Page 11.</p> <p>This is used when saving a refresh of your training library or another single library in an encrypted format.</p>
5 AES Key File Save	<p>Prompts for a tape device and performs a SAVOBJ command.</p> <p>This is used to save a copy of the encryption keys to a backup tape. This tape must be stored in a secure, convenient off-site location, but NOT the same location as where the backup tapes themselves are stored.</p>
<i>Setup/Auditing</i>	
NOTE: This area currently has only setup options but is also intended for future enhancements designed for auditing purposes.	
16 Library Backup Designation	Scans system for new libraries (UDMDLIBCL). Displays list of all libraries on system and the backup designation codes. See Page 14.
17 Configure CU*BASE Backups	Links to CU*BASE backup configuration program UBACUPCL. See Page 13.
<i>Restore Processing</i>	
26 Restore Objects	Calls the DMDRSTOBJ command. See Page 12. Can be used to restore a library, such as your end-of-month files, or even a single file.
27 Restore Library	<p>Calls the DMDRSTLIB command. See Page 12.</p> <p>This is used to restore a fresh copy of your training library or another single library that was encrypted.</p>
29 Full System - Disaster Rcvry	Calls the CUADRMNUCL command. Not used by self processing credit unions.

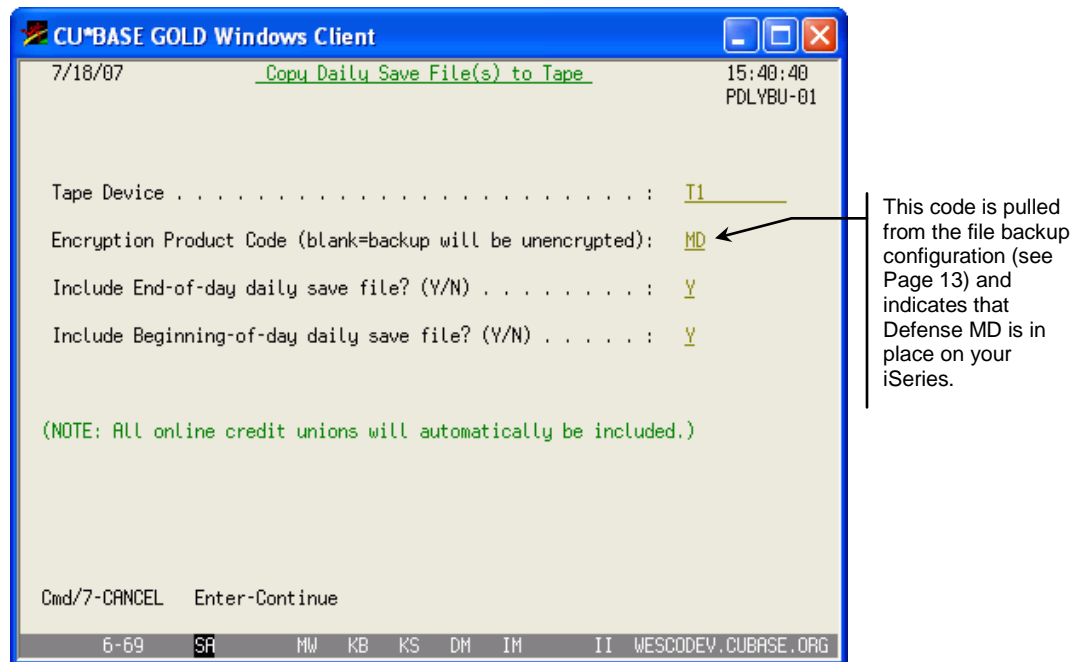
ENCRYPTING YOUR DAILY/MONTHLY BACKUPS

After Defense MD has been installed and configured on your computer, you will proceed to handle your daily and monthly processing exactly as before, using the same menu commands as usual. The main difference will occur when backups are copied to disk.

IMPORTANT: If your credit union previously did backups directly to tape, your Operator will now need to complete an additional step to select the special “copy to tape” command on either the MNOPO4 Daily Processing or MNOPO3 Monthly Processing menus.

Remember that data is never stored encrypted on the iSeries itself; encryption occurs at the point when files are copied from disk to tape.

OPER #2 “Daily Processing” then #6 “Copy Daily Save Files to Tape” (or OPER #3 “Monthly Processing” then #11 “Copy Month-End Files to Tape”)



Because Defense MD has been configured for your credit union, this option will now automatically encrypt the data as it is copied to the tape (two copies will still be produced, as usual).

As with your full system backups, a printout will be produced showing the contents of the tape. (See Page 11 for a sample of this report.) We recommend that you keep the report with the tape to assist with future restores.

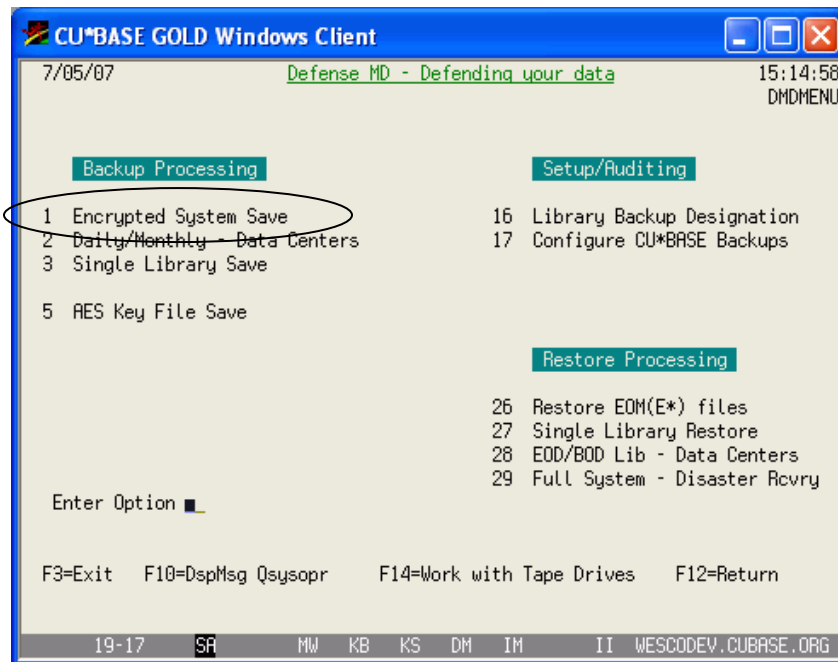
YOUR FULL SYSTEM BACKUP

The following instructions should be used instead of the “GO SAVE” command to perform a full system backup for your iSeries.

IMPORTANT: When you sign in as QSECOFR to do your backup, remember that your library list will not automatically contain the DEFMD library needed to handle the encryption routines. Therefore, you’ll need to **edit your library list** using the following command:

ADDLIBLE LIB(DEFMD) POSITION(*LAST)

Defense MD Main Menu (command DEFMD)



From now on, you will use **option 1 Encrypted System Save** on the Defense MD menu to process your full system backup. (A confirmation screen with instructions will appear before continuing.)

This method uses a special configuration (see Page 14) to determine which data should be encrypted (member file libraries, employee libraries, etc.) and which can be saved without encryption (such as application files).

Two separate backup tapes will be generated. The system will instruct you when to load the first (encrypted) tape and then when to load the second tape for unencrypted data. Following is a summary of what happens when you select this option:

1. Retrieves the device ID from DEFMD config
2. Checks for libraries designated for encrypted backups (these are configured using the screen shown on Page 14)
3. Initializes the encrypted tape
4. Saves libraries flagged for encrypted saves
5. Displays the tape to print out
6. Initializes the unencrypted tape

7. Puts system in restricted state
8. SAVSYS
9. SAVLIB *NONSYS w/ omitted libraries flagged in DEFMD config
10. SAVDLO
11. SAVE IFS
12. Displays the tape to print out and keep with the backup tapes (see Page 11)
13. IPLs the system

WORKING WITH ENCRYPTED FILE TAPES

When daily/monthly or full system backups are done as described above, the system will produce a report showing the contents of the tape:

5722SS7 V5R4MO 060210		TAPE VOLUME INFORMATION				TEST	TESTCOMM	7/25/07 23:32:02	Page	1	
Device	T1	Volume	TEST								
Owner ID		Density	*ULTRIUM3								
Type	*SL	Code	*EBCDIC								
Data File Label	File Sequence	Record Block Format	Recg Tech	Record Length	Block Length	File Length	Mvol Ind	Mvol Sequence	Date Created	Expiration Date	System Where Created
FILECLEOD	0000000001	*F	P	32736	032736	0000574523		0000000001	07/25/07	*PERM	IBMOS400
FILECLBOD	0000000002	*F	P	32736	032736	0000573426		0000000001	07/25/07	*PERM	IBMOS400

This report should be printed and kept with the tape itself to make it easier to see what is on the tape, and to provide the details you will need later should something need to be restored from the backup.

COMMANDS FOR SAVING & RESTORING INDIVIDUAL ENCRYPTED FILES

DMDSAVLIB Command

This command (also available via option #3 on the Defense MD menu) is used to encrypt and save a single library to tape, such as your training library.

From a command line type in the command **DMDSAVLIB** then press F4 (Prompt) and complete the fields as appropriate:

Field Name	Description
Library	The library that you want save.
Device	The tape drive you will be saving to.
Save file already exists?	Answer Y if you have already saved your library to a save file. <div style="border-left: 2px solid black; padding-left: 10px; margin-left: 20px;"> IMPORTANT: It is recommended that the save file name you use is the same name as the library name so that the DMDRSTLIB command can be used to restore the encrypted library. </div>
If Y, name of save file If Y, library save file in	The name and location of the file that is to be encrypted and saved to tape.

DMDRSTOBJ Command

This command (also available via option #26 on the Defense MD menu) is used to restore the E* files from End of Month backup tapes that are encrypted.

From a command line type in the command **DMDRSTOBJ** then press F4 (Prompt) and complete the fields as appropriate:

<i>Field Name</i>	<i>Description</i>
Device	The tape drive you will be restoring from.
Date saved	The date (mmddyy) that files were written to the backup tape. This appears as "Date Created" on the DSPTAP printout.
Save file	The name of the file, as shown under "Data File Label" on the DSPTAP printout.
Sequence number	The sequence number of the save file. This is shown under "File Sequence" on the DSPTAP printout.
Objects	The name of the objects you want to restore. <ul style="list-style-type: none"> ▪ For end-of-month files, use E* ▪ For a single file, enter the file name
Saved library	The library that the files were in when they were saved. For month-end files, use FILExx (<u>not</u> FILExxE).
Restore to library	The library where you want the objects restored, such as FILExxE for month-end files.

DMDRSTLIB Command

This command (also available via option #27 on the Defense MD menu) is used to restore file libraries that are encrypted, such as your training library. (If a library on the tape is unencrypted, such as CUBASE libraries, then just use the normal RSTLIB command.)

From a command line type in the command **DMDRSTLIB** then press F4 (Prompt) and complete the fields as appropriate:

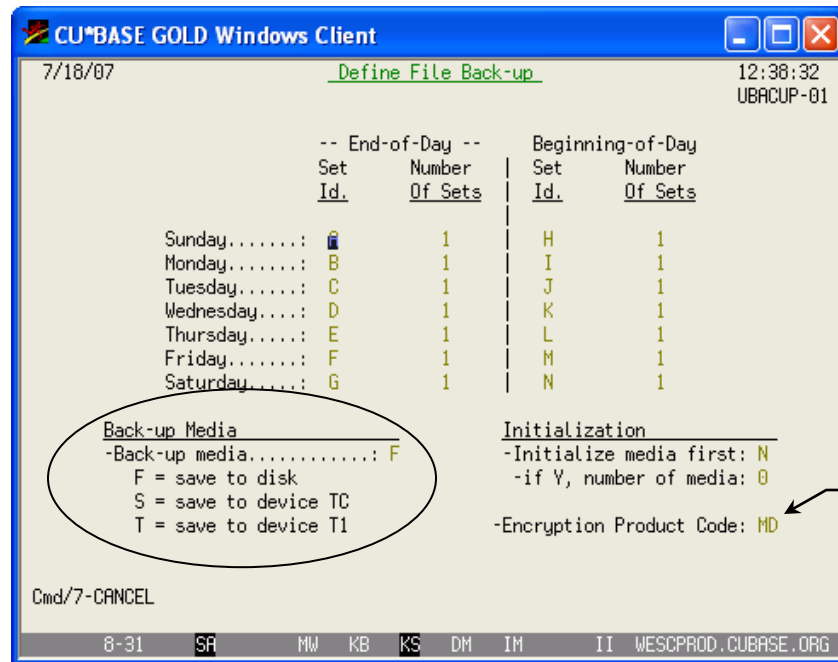
<i>Field Name</i>	<i>Description</i>
Device	The tape drive you will be restoring from.
Date saved	The date (mmddyy) that library was written to the backup tape. This appears as "Date Created" on the DSPTAP printout.
Save file	The name of the save file, as shown under "Data File Label" on the DSPTAP printout. For an end-of-day library being restored as a new training library, the file name should be FILExxEOD.
Sequence number	The sequence number of the save file. This is shown under "File Sequence" on the DSPTAP printout.
Saved library	The library that was put to the save file. For an end-of-day library, use FILExx.
Restore to library	The name of the new library you are creating. For a training library, use FILEXX where the XX is NOT your credit union ID.

CONFIGURATION OPTIONS

IMPORTANT: The following configuration steps will be done for you as part of your initial configuration and setup for the Defense MD system. This section is presented for your information only and will generally not need to be changed unless you wish to alter which files are being included/encrypted in your full system backup.

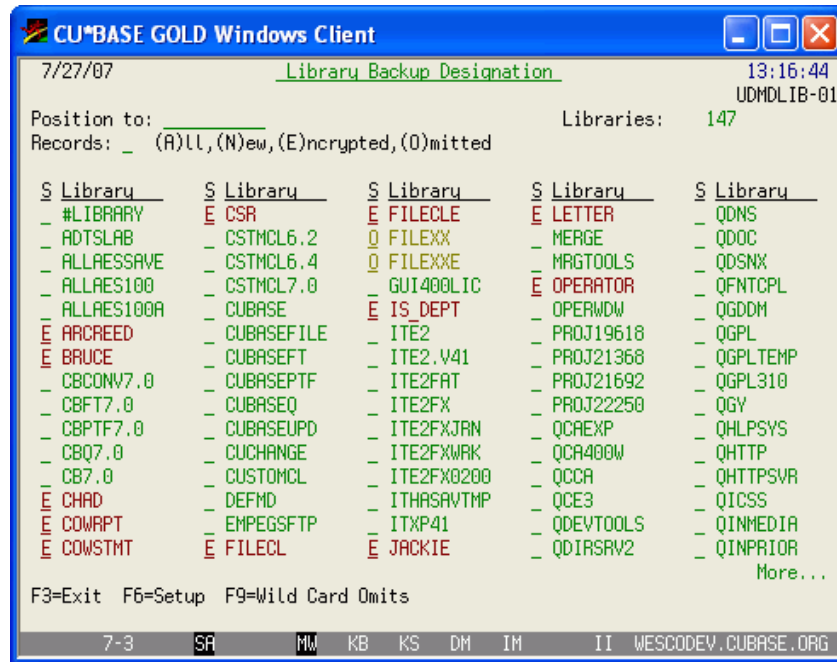
The first step in configuring Defense MD will be to alter the way daily and monthly backups are processed.

Option 17 "Configure CU*BASE Backups" from the Defense MD menu (pg. 6)



The Back-up media option must be set to "F" so that backup files are saved to disk (in your FILExxE library) rather than going directly to tape. (Your credit union may already be using this method.) An *Encryption Product Code* of MD will also be entered to indicate that the software has been set up on your iSeries.

Next, a special Defense MD configuration is used to specify how full system backups (see Page 9) will be handled. This configuration itemizes which libraries should be encrypted (your member data), and which libraries have files that can be saved in plain text, such as the libraries that contain system and application files.



The system first performs a scan (UDMDLIBCL) for any new libraries that have been added since the last time the configuration was done. The screen shows all libraries on the iSeries and any existing encryption codes you have set up.

Use the "position to" search field at the top of the screen to enter a library name and scroll quickly to that library. Or type one of the four "Records" types and press Enter to display only those libraries (clear the field or type A and press Enter to see all libraries again).

To modify the configuration, simply enter one of the following designation codes in front of the library name. When done, use Enter to save, then F3-Exit to return to the menu.

The decision about whether to encrypt a library or omit it from your full system backup will depend on your Disaster Recovery policy. Since your normal daily/monthly backups will be encrypted, some CUs use their full system back up to save only system files, omitting the ones that are encrypted on their regular daily backups. Then they would need both tapes (as well as the separate tape containing the encryption keys) in the event of a disaster or DR test.

Designation Codes

Code	Description
E - Encrypt	Libraries marked with this code WILL be encrypted and included on the separate encrypted data tape when a full system backup is done using option #1 on the Defense MD main menu (see Page 9). <p>Don't forget about your QUERYxx library or any other employee libraries that might contain member data created via Query!</p>

<i>Code</i>	<i>Description</i>
O - Omit	<p>Libraries marked with this code will not be backed up at all when a full system backup is done using option #1 on the Defense MD main menu (see Page 9).</p> <p>Depending on your disaster recovery policy, you might use this option to omit the FILExx libraries that are already being backed up on your normal daily backups. (But if you <i>do</i> include those, make sure to encrypt them!)</p>
N - New	All libraries that have been added since the last time this configuration was accessed will be marked with this code. These will be handled as <u>un</u> encrypted items (same as blank) until you change them to the desired code.
(Blank) - Unencrypted	Libraries that are not marked with any code will NOT be encrypted. They will be included on the unencrypted tape when a full system backup is done using option #1 on the Defense MD main menu (see Page 9).

Command Keys

<i>Command Key</i>	<i>Description</i>
F6-Setup	<p>Used to configure some parameters used when copying encrypted files to tape, including your credit union's assigned 2 digit key ID (unique by iSeries) and default tape device. <i>(This setup will be done for you during your initial Defense MD installation.)</i></p> <p>NOTE: You can also specify an email address. This is for a future enhancement planned to create a new daily job that causes the iSeries to kick out an email whenever new libraries are added. This should generally be a group email address that is monitored by more than one person.</p>
F9-Wild Card Omits	<p>To configure up to 10 wildcards (i.e. FILE*) for <u>omission</u> on the non-encrypted full system save.</p> <p>This feature was intended for use in service bureau situations where there are a number of libraries with similar naming convention, such as FILExx, to speed up the process of setting the designation codes.</p>

SPECIAL NOTE TO CUS USING HIGH AVAILABILITY (HA)

If your credit union has an HA backup system for production redundancy, the Alliance AES/400 software will be loaded and configured separately for each iSeries. The software file libraries are not typically mirrored between the two systems because of the way the software is configured.

It may be appropriate, however, to mirror the DEFMD libraries that store the configuration settings above. If not, you would need to make the same changes to both boxes separately, whenever new libraries are added.

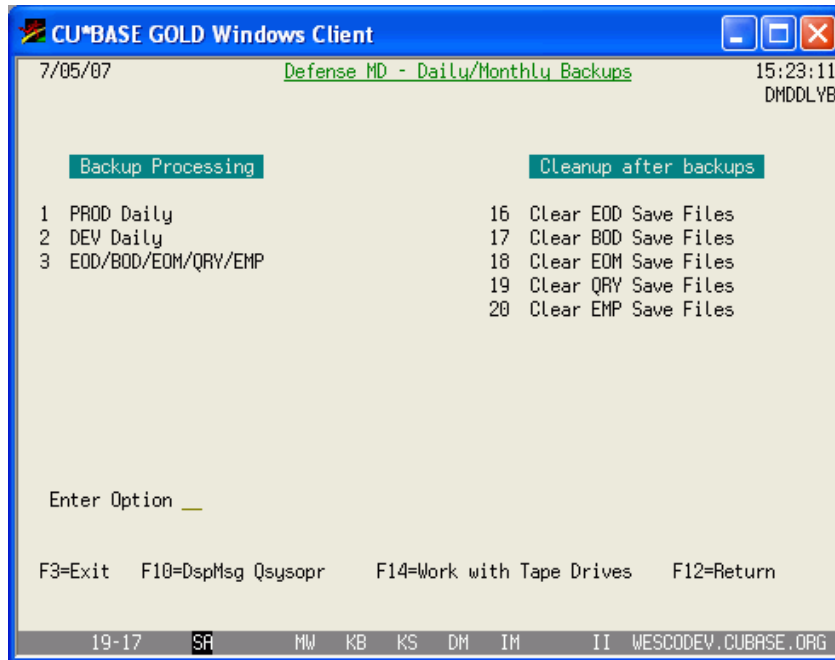
If CU*Answers acts as your HA backup system, we cannot mirror the DEFMD libraries as it would cause a conflict with our system. Therefore, we would need to coordinate changes to this configuration with you.

OTHER DEFENSE MD FEATURES

DAILY/MONTHLY BACKUPS FOR SERVICE BUREAUS

The following menu is NOT used by self processing credit unions. It was designed specifically for the special needs of CU*Answers and other service bureau environments who handle backup tasks independent of daily processing.

Option 2 “Daily/Monthly – Data Centers” from the Defense MD menu (pg. 6)



Menu Options

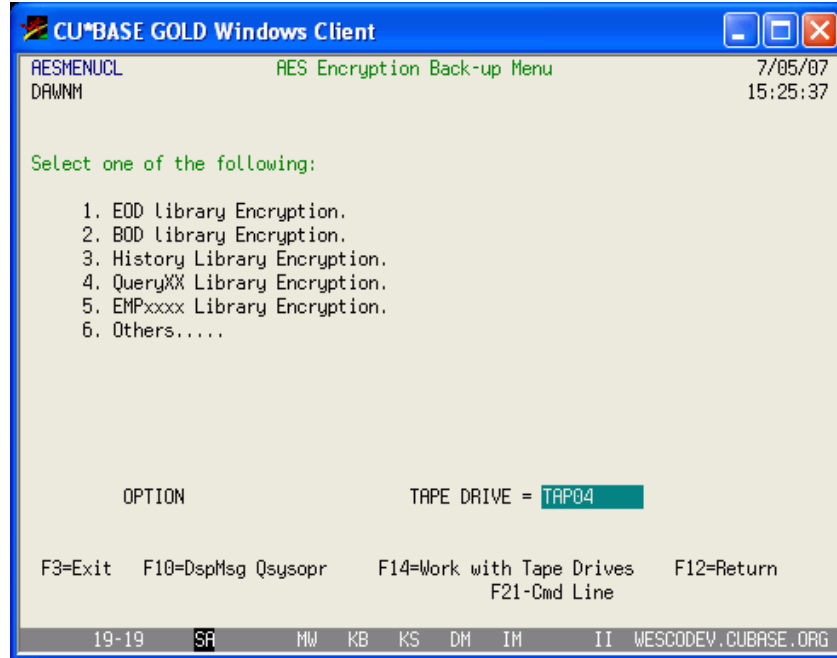
<i>Option</i>	<i>What it does</i>
<i>Backup Processing</i>	
1 PROD Daily	Calls command PRODDLY which prompts for tape device PRODDLYCL submits job PRODDLYBKP <ul style="list-style-type: none"> ▪ Initializes tape ▪ Encrypted backup of OPERATOR ▪ Unencrypted backup of ZMODLIB10 ▪ Displays tape to printout
2 DEV Daily	Calls command DEVDLY which prompts for tape device DEVDLYCL submits job DEVDLYBKP <ul style="list-style-type: none"> ▪ Initializes tape ▪ Encrypted backup of CNV*, EMP*, PROJ*

<i>Option</i>	<i>What it does</i>
	libraries <ul style="list-style-type: none"> ▪ Unencrypted backup of CUBASE*, ZMODLIB10 ▪ Displays tape to printout
3 BOD/EOD/EOM/QRY/EMP	Calls AESMENUCL and displays backup options. See Page 18.
<i>Cleanup After Backups</i>	
16 Clear EOD Save Files	Calls EODSAVCLR and clears save files in the BKPEOD library.
17 Clear BOD Save Files	Calls BODSAVCLR and clears save files in the BKPBOD library.
18 Clear EOM Save Files	Calls HSTSAVCLR and clears save files in the BKPHST library.
19 Clear QRY Save Files	Calls QRYSAVCLR and clears save files in the BKPQRY library.
20 Clear EMP Save Files	Calls EMPSAVCLR and clears save files in the BKPEMP library.

AES ENCRYPTION BACKUP MENU

The following menu is NOT used by self processing credit unions. It was designed specifically for the special needs of CU*Answers and other service bureau environments who handle backup tasks independent of daily processing.

Option 3 "BOD/EOD/EOM/QRV/EMP" from the Defense MD Daily/Monthly Backups menu (pg. 16)



Each option calls AESSAVECL with the appropriate 2 parameters:

- Type of backup: B, E, H, Q, C
- Tape Device

Sets up key and save file library names. Calls corresponding CL for encryption processing:

- E – AESEODSAV
- B – AESBODSAV
- H – AESHSTSAV
- Q – AESQRYSAV
- C – AESEMPSAV

These options can be run interactively or submitted to batch.

APPENDIX

SAMPLE DATA ENCRYPTION POLICY