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.

[Ordering Information](#)
[Program Description](#)
[Batch File Usage](#)

[Template Information](#)
[Adding Users](#)
[Deleting Users](#)
[Changing User Restrictions](#)
[Generating Lists of User Restrictions](#)
[List of Menus](#)

Ordering Information

Mass User Management is available on a per server licensing agreement. **

Company Information:

Name _____

Company Name _____

Street Address _____

City _____ State _____ Zip _____

Telephone Number _____

Ordering:

Quantity_____@ $350*   _____Sub Total

_____ Tax

(Utah residents add 6.25% Sales Tax)

_____ Total

Department name to appear in licence agreement:

_____

Send Check or Money Order to:

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

*Price subject to change without notification.
**For information about site licences (or any other questions) write to the above address or send E-mail to:

       PARTNERS@bones.caedm.byu.edu

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.

Overview:

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

1) <u>Add</u> 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) <u>Delete</u> users from a text file listing usernames, a certain group, disabled accounts and expired accounts.
3) <u>Change</u> 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) <u>Generate</u> 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.

Advantages of Mass User Management:

Mass User Management is an essential tool for all managers required to manage large numbers of users. It adds and deletes users dynamically and then allows managers to modify restrictions once the users are created.   It also allows managers to create lists of users and their restrictions.

1) MUM drastically saves time for the system manager who is constantly adding new users or the system manager who needs to add large numbers of users at one time.

2) MUM adds and deletes users dynamically.   It allows managers to define a template for each user group, and then add users according to a set of templates without separating users into different lists or having to add each user individually.

   <u>MUM vs. UserDef</u>
   - Novell's utility *UserDef* allows system managers to define different templates for different groups of users, but requires that managers select a current template and then add users one-by-one.
   - MUM allows system managers to define different templates for different departments and then add any number of users from any of the defined departments all at once.

   <u>MUM vs. MakeUser</u>
   -   Novell's utility *MakeUser* allows system managers to add larger numbers of users at one time but managers loose the advantage of having templates defined for different groups.   The files for *MakeUser* need to be specially prepared for *MakeUser* and are not really reusable.   Users need to be group together and the restrictions file layout is not cohesive to large numbers of users.

3) MUM will deleted all disabled accounts or accounts that have not logged in for a certain period of time.   It can deleted all users in a certain server group or delete all users listed in a text file.

4) MUM allows system managers to modify user restrictions in bulk after they are added.

5) MUM allows managers to create lists of users and their restrictions.   These lists can be read back into spreadsheet or database programs.

6) MUM was written to allow system managers to add and delete users from a <u>batch file</u>; this can be performed by calling MUM's child process, *MassMode*.

Overall, no program on the market offers the features to system managers that Mass User Management does.   Some programs limit the number of users that can be managed, but MUM is not limited by such restrictions.   Mass User Management is a critical tool enabling managers to stay in control of their networks.

Batch File Usage

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:

a1   NONE   filename_to_use_to_add   accounts   password   run   template_name

ARGUMENTS	MEANING
a1	Adding code
NONE	Put any character into this field
filename_to_use_to_add	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:* 　1 = Same as Username 　0 = Password Algorithm
run	*Type of Run Option:* 　1 = Mock Run 　0 = Add Users
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 0

MassMode format for DELETING USERS:

Depending upon the source of usernames, MassMode can delete users given the following criterion:

Username Source	d#	group	filename_to_use_to_delete	month	day	year	NONE	NONE
a file	d1	NONE	filename_to_use_to_delete	NONE	NONE	NONE	NONE	NONE
a group	d2	group	NONE	NONE	NONE	NONE	NONE	NONE
disabled accounts	d3	NONE	NONE	NONE	NONE	NONE	NONE	NONE
expired accounts	d4	NONE	NONE	month	day	year	NONE	NONE

ARGUMENTS	MEANING
d#	Deleting code
group	Group to use to delete from
filename_to_use_to_delete	The name of the text file to delete users from
month	The month to use for expired accounts
day	The day to use for expired accounts

year	The year to use for expired accounts
NONE	Put any character into this field
NONE	Put any character into this field

Examples:

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

Adding Users

How MUM Adds Users:

Mass User Management allows you to use a text file, similar to the format indicated in Table 1, 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 define which server groups the user belongs to; 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.

<u>Table 1</u>.   Database or Spreadsheet data: (delimiters are tabs)

Last Name	First Name	Middle	Department (Template name)
Holmstead	S.	Bruce	Mechanical Engineering
Holmstead	Shawn	Matthew	Mechanical Engineering
Benzley	Steve		Administration
McClellan	Ron	C.	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 will be given <u>username or full name options</u>, <u>password options</u> and <u>type of run options</u>.   When these are selected, indicate which text file to add from and press OK.

Related Topics:
<u>Text File Format for Adding Users</u>
<u>Creating Templates</u>
<u>Examples of Adding Users</u>

<u>Username and Full Name Options</u>
<u>Password Options</u>
<u>Type of Run Options</u>

<u>Viewing Reports</u>

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) Extra Data -- optional

Templates created using MUM need to be named exactly like the department listing in the text file (see Table 1).   When MUM reads data from the text file for a users department, it looks through the templates loaded and finds a match.   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.

If you have a data base that includes more fields than the ones required for MUM, you may include these after the standard 4 (or 5--depending on the username/full name option) 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.

Related Topics:
How MUM Adds Users
Creating Templates
Examples of Adding Users

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:

> -Tieing 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

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, its MUM to the rescue!   MUM allows you to create a template in which you identify these 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 <u>Table 1</u> (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 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.

Related Topics:
<u>How MUM Adds Users</u>
<u>Text File Format for Adding Users</u>
<u>Creating Templates</u>

Creating Templates

MUM uses a template to connect server groups and restrictions to the department references in the text file.   The template allows you to define which server groups the user belongs to; 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.

Related Topics:
Setting Account Restrictions using Templates
Text File Format for Adding Users

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.   Al 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.

Related Topics:
Creating Templates
Username and Full Name Options
Password Options
Type of Run Options

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 (up to seven) and the first initial of the first name.

All full names are generated from first, middle and last name text file fields.   Full names are converted to capital letters for comparison.

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, the user will not be added.

Related Topics:
Creating Templates
Setting Account Restrictions using Templates
Password Options
Type of Run Options

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", MUM will generate an eight character password using the first four characters of the username and four random numbers.
(ie.   If the username is HOLMSTES, the password will be essentially HOLM8324.)

Related Topics:
Creating Templates
Setting Account Restrictions using Templates
Username and Full Name Options
Type of Run Options

Type of Run Options:

If you want to do a trial run to see how MUM works when adding users, select the "Mock Run" option.

To actually add accounts, select the "Add New Users" option.

Related Topics:
Creating Templates
Setting Account Restrictions using Templates
Username and Full Name Options
Password Options

Viewing Created, Not Created and MakeUser.rpt Lists:

The MakeUser.rpt is the information given by Novell's utility *MakeUser* when users are added or deleted. When users are added, MUM allows you to view those users created and not created.   Just select the menu item under the <u>Add Users</u> menu.

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 two text files for you when you delete users.   It creates a <u>MakeUser.rpt</u> file a <u>Deleted.rpt</u> and a <u>Notdelet.rpt</u> file.   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.

Related Topics:
<u>Deleting Users using a File</u>
<u>Deleting Members of a Group</u>
<u>Deleting Disabled Accounts</u>
<u>Deleting All Expired Accounts</u>

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.   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--this is because all files generate by MUM will list the username first.

Table 3.   Sample of Data Generated from the <u>Generate Menu</u>.   These lists can also 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 C. McClellan	None	Enabled
SUPERVISOR	CAEDM SUPERVISOR	None	Enabled
SEB	Steve Benzley	None	Enabled

If you wish to use generated lists as deleting lists, you should delete the header on the file; however, it is not necessary.   MUM uses the first word on each line of the text file as the username.

The <u>Deleted.rpt</u> file lists users that were deleted along with any extra data that was included in the text file MUM read in.   The <u>Notdelet.rpt</u> file lists users that were not deleted along with any extra data that was included in the text file used to delete.

Related Topics:
<u>Deleting Members of a Group</u>
<u>Deleting Disabled Accounts</u>
<u>Deleting All Expired Accounts</u>

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.

Related Topics:
Deleting Users using a File
Deleting Disabled Accounts
Deleting All Expired Accounts

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 Change Users menu can help managers to identify accounts with certain criterion and disable them with the Change Users 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 <u>Change Users menu</u> to identify users with old login dates and disable them.   Then they would use this option to delete those disabled accounts.

Related Topics:
<u>Deleting Users using a File</u>
<u>Deleting Members of a Group</u>
<u>Deleting All Expired Accounts</u>

Deleting All Expired Accounts:

This option prompts you for todays 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.

Related Topics:
Deleting Users using a File
Deleting Members of a Group
Deleting Disabled Accounts

Viewing Deleted, Not Deleted and MakeUser.rpt Lists:

The MakeUser.rpt is the 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.   Just select the menu item under the Delete Users menu.

Change User Restrictions

Mass User Management allows system managers to change restriction 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.

Related Topics:
User Restrictions that can be Changed
Changing Restrictions for All Users
Changing Restrictions for a Group of Users
Changing Restrictions for Users with Old Expiration Dates
Changing Restrictions for Users with Old Login Dates
Changing Restrictions for Users Listed in a Text File

User Restrictions that can be Changed:

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

Account Expiration Date: Enter the month, day and year you wish the account to be changed to.

Password Expiration Date: Enter the month, day and year you wish the password to expire.

Grace Logins Allowed: The number of logins allowed (after the password has expired) to change the password before the account is disabled (1-20).

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

Maximum Connection: The number of connections a user may simultaneously login (1-200).

Minimum Password Length: The length of login passwords (1-20).

Days Between Password Change   Number of days before password will change (1-365).

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

Related Topics:
Changing Restrictions for All Users
Changing Restrictions for a Group of Users
Changing Restrictions for Users with Old Expiration Dates
Changing Restrictions for Users with Old Login Dates
Changing Restrictions for Users Listed in a Text File

Changing 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 change all user restrictions to those that are indicated.

Related Topics:
User Restrictions that can be Changed
Generating Restrictions for All Users

Changing 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 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 group indicated.

Related Topics:
User Restrictions that can be Changed
Generating Restrictions for a Group of Users

Changing 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 "Change New Restrictions" dialog.   Fields left blank in this dialog will not be modified.   When OK is pressed MUM will change user restrictions with expiration dates older than the date prompted for to the new restrictions.

Related Topics:
User Restrictions that can be Changed
Generating Restrictions for Users with Old Expiration Dates

Changing 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 "Change 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.

Related Topics:
User Restrictions that can be Changed
Generating Restrictions for Users with Old Login Dates

Changing 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.   Lists generated using MUM may be used. 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.

Related Topics:
User Restrictions that can be Changed
Generating Restrictions for Users Listed in a Text File

Generating Lists of User Restrictions

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.

Related Topics:
User Restrictions that can be Displayed
Generating Restrictions for All Users
Generating Restrictions for a Group of Users
Generating Restrictions for Users with Old Expiration Dates
Generating Restrictions for Users with Old Login Dates
Generating Restrictions for Users Listed in a Text File

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 length of login passwords

Days Between Password Change: The number of days before the password will change.

Account Disabled: Whether the account is enabled or disabled.

Related Topics:
Generating Restrictions for All Users
Generating Restrictions for a Group of Users
Generating Restrictions for Users with Old Expiration Dates
Generating Restrictions for Users with Old Login Dates
Generating Restrictions for Users Listed in a Text File

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.

Related Topics:
User Restrictions that can be Displayed
Changing Restrictions for All Users

Generating Restriction Lists for a Group of Users:

When this option is selected, managers are prompted for which group to generate lists for.   They 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 change user restrictions for the group indicated.

Related Topics:
User Restrictions that can be Displayed
Changing Restrictions for a Group of Users

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 password expiration to search for.   All accounts with expiration 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 login dates older than the date prompted for.

Related Topics:
User Restrictions that can be Displayed
Changing Restrictions for Users with Old Expiration Dates
Changing Restrictions for Users with Old Login Dates

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.   List files generated using MUM may be used. 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.

Related Topics:
User Restrictions that can be Displayed
Changing Restrictions for Users Listed in a Text File

Lists of Menus

FILE MENU
New Templates
Load Templates
Edit Templates

Ordering Info

Exit

ADD MENU
Add Users from a List

View MakeUser.rpt
View Users Created
View Users NOT Created

DELETE MENU
Delete Users from a List
Delete All Members of a Group
Delete All Disabled Accounts
Delete All Expired Accounts

View MakeUser.rpt
View Users Deleted
View Users NOT Deleted

MODIFY MENU
All Users
Members of a Certain Group
By Expiration Dates
By Last Login Dates
From a List

LISTS MENU
All Users
Members of a Certain Group
By Expiration Dates
By Last Login Dates
From a List

HELP MENU
Contents

Ordering Info
About

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

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