MASS USER MANAGEMENT

(MUM)

Finally, there's a MUM to clean-up after you at work!

by Bruce and Shawn Holmstead
Holmstead Partners, Copyright (c) 1992.
All Rights Reserved.

Table of Contents

Introduction 4
- Program Description 4
- Changes in version 1.2 4

Chapter 1: Adding Users 5
- How MUM Adds Users 5
- Text File Format for Adding Users 6
  - A Note About Text File Format 7
  - Checking the Text File for Errors 7
- Examples of Adding Users 7
- Creating Templates 8
- Setting Account Restrictions using Templates 9
- Adding Options 10
  - Username and Full Name Options 10
  - Password Options 11
  - Type of Run Options--Adding 11
- Viewing Created, Not Created and MakeUser.rpt Lists 11

Chapter 2: Deleting Users 12
- Deleting Users using a File 12
- Deleting Members of a Group 13
- Deleting Disabled Accounts 13
- Deleting All Expired Accounts 13
- Deleting Directories 14
- Type of Run Options--Deleting 14
- Viewing Deleted, Not Deleted and MakeUser.rpt Lists 14

Chapter 3: Modifying Users 15
- User Restrictions that can be Changed 15
- Changing All Users 16
- Changing a Group of Users 16
- Changing Users with Old Expiration Dates 16
- Changing Users with Old Login Dates 16
- Changing Users Listed in a Text File 16

Chapter 4: Generating User Information Lists 18
- User Restrictions that can be Displayed 18
- Generating Lists for All Users 19
- Generating Lists for a Group of Users 19
- Generating Lists for Users with Old Expiration and Login Dates 19
- Generating Lists for Users Listed in a Text File 19

Chapter 5: Command Line/Batch File Usage 20
- Why MUM drops to DOS to perform operations 20
- MassMode format for ADDING USERS 20
- MassMode format for DELETING USERS 21

Chapter 6: Getting Help or Service 22
Questions about MUM 22
Upgrades/Updates 22

List of Figures and Tables

Figures

Figure 1.1: Add Menu 5
Figure 1.2: Add Users dialog box 6
Figure 1.3: List of Templates dialog box 8
Figure 1.4: Template Account Restrictions dialog box 10
Figure 1.5: Add Users dialog box 10
Figure 2.1: Delete Menu 12
Figure 2.2: Are You Sure dialog box 14
Figure 3.1: Modify Menu 15
Figure 3.2: Enter New Restrictions dialog box 16
Figure 4.1: Lists Menu 18
Figure 4.2: Choose Restrictions dialog box 19

Tables

Table 1: Sample text file 5
Table 2: Requirements for users 7
Table 3: Sample generated data 13

Introduction

Program Description:

Mass User Management (MUM) facilitates the management of four critical areas system managers frequently encounter. These include adding, deleting, updating and monitoring user accounts.

You must be a SUPERVISOR equivalent for Mass User Management to function properly. Certain information in the bindery can only be accessed by a SUPERVISOR equivalent.

Mass User Management will allow system managers to do the following:

1) **Add** large numbers of users from lists generated by a database, spreadsheet or word processing program. Mass User Management will verify names of existing users and add those who do not have accounts.
2) **Delete** users from a text file listing usernames, a certain group, disabled accounts and expired accounts.
3) **Modify** user restrictions for all users, users in a certain group, users with expirations dates older than a specified date, users with login dates older than a specified date and users in a text file.
4) Generate **Lists** of user restrictions for all users, users in a certain group, users with expirations dates older than a specified date, users with login dates older than a specified date and users in a text file.

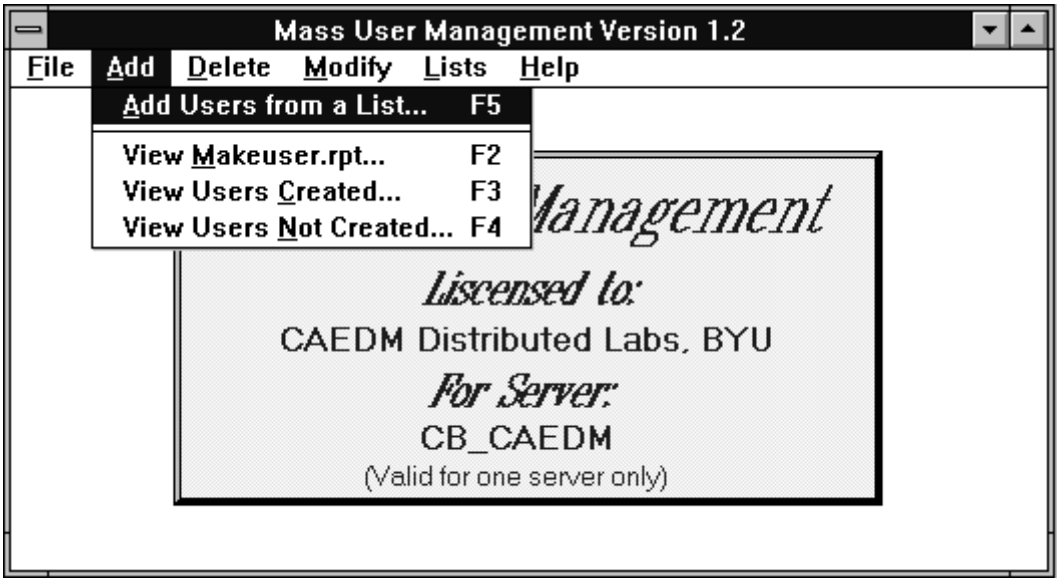
Changes in Version 1.2:

1) The password options have been expanded to allow supervisors to provide their own passwords while adding users. An additional password field can now be included in the text file used to add accounts. See Password Options for more information.
2) Under the "Delete" menu, a menu item entitled "Delete Directories" was added to allow supervisors to delete ALL trustee directory assignments of users that were deleted using MUM. This option will delete the trustee directories, their files, and sub-directories. Note that this option will delete all files including hidden and read-only files in the trustee directories given. We recommend using caution when using this new option. See Deleting Directories for more information.
3) Under all deleting options, supervisors can now execute a mock deleting run. This can be used to get a listing of trustee directory assignments. See Type of Run Options--Deleting for more details.
4) Under all menu items on the "Modify" menu, supervisors can now modify user's account balance and low limit or add to the current account balance. See User Restrictions that can be Modified for more information.
5) Also under all menu items on the "Modify" menu, supervisors can now modify user's volume restrictions for any or all volumes. See User Restrictions that can be Modified for more information.
6) Under all menu items on the "Lists" menu, supervisors can now display user's current account balance and low limit. See User Restrictions that can be Displayed for more information.
7) Also under all menu items on the "Lists" menu, supervisors can now display user's current volume restrictions and current disk space in use for all volumes on the server. See User Restrictions that can be Displayed for more information.
8) MassMode (MassUser's child program) has a completely new user interface that facilitates error checking and keeps supervisors completely informed of MUM's progress.
9) Some general bug fixes involving file sharing between MassUser and MassMode.
10) Some general bug fixes involving displaying windows on the "Modify" and "Lists" menus.
11) Help buttons have been added to all dialog boxes to allow easy access to on-line help.

Chapter 1: Adding Users

Mass User Management has the capability of adding large numbers of users at one time even if the users require varying restrictions. The adding capability of MUM makes adding ten users as easy as adding one thousand users. Templates are designed for each group of users, then used dynamically to add the users. Once users are created the system manager can review the results in the created.rpt, notcreat.rpt and makeuser.rpt report files.

Figure 1.1: The adding menu for Mass User Management allows managers to add from a list and then view the created.rpt, notcreat.rpt and makeuser.rpt report files.



How MUM Adds Users:

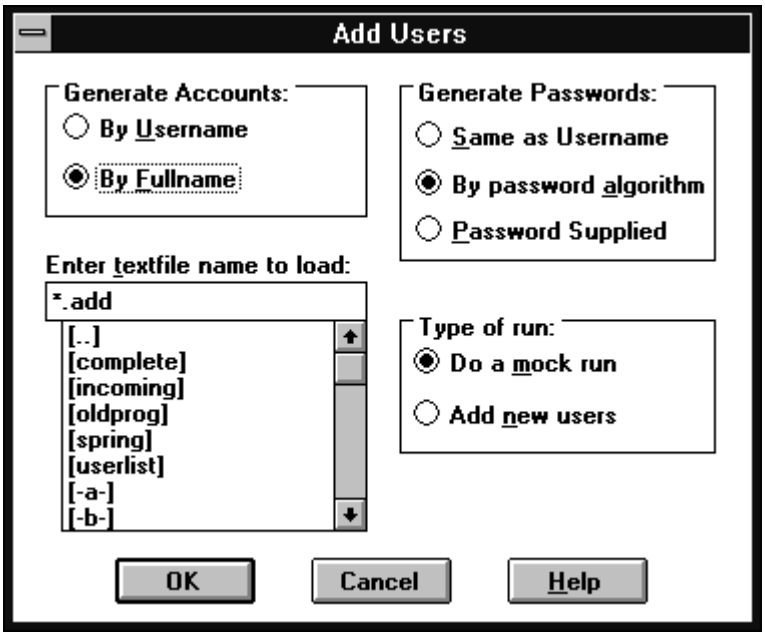
Mass User Management allows you to use a text file, similar to the format indicated in Table 1 (on the next page) to generate accounts. The text file is just an ASCII file created from database, spreadsheet or word processing programs, and uses TABS to delineate categories. MUM uses a template to connect server groups and restrictions to the department references in the text file. The template allows you to assign a user to the desired server groups; it allows you to specify volume restrictions, home directory locations, login scripts to use, and account restrictions. MUM uses the Novell utility *MakeUser* in a dynamic manner to actually add the users, so it is important that this utility be in your public folder.

Table 1. Database or Spreadsheet data: (using tabs as delimiters)

Last Name	First Name	Middle	Department (Template name)
Holmstead	S.	Bruce	Mechanical Engineering
Holmstead	Shawn	Matthew	Mechanical Engineering
Benzley	Steve		Administration
McClellan	Ron	A	CAEDM Faculty
Doe	John	Henry	Sales Group
Doe	Jane		Sales Group
Brown	Mary	Jane	Marketing Group

When you choose the **Add Users from a List** Option, you can select the following: username or full name options, password options and type of run options. When these are selected, indicate which text file to add from and press OK.

Figure 1.2: Dialog box associated with Add Users from a List.



Text File Format for Adding Users:

Text files utilized to add users should use tabs as delimiters and include at least the following fields (in this order):

1) Last Name
2) First Name
3) Middle Name
4) Department identifier
5) Username -- optional
6) Password -- optional
7) Extra Data -- optional

Templates created using MUM need to be named exactly like the department identifier in the text file (see Table 1). When MUM reads data from the text file for a user's department, it looks through the templates loaded and finds a matching department identifier. If a match is not found, MUM uses the first template in the list.

The adding function gives you the option of including a username for each individual. If you want to specify the individual's username, the 5th column should include the username.

The adding function also gives you the option of including a password for each individual. If you want to specify the individual's password, the 5th column should include the password. If you want to specify the individual's username and password, the 5th column should include the username, and the 6th column should include the password.

If you have a database that includes more fields than the ones required for MUM, you may include these after the standard 4 (or 6--depending on the username/full name and password options) required fields. The extra data (up to 512 characters) will be stored and tacked on to the end of output reports but will not be used by MUM while generating accounts.

A Note About Text File Format:

Certain editors will not save tabs when files are saved as text files.

- Some of the editors that do NOT save tabs include:
  MS DOS 5.0 Editor and WordPerfect.
- Some of the known programs that will save tabs include:
  Most spreadsheets and data base programs, WordPerfect's PEdit, and MS QuickC.

Checking the Text File for Errors:

A small utility called *VTFile* (Verify Text File) is packaged with MUM to help managers verify whether the format of their text file is correct. Just enter "vtfile" on the DOS prompt to see the purpose and format of *VTFile*.

The Mock Run option will also show you whether the format of the text file is correct. MUM v1.2 has been dramatically changed when you add users so that it now tells you exactly the data it is processing and tells you when it encounters an error in the text file format.

Examples of Adding Users:

Suppose you are charged with managing accounts for all engineering students and faculty for a large university. Each semester you receive an updated list of students from which you are to add accounts. You need to provide different restrictions for different departments (See Table 2). You are posed with the problem of:

-Tying users to their correct department server groups
-Providing home directories corresponding to departments
-Restricting volume use differently for different departments
-Giving different login scripts for each department
-Giving different account restrictions for each department
-Giving accounts only to students that do not already have an account

You need to do all of this for a large number of students and while maintaining all these changing accounts!

Table 2. Requirements for users.

Department Listing	Server Groups Home Directory Login Script
Mechanical Engineering	ME, STUDENT USER:STUDENT\ME f:\usr\supervis\std.scr
Administration	ADMIN, FACULTY FAC:ACCTS\ADMIN f:\usr\supervis\admin.scr
Sales Group	SALES, PRODUCT_GROUP USER:SALES f:\usr\supervis\sales.scr
101328 (Major Code)	CHEME, GRADUATE, STUDENT USER:STUDENT\CHEME f:\usr\supervis\std.scr

Well, it's MUM to the rescue! MUM will allow you to create templates to define different restrictions for your various group requirements. Then, it allows you to add the users using your list of students, while checking for existing accounts. Later, if you want to change the restrictions for any of your groups, MUM will allow you to change them *en masse.* You can also delete users dynamically and generate reports of your users at any time. Here's how the adding works.
MUM allows you to create a template in which you identify your different restrictions and requirements. You need to make a template for each department group and name it exactly the same as your text file department listing. For example, from Table 2 we see that we need to make a *Mechanical Engineering*, *Administration*, *Sales Group* and *101328* template. Once the templates are generated and saved in a template file, you can add the accounts.

When MUM reads in data, such as that listed in Table 1 (don't include the headings), it searches the currently loaded template file to find a template matching the data in the department field. Once found, MUM creates a username (if not provided) and adds the user according to the given requirements. If a matching template is not found, the first template entered is used as the default template.

For example, Steve Benzley, who is in administration, would be assigned to the *Administration* template. The template would link Steve with the ADMIN and FACULTY server groups; he would be given a home directory in the FAC:ACCTS\ADMIN directory so that the path to his directory would be something like: f:\accts\admin\BENZLEYS. Similarly, Bruce and Shawn Holmstead would be assigned to the *Mechanical Engineering* template which would link them to ME and STUDENT groups. Their directory paths would look like: g:\student\me\HOLMSTEB and g:\student\me\HOLMSTES respectively.

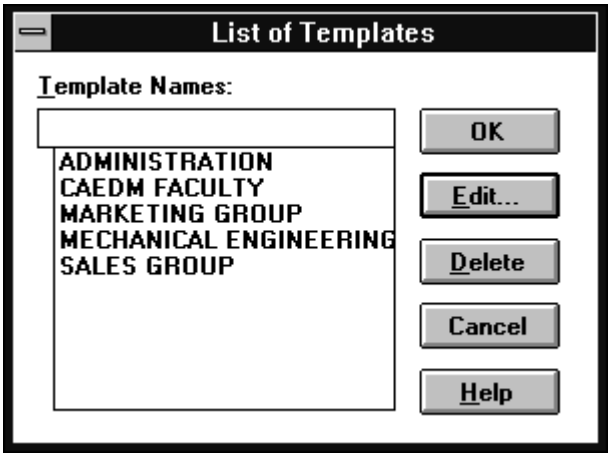
Creating Templates

MUM uses a template to connect server groups and restrictions to the department identifier in the text file. The MUM template allows you to define to which server groups the user belongs; it allows you to specify volume restrictions, home directory locations, login scripts to use, and account restrictions. MUM uses the Novell utility *MakeUser* in a dynamic manner to actually add the users, so it is important that this utility be in your public folder.

For example, using the text file listed in Table 1, you will need to make the following MUM templates (displayed in Figure 1.3):

Mechanical Engineering
Administration
CAEDM Faculty
Sales Group
Marketing Group
(case is not important)

Figure 1.3: Templates created in MUM should be named exactly as they appear in the text file.

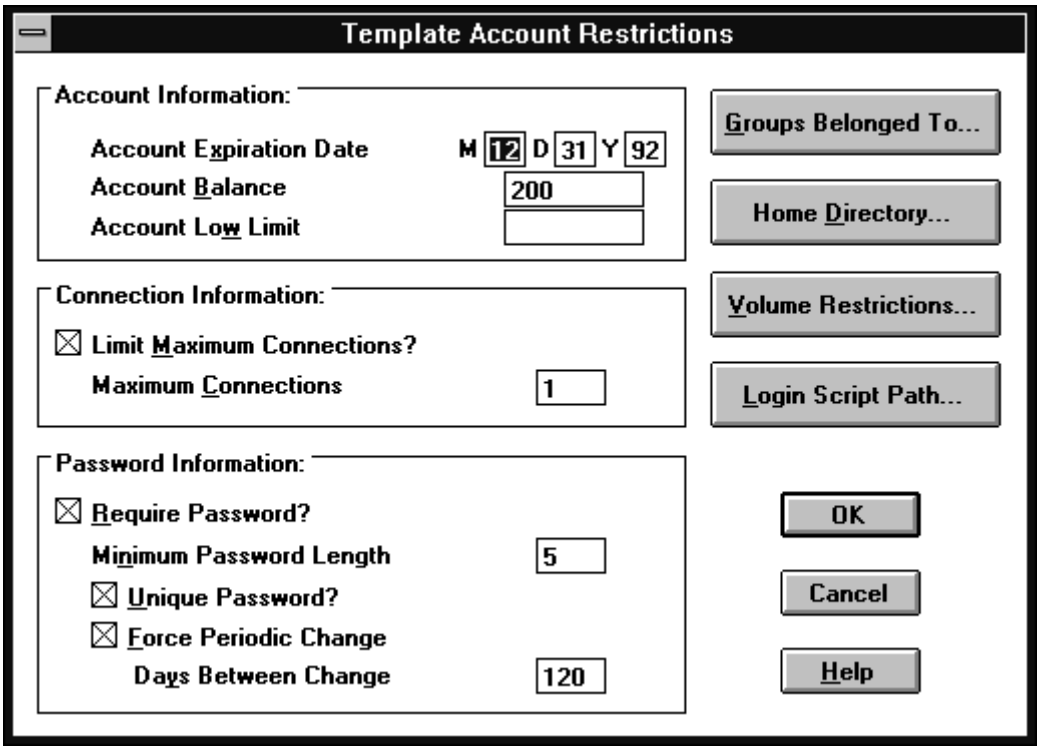


Setting Account Restrictions using Templates:

You may set the following parameters for users assigned to the particular template:

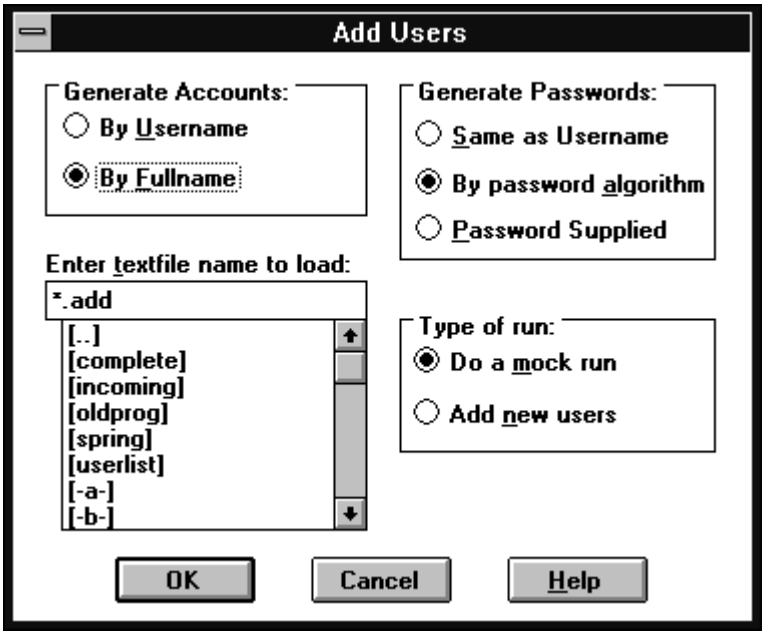
Account Information:	Set the expiration date, account balance and account low limit (Make sure accounting is installed on your server before setting account balance and account low limit).
Connection Information:	Limit the number of connections the users can have.
Password Information:	If a password is required, set the length; indicate whether or not to require a unique password and indicate whether or not to force a periodic password change.
Groups Belonged To:	Assign the users to groups *currently* existing on the server from which MUM is launched. The group must be in existence. All users will be added to the server group EVERYONE by default.
Home Directory:	Enter the volume and path for the base directory. The Home Directory will be the base directory plus the username. If the username is DOEJ and USR:STUDENT is indicated as the home directory, the real Home Directory will be: USR:STUDENT\DOEJ
Volume Restrictions:	Enter the volume name and indicate whether or not to limit space; if space is limited, indicate the limitation. Enter the exact title of the volume (ie. APPS). If a volume is not listed in Volume Restrictions, it will not be limited. For NetWare versions 2.xx, you cannot limit volumes individually; you can only enter the maximum disk space for all volumes collectively. If you are running NetWare versions 2.xx, MUM will take your volume restrictions from the SYS volume definition; if a SYS volume is not defined in the template, disk space will not be limited for any volumes.
Login Script Path:	Enter the path name and name of the login script file (ie. F:\USERS\SUPERVIS\login.scr). The login script file is an ASCII text file containing individual login script information for users assigned to the template.

Figure 1.4: MUM's account restrictions template. Templates are made for each seperate department identifier in the text file.



Adding Options:

Figure 1.5: Adding options include "Generate Accounts", "Generate Passwords", and "Type of Run".



Generate Accounts--Username and Full Name Options:

If you choose the "**Full Name**" option, MUM will check the full name field for every user on the network to see if a matching full name exists. If the full name exists, an account will not be made for that user. If the full name doesn't exist, a unique username will be generated and the account will be added. The generated username will usually be the first seven letters in the last name and the first initial of the first name. If the last name is shorter than seven letters, the username will

include the entire last name. For example, Bruce Lee would have a username of LEEB. All full names are generated from first, middle and last name text file fields.

If you choose the "**Username**" option, MUM will use data from the username field in your text file for the username. If the username already exists on the server or if a username is not found in the fifth field of the text file, the user will not be added.

Password Options:

If you choose the "**Same as Username**" option, MUM will make the passwords identical to the username with one exception. If the username is shorter than the required password length, extra "A" characters will be added to the end of the password until the password is the same length as the required password length. (ie. If the username is LEEB and the required password length is six, the actual password will be LEEBAA.)

If you choose the "**Password Algorithm**" option, MUM will generate up to an eight character password using the first four characters of the username and four random numbers. For example, if the username is HOLMSTES, the password will be essentially HOLM8324. If the username is shorter than four characters, the algorithm will use as the entire username plus four random numbers. For example, if the username is LEE, the password will be LEE1234 (4 random numbers).

If you choose the "**Password Supplied**" option, MUM will take the supplied password from the 5th field (or the 6th field if you are also supplying usernames) of the text file. If the supplied password length is less than the required password length, the user will be rejected and an account will not be made for that user. This option is new to version 1.2.

Type of Run Options--Adding:

Both run options have been dramatically changed in version 1.2. MUM will show you exactly the data it is working on and tell you if it encounters an error in the text file format. Pressing "O" for options, while in MUM's child process *MassMode*, will display the username, password and mode options you selected. It will also display the required fields for that particular operation.

If you choose the "**Mock Run**" option, MUM will step through each user in the text file showing you the data read as well as the username and password created or found. If there is an error in the text file, MUM will tell you exactly what the error is so you may fix the problem. The created.rpt and notcreat.rpt reports will also be filled with data for the users in the text file, but accounts will NOT be created for the users.

If you choose the "**Add New Users**" option, MUM will run continuously and show you the data it read for each user as well as the username and password created or found. If there is an error in the text file, MUM will tell you exactly what the error is so you may fix the problem. If you want to step through each user in the text file, press a key to pause MUM's execution (once MUM has dropped to DOS).

The created.rpt, notcreat.rpt, and makeuser.rpt reports will also be filled with data for the users in the text file, and accounts will be created for the users.

Viewing Created, Not Created and *MakeUser*Report Files:

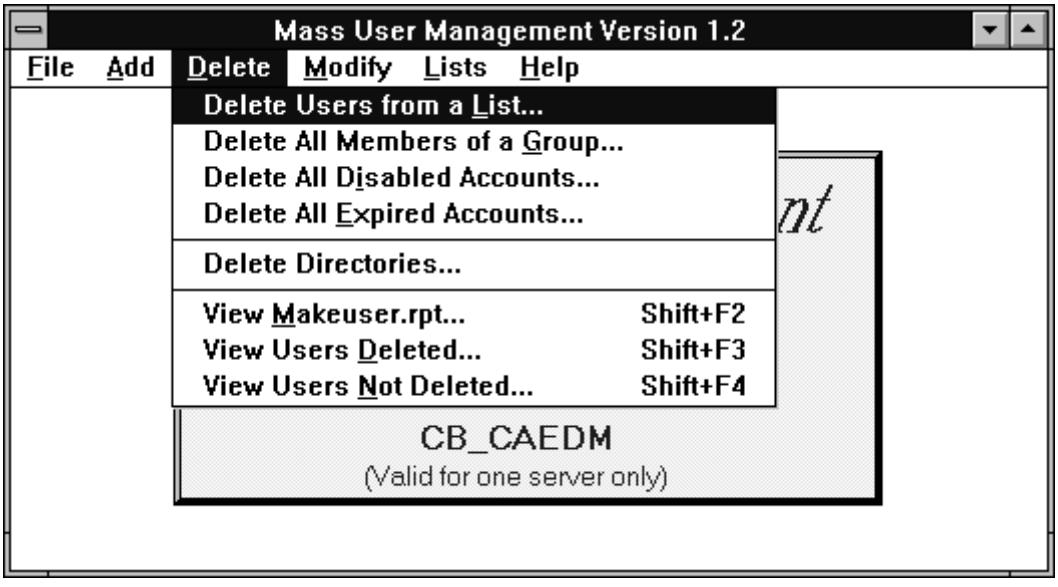
The MakeUser.rpt report is the information given by Novell's utility *MakeUser* when users are added or deleted (a MakeUser.rpt report will NOT be made when using the "Mock Run" option) . When users are added, MUM allows you to view those users created and not created. The created.rpt and notcreat.rpt files are generated by MUM each time users are added or a mock run is preformed.

System managers wanting to reuse data from the created.rpt should rename the report file before attempting to do another add run. An error will occur if the created.rpt file is selected to be used as the source text file for adding users since a new created.rpt is generated for each add run. However, the created.rpt and notcreat.rpt files CAN be used for the Delete, Modify, or Lists options; they can be renamed and then used for the Adding option.

Chapter 2: Deleting Users

Mass User Management allows system managers with supervisory status to delete users in four ways: by file, by group, by disabled account status and by last login status. MUM will output three text files for you when you delete users. It creates the MakeUser.rpt, Deleted.rpt and Notdelet.rpt files. The MakeUser.rpt file tells if users were actually deleted and reasons why they weren't. The Deleted.rpt file lists users that were deleted and the Notdelet.rpt lists users that were not deleted.

Figure 2.1: The deleting menu for Mass User Management allows managers to delete users in various categories. Once deleted they can then delete directories and view the deleted.rpt, notdelet.rpt and makeuser.rpt report files.



To delete the user's Trustee Directory assignments, use the "**Delete Directories**" option and specify the Deleted.rpt file to use as the source file containing the list of directories to be deleted. If the headers and usernames are still listed in the Deleted.rpt file when you run the "Delete Directories" option, MUM will ignore them. This option is new to version 1.2.

WARNING! If you are not careful, you could destroy your system VERY quickly. You will want to look at the Deleted.rpt file BEFORE running the "Delete Directories" option. MUM will take the given directories and delete the given directory, it's files, it's sub directories and their files. If the Deleted.rpt file gives the SYS: volume root directory as one of the Trustee Directory assignments to one of the deleted users, IT WILL DELETE THE ENTIRE SYS VOLUME. This option will delete hidden and read-only files and directories supplied (ie. BINDERY files, etc).

RECOMMENDATION: Back up your entire system before running the "Delete Directories" option. This option is very capable of deleting BINDERY files, hidden files, read-only files etc. Look through the Deleted.rpt file BEFORE running the "Delete Directories" option.

IMPORTANT: Since Mass User Management uses Novell's utilitiy *MakeUser* to actually delete the accounts, and since *MakeUser* will not re-optomize your bindery, we recommend running Bindfix quarterly to clean up your bindery.

Deleting Users using a File:

To delete using a text file, Mass User Management only requires that the username be listed first and be separated from all other fields by a tab. All files generated by MUM can be used to delete users (ie. All *.rpt files as well as any file generated using the Modify or List menu options). MUM will look for the first item on each line and assume it is the username. Table 3 illustrates how lists generated using MUM can also be used as delete lists.

Table 3. Sample of data generated from the Generate Menu. These lists can be used for deleting.

Data for Group: CAEDM

USERNAME	FULL NAME	ACCT EXP	ACCT DISAB
DUDE	S. Bruce Holmstead	None	Enabled
PUZZLED	Shawn Holmstead	None	Enabled
RON	Ron A McClellan	None	Enabled
SUPERVISOR	CAEDM SUPERVISOR	None	Enabled
SEB	Steve Benzley	None	Enabled

If you wish to use generated lists for deleting, you should delete the header on the file; however, it is not necessary.

If you select a real run, MUM will generate a Deleted.rpt, Notdelet.rpt and MakeUser.rpt files. A mock run will only generate Deleted.rpt and Notdelet.rpt files since no calls will be made to *MakeUser*.

For both types of run, the Deleted.rpt file lists users that were (or would have been) deleted along with any extra data that was included in the text file MUM read in. It will also list the deleted users trustee directories. The Notdelet.rpt file lists users that could not be deleted along with any extra data that was included in the text file used to delete.

Deleting Members of a Group:

Deleting members of a group is as easy as entering the group name. MUM will generate a report in the Delete.rpt file that lists the users deleted, and a file called Notdelet.rpt that lists users that could not be deleted.

This option supports both real and mock runs and is new to version 1.2. See Type of Run Options--Deleting for more details.

Deleting Disabled Accounts:

This option allows the system manager to scan and delete all disabled accounts on the network. Using this option in conjunction with the Modify and Lists menus can help managers to identify accounts with certain criterion and disable them with the Modify options. Managers can then use the "**Delete Disabled Accounts**" option to delete the unwanted accounts.

For example, if system managers wanted to delete all users who had not logged in for 6 months, they would use the Modify menu to identify users with old login dates and disable them. Then they would use this option to delete those disabled accounts.

MUM will generate a report in the Delete.rpt file that lists the users deleted, and a file called Notdelet.rpt that lists users that could not be deleted.

This option supports both real and mock runs and is new to version 1.2. See Type of Run Options--Deleting for more details.

Deleting All Expired Accounts:

This option prompts you for today's date and then searches the server for users with account expirations older than the date indicated. When these accounts are found they are deleted.

NOTE: Users with no expiration dates on their accounts are not deleted with this option.

MUM will generate a report in the Delete.rpt file that lists the users deleted, and a file called Notdelet.rpt that lists users that could not be deleted.

This option supports both real and mock runs and is new to version 1.2. See Type of Run Options--Deleting for more details.

Deleting Directories:

To delete the user's Trustee Directory assignments, use the "**Delete Directories**" option and specify the Deleted.rpt file to use as the source file containing the list of directories to be deleted. If the headers and usernames are still listed in the Deleted.rpt file when you run the "Delete Directories" option, MUM will ignore them. This option is new to version 1.2.

WARNING! If you are not careful, you could destroy your system VERY quickly. You will want to look at the Deleted.rpt file BEFORE running the "Delete Directories" option. MUM will take the given directories and delete the given directory, it's files, it's sub directories and their files. If the Deleted.rpt file gives the SYS: volume root directory as one of the Trustee Directory assignments to one of the deleted users, IT WILL DELETE THE ENTIRE SYS VOLUME. This option will delete hidden and read-only files and directories supplied (ie. BINDERY files, etc).

RECOMMENDATION: Back up your entire system before running the "Delete Directories" option. This option is very capable of deleting BINDERY files, hidden files, read-only files etc. Look through the Deleted.rpt file BEFORE running the "Delete Directories" option.

Type of Run Options--Deleting

MUM has been recently updated to allow system managers to do a real or mock run for deleting users.

If you choose the "**Mock Run**" option, MUM will step through each user, showing you the user it is processing along with the user's trustee directories. MUM will alert you of any errors it encounters. You may press "C" to run continuously at any time; if you need to MUM to halt while processing users, just press any key. A mock run will generate Deleted.rpt and Notdelet.rpt files indicating users that would have been deleted as well as users that could not be deleted.

If you choose the "**Real Run**" option, MUM will run continuously through the users, showing you the user it is processing along with the user's trustee directories. MUM will alert you of any errors it encounters. You may press any key to pause the processing, and then if you wish to continue processing continuously press "C". A real run will first gather all the data for the users to be deleted and then it will make calls to *MakeUser* to delete the users. Any errors from *MakeUser* will appear in the MakeUser.rpt file, while all other information concerning users deleted and not deleted will be reported in the Deleted.rpt and Notdelet.rpt files.

Figure 2.2: The "Are you sure" dialog box now allows managers to choose whether to do a real or mock run.

Viewing Deleted, Not Deleted and *MakeUser* Report Files:

The MakeUser.rpt report is generated from information given by Novell's utility *MakeUser* when users are added or deleted. When users are deleted, MUM allows you to view those users deleted and not deleted in the Deleted.rpt and Notdelet.rpt files respectively.

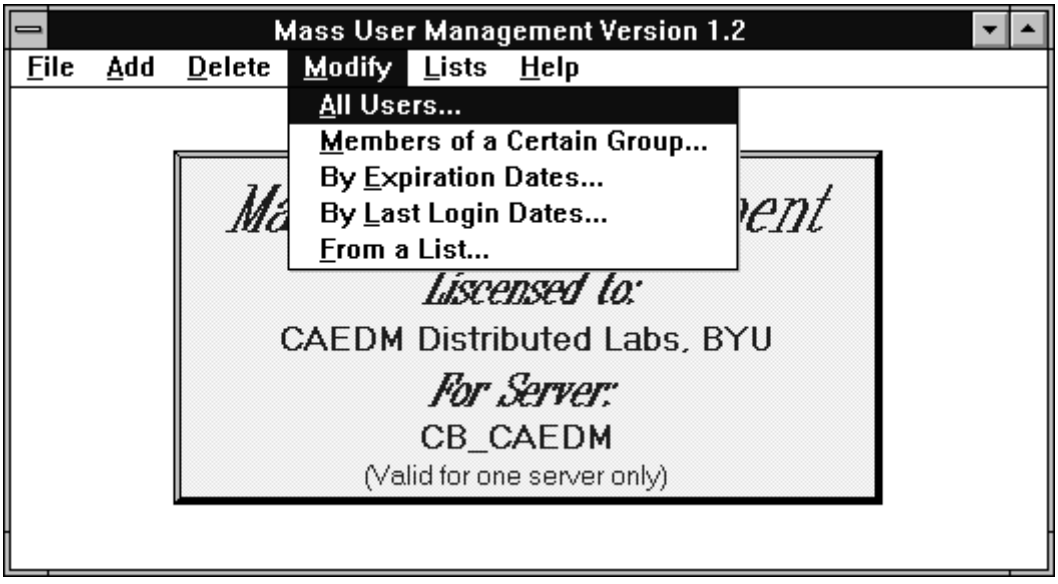
System managers wanting to reuse data from the deleted.rpt should rename the report file before attempting to do delete run. An error will occur if the deleted.rpt file is selected to be used as the source text file for deleting users since a new deleted.rpt is generated each delete run. Also, the deleted.rpt will be deleted if an error occurs during the run.

Chapter 3: Modifying Users

Mass User Management allows system managers to modify restriction for: all users, members of a certain group, users with old expiration dates and users with old login dates. For all options, output may be displayed to the screen or saved to a file. See User Restrictions that can be Modified for a detailed list of restrictions. Any fields left blank will not be changed.

Output files generated by the modify menu options are all delineated by tabs and can therefore be imported into any database, spreadsheet or word processing program. This feature allows managers to closely integrate system database files with network users to generate graphs or reports on system usage.

Figure 3.1: The Modify menu for Mass User Management allows managers to change user restricions for users in various categories.



User Restrictions that can be Modified:

(Note: Any field left blank will not be modified)

Account Expiration Date: Enter the month, day and year you wish the account expiration date to be changed to or check the "No Expiration" box to make the accounts have no expiration date.

Password Expiration Date: Enter the month, day and year you wish the password to expire or check the "No Expiration" box to make the password never expire.

Grace Logins Allowed: Enter the number of logins allowed (after the password has expired) to change the password before the account is disabled (1-20) or check the "Unlimited" box to allow unlimited logins after the password has expired.

Grace Logins Remaining: Enter the number of logins remaining to change the password (1 to Grace Logins Allowed).

Maximum Connection: Enter the number of connections a user may simultaneously login (1-200) or check the "Unlimited" box to allow an unlimited number of connections.

Minimum Password Length: Enter the minimum length of login passwords (1-20).

Days Between Pswd Change: Enter the number of days before password will change (1-365).

Enable/Disable Button: Check whether to enable or disable the account (default is to enable).

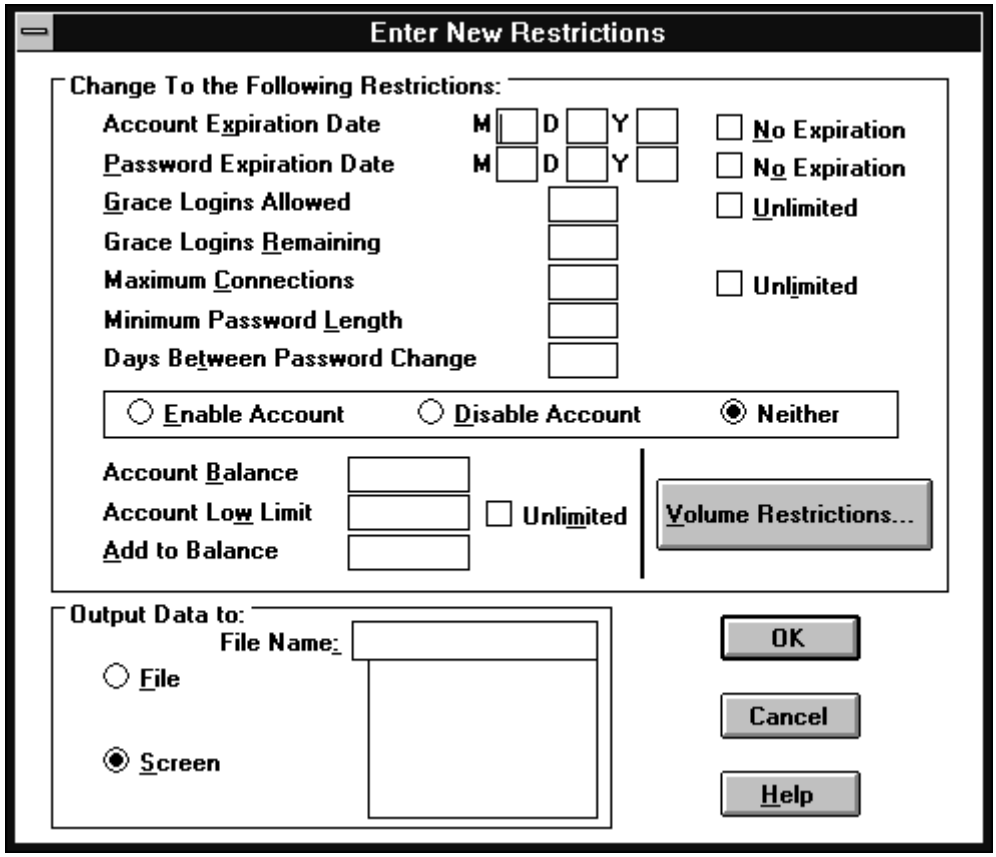
Account Balance: Enter the amount to set the account balance to (-99,999,999 to 99,999,999). Make sure accounting is set up on the server before modifying the account balance. This is new to version 1.2.

Account Low Limit: Enter the amount to set as the account low limit (-99,999,999 to 99,999,999) or check the "Unlimited" checkbox to allow unlimited credit. Make sure accounting is set up on the server before modifying the account low limit. This is new to version 1.2.

Add to Balance: Enter the amount to add to the user's current account balance (-99,999,999 to 99,999,999). Make sure accounting is set up on the server before modifying the account balance. This is new to version 1.2.

Volume Restrictions: Enter the volume name and indicate whether or not to limit space; if space is limited, indicate the limitation. Enter the exact title of the volume (ie. APPS). If a volume is not listed in Volume Restrictions, it will not be modified. For NetWare versions 2.xx, you cannot limit volumes individually; you can only enter the maximum disk space for all volumes collectively. If you are running NetWare versions 2.xx, MUM will take your volume restrictions from the SYS volume definition; if a SYS volume is not defined in the template, disk space will not be modified. This is new to version 1.2.

Figure 3.2: The "Enter New Restrictions" dialog box allows managers to change various user restrictions. The account balance and volume restrictions are new to version 1.2.



Modifying Restrictions for All Users:

When this option is selected, managers are given a choice of which field they would like to change and whether to print to the screen or to a file. Fields that are left blank will not be modified. When OK is pressed, MUM will modify all user restrictions to those that are indicated.

Modifying Restrictions for a Group of Users:

When this option is selected, managers are prompted for which group to modify. They are then taken to the standard modify dialog where they're given a choice of which field they would like to modify and whether to print to the screen or to a file. Fields that are left blank will not be modified. When OK is pressed, MUM will change user restrictions for the group indicated.

Modifying Restrictions for Users with Old Expiration Dates:

When this option is selected, managers may identify an expiration date to search for. All accounts with expiration dates older than the date indicated will be modified according to specifications identified in the "Enter New Restrictions" dialog. Fields left blank in this dialog will not be modified. When OK is pressed, MUM will modify user restrictions with expiration dates older than the date prompted for to the new restrictions.

Modifying Restrictions for Users with Old Login Dates:

When this option is selected, managers may identify a last login date to search for. All accounts with last login dates older than the date indicated will be modified according to specifications identified in the "Enter New Restrictions" dialog. Fields left blank in this dialog will not be modified. When OK is pressed, MUM will change user restrictions with last login dates older than the date prompted for to the new restrictions.

Modifying Restrictions for Users Listed in a Text File:

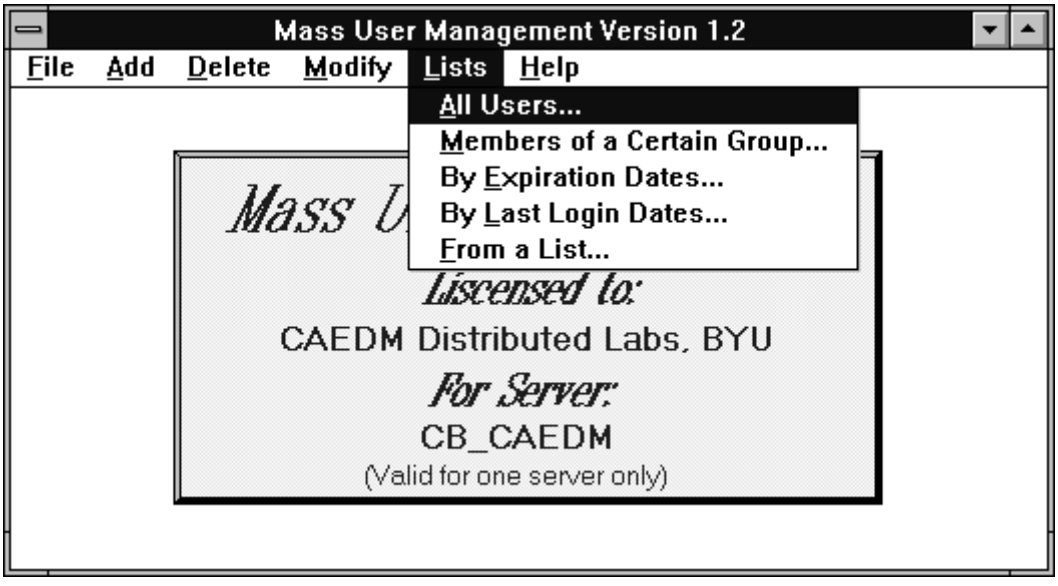
When this option is selected, managers may identify a text file containing usernames to be modified. The text file must list each username on a separate line. All list files generated using MUM may be used, as well as any of the report (.rpt) files. When the text file is selected, managers are then taken to the standard modify dialog where they're given a choice of which field they would like to change and whether to print to the screen or to a file. Fields that are left blank will not be modified. When OK is pressed, MUM will change user restrictions for the users in the text file indicated.

Chapter 4: Generating User Information Lists

Mass User Management allows system managers to generate restriction information for: all users, for members of a certain group, for old expiration dates and for old login dates. For all options, output may be displayed to the screen or saved to a file. See User Restrictions that can be Displayed for a detailed list of restrictions.

Output files generated by the lists menu options are all delineated by tabs and can therefore be imported into any database, spreadsheet or word processing program. This feature allows managers to closely integrate system database files with network users to generate graphs or reports on system usage.

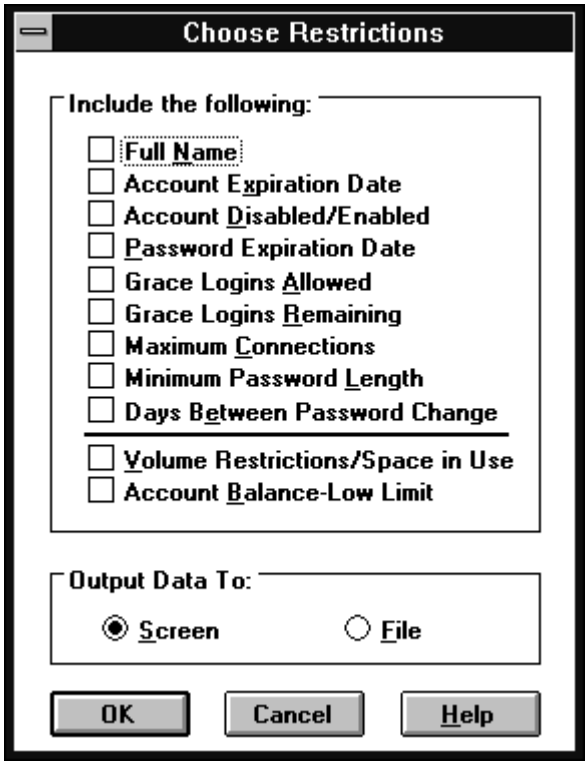
Figure 4.1: The Lists menu for Mass User Management allows managers to generate reports of user restricions for users in various categories.



User Restrictions that can be Displayed:

Full Name:	The users full name.
Account Expiration Date:	The month, day and year the account expires.
Password Expiration Date:	The month, day and year the password expires.
Grace Logins Allowed:	The number logins allowed (after the password expired) to change the password before the account is disabled.
Grace Logins Remaining:	The number of logins remaining to change the password.
Maximum Connection:	The number of connections a user may simultaneously login to.
Minimum Password Length:	The minimum length of login passwords.
Days Between Pswd Change:	The number of days before the password will change.
Account Disabled:	Whether the account is enabled or disabled.
Vol. Restrictions/Space in Use:	The volume restrictions for each volume on the server as well as the disk space in use on each volume for the individual users. This is new to version 1.2.
Account Balance--Low Limit:	The account balance and low limit for the users. This is new to version 1.2.

Figure 4.2: The "Enter New Restrictions" dialog box allows managers to change various user restrictions. The account balance and volume restrictions are new to version 1.2.



Generating Restriction Lists for All Users:

When this option is selected, managers are given a choice of which field they would like to display and whether to print to the screen or to a file. Restrictions that are not checked in the "Choose Restrictions" dialog will not be included. When OK is pressed, MUM will generate user restrictions for all users.

Generating Restriction Lists for a Group of Users:

When this option is selected, managers are prompted a group. They are then taken to the standard dialog where they are given a choice of which field they would like to display and whether to print to the screen or to a file. Restrictions that are not checked in the "Choose Restrictions" dialog will not be included. When OK is pressed, MUM will change user restrictions for the group indicated.

Generating Restriction Lists for Users with Old Expiration Dates and Old Login Dates:

When this option is selected, managers may identify an expiration date (or a login date) to search for. All accounts with expiration dates (or last login dates) older than the date indicated will be displayed according to specifications identified in the "Choose Restrictions" dialog. Restrictions that are not checked in the "Choose Restrictions" dialog will not be included. When OK is pressed, MUM will display user restrictions for users with expiration dates (or last login dates) older than the date prompted for.

Generating Restriction Lists for Users Listed in a Text File:

When this option is selected, managers may identify a text file containing usernames to generate lists for. The text file must list each username on a separate line. All list files generated using MUM may be used, as well as any of the report (.rpt) files. When the text file is selected, managers are then taken to the standard dialog where they're given a choice of which field they would like to display and whether to print to the screen or to a file. Restrictions that are not checked in the "Choose Restrictions" dialog will not be included. When OK is pressed, MUM will generate user restrictions for the users listed in the text file indicated.

Chapter 5: Command Line/Batch File Usage

Mass User Management has the capability of performing various core functions in DOS mode. Descriptions of the command line arguments of MUM's child process, *MassMode* are detailed below. Command line arguments are listed for MUM's adding and deleting capabilities.

Why MUM drops to DOS to perform operations:

1) One reason MUM drops into DOS to perform network operations is to allow system managers to add and delete users from a batch file. Managers who have their templates created and need to add or delete users on a regular basis can make the appropriate calls to *MassMode* without having to run *MassUser* each time.

2) Another reason MUM drops to DOS is so that it can be more backwards compatible with older versions of NetWare. Mass User Management uses Novell's utility *MakeUser* in a dynamic way to add users. Because the NetWare utility *MakeUser* is available with NetWare versions 2.11 and up, *MassUser* will provided needed service to more versions of NetWare.

MassMode format for ADDING USERS:

MassMode can add users given the following command line arguments:

a1 NONE filename accounts password run template_name

Description of arguments:

Argument	**Meaning**
a1	Adding code
NONE	Put any character into this field
filename	The name of the text file to add users from
accounts	*Generate Accounts Option:* 1 = Username option 0 = Full name option
password	*Generate Password Option:* 2 = Password Provided 1 = Same as Username 0 = Password Algorithm
run	*Type of Run Option:* 1 = Mock Run 0 = Real Run
template_name	Name of the template file to use to add users
NONE	Put any character into this field

Example: f:> massmode a1 0 students.add 1 1 0 winter.tmp

NOTE: Mock runs will be automatically paused while in *MassMode*; system managers can then choose to step through the run or allow it to run continuously. Real runs will not be paused unless a key is pressed while running.

MassMode format for DELETING USERS:

MassMode can delete users from several different username sources given the following command line arguments:

Username Src	d#	group	file	month	day	year	run
a file	d1	NONE	file_d1	NONE	NONE	NONE	run
a group	d2	group	NONE	NONE	NONE	NONE	run
disabled accounts	d3	NONE	NONE	NONE	NONE	NONE	run
expired accounts	d4	NONE	NONE	month	day	year	run
delete dir's	d5	NONE	file_d5	NONE	NONE	NONE	NONE

Description of arguments:

Argument	Meaning
d#	Deleting code
group	Group to use to delete from
file_d1	The name of the text file containing users to be deleted
file_d5	The text file (usually DELETED.RPT) containing paths of directories to be deleted.
month	The month to use for expired accounts
day	The day to use for expired accounts
year	The year to use for expired accounts
run	*Type of Run Option:* 1 = Mock Run 0 = Real Run (The default is Real Run if this field is left blank.)
NONE	Put any character into this field

Examples:

Mock Runs

```
f:> massmode d1 0 students.add 0 0 0 1
f:> massmode d2 faculty 0 0 0 0 1
f:> massmode d3 0 0 0 0 0 1
f:> massmode d4 0 0 12 31 91 1
f:> massmode d5 0 deleted.rpt 0 0 0 1
```

Real Runs

```
f:> massmode d1 0 students.add
f:> massmode d2 faculty
f:> massmode d3
f:> massmode d4 0 0 12 31 91
```

NOTE: Mock runs will be automatically paused while in *MassMode*; system managers can then choose to step through the run or allow it to run continuously. Real runs will not be paused unless a key is pressed while running.

Chapter 6: Getting Help or Service

Questions about MUM:

Questions about MUM are answered by E-mailing to:

PARTNERS@world.std.com

If you are unable to E-mail, you can write to:

Holmstead Partners
P. O. Box 50452
Provo, UT 84605-0452

As of the time of printing, phone support is not available. If necessary, we will be happy to set up phone support with you directly if you provide us with a phone # and time to call.

Upgrades/Updates:

We will notify all registered users of any updates to the software and how to obtain them.

If upgrades become available, registered users will be entitled to them at a discounted price. Only the person/entity who originally purchases the program are considered registered. Discounted upgrades apply only to the person/entity who originally purchased the software.

Notes: