MASS USER MANAGEMENT for NetWare 3.x (MUM)

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

by Bruce and Shawn Holmstead
Holmstead Partners, Copyright (c) 1992-1993.

Table of Contents

Part 1: Program Description

1.1 Program Brief

Mass User Management for NetWare 3.x (MUM) facilitates the management of four critical areas Novell system managers frequently encounter. These include adding, deleting, updating and monitoring user accounts.

You must be a SUPERVISOR equivalent on a Novell 3.x server for Mass User Management to function properly. Certain information in the bindery can only be accessed by a SUPERVISOR equivalent.

1.2 Program Functionality

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 user names, 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.

Part 2: Installing Mass User Management

2.1 System Requirements

These are the minimum system requirements to run Mass User Management for 386 NetWare v1.3:

Novell NetWare 3.x Server
Microsoft Windows 3.1
Minimum of 1.5 megabytes (1,500 kbytes) of free hard disk space
The NetWare client software for DOS and Windows

2.2 Installing the Program

Installing Mass User Management

1) Enter the MUM System Disk into drive a (or b).
2) From Windows select Run under the File Menu and enter **a:install**
3) Answer any questions the install program prompts you for.

Adding the MUM Icon to your Desktop

1) In the Program Manager select the New menu item under the **File** Menu.
2) Select a new program item
3) Enter the path and program name in the Command Line text box. (e.g. c:\mum\massuser.exe)

Part 3: Managing Templates

3.1 Creating Templates

Mass User Management uses a template to connect Novell server groups and restrictions to a particular user while adding or modifying users. When adding or modifying from a list, templates are matched with a field in the text file representing the department identifier. Templates allow you to define which Novell server groups the user belongs to; it also allows you to specify volume restrictions, home directory locations, login scripts to use, account restrictions, etc.

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

Development
Marketing
Sales Group
Tech Support
(case is not important)

A template file (*.tmp) can contain up to 100 individual templates and you can have as many template files as your heart desires.

Related Topics
Setting Account Restrictions using Templates

3.2 Setting Account Restrictions using Templates

The Current Settings windows reflects a summary of the account restrictions for the current template. To edit these restrictions choose the appropriate button in the Edit Settings section of the window.

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

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. You can also enter the number of days before the account will expire, and MUM will determine the appropriate expiration date. The "Days Before Account Expires" is not saved anywhere in the Bindery -- it is only for convenience while running MUM. Only the "Account Expiration Date" or "No Expiration" fields are saved in the Bindery.

Enable/Disable/Remain Same Buttons: Check whether to enable or disable the account (default is to remain same). If you choose "Remain Same", the account status will remain the same as it is currently configured for each user.

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.

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.

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.

Change Password: You may change the password if you are modifying an individual user. Press the "Change Password" button and then enter the new password. Retype the password to make sure you entered the correct password.

Require Password: Check the "Require Password" checkbox to force the users to have a password. If the users are not forced to have a password, they may still have a password however.

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

Unique Passwords Required: Check the "Unique Passwords Required" checkbox to force the users to supply a unique password when they change their password.

Require Periodic Change: Check the "Require Periodic Change" checkbox to force the users to supply a new password periodically. The length of this period is defined in the "Days Between Change" edit box.

Days Between Change: Enter the number of days between forced password changes. When you enter the number of days between changes, the password expiration date is automatically calculated for you. You can uncheck the "Require Periodic Change" checkbox to make the password never expire.

Password Expiration Date: Enter the month, day and year you wish the password to expire or uncheck the "Require Periodic Change" box to make the password never expire. The password expiration date does not have to match the "Days Between Change" edit box. You can set the password to expire earlier or later than the "Days Between Change". Once the password has expired, the "Days Between Change" will calculate the next password expiration date.

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.

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).

Volume Restrictions: Highlight the volume name and press "Edit" to set the space restriction for that volume. Indicate whether or not to limit space; if space is limited, indicate the limitation.

Remove Other Volume Restrictions: Check the "Remove Other Volume Restrictions" checkbox to not limit volume space on the volumes you do not explicitly specify. For instance, if you only specify to limit the SYS volume and then check the "Remove Other Volume Restrictions" checkbox, the users will only have a volume restriction on the SYS volume. Any volume restrictions on other volumes will be removed. Do not check the "Remove Other Volume Restrictions" checkbox to limit only certain volumes and to leave the other volume restrictions as they are. For instance, to limit the SYS volume and leave the other volume restrictions intact, do not check the "Remove Other Volume Restrictions" checkbox.

Groups Belonged To: The "Groups Belonged To" are shown on the left list box, and the other "Available Groups" are displayed on the right list box. To make the users belong to a group displayed in the "Available Groups", either highlight the group in the "Available Groups" list box and press the "Insert" button or double click on the group. To remove a group from the "Groups Belonged To", either highlight the group and press the "Delete" button or double click on the group.

Remove Other Groups Belonged To: Check the "Remove Other Groups Belonged To" checkbox to make the users only belong to the groups you

specify. If you do not check the "Remove Other Groups Belonged To" checkbox, the groups shown in the "Groups Belonged To" list box will be added to the user's list of groups belonged to. For instance, if you want to make sure the users you are modifying are in the APPS group, double click on the APPS group in the "Available Groups" list box so the group is displayed in the "Groups Belonged To" list box. By leaving the "Remove Other Groups Belonged To" checkbox unchecked, the users modified will belong to all groups they previously belonged to plus be added to the APPS group.

Create Group: MUM gives you the ability to create a new group on the fly. Just press the "Create Group" button and enter the new group name. The recently created group will then appear in the "Available Groups" list box.

Home Directory: Enter the volume and path for the base directory. The Home Directory will be the base directory plus the user name. If the user name is DOEJ and USR:STUDENT is indicated as the home directory, the real Home Directory will be: USR:STUDENT\DOEJ. A browse facility is provided to browse existing directories. If the directory you enter does not exist, MUM will attempt to create the directory.

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. A browse facility is provided to browse existing files. An edit facility is also provided to allow you to edit the file.

Batch File: Enter the path name and name of the batch file to be run in conjunction with adding users (ie. F:\USERS\SUPERVIS\ addbat.bat). This will not be executed when the users are added but can be run from the menu when an add run is completed (a DOS program called RunBatch.exe is spawned when this menu is selected.) A browse facility is provided to browse existing files. An edit facility is also provided to allow you to edit the file.

Related Topics
Creating Templates

3.3 Changing Servers

To facilitate the use of Mass User Management on multiple servers, you may select a desired server. You will need to be attached to the selected server to make MUM fully functional on that server.

NOTE:

MUM is still licensed on a per server basis so be careful that you are not violating your license agreement when selecting another server. If you do work on two servers using MUM then you need two licenses, etc.

Part 4: Adding Users

4.1 How MUM Adds Individual Users

Mass User Management allows you to enter an individual's name and criterion to use to add the user. You have the following options:

Use a personalized user name algorithm or supply your own user name
Use a password algorithm or supply your own password
Define what to do if the account exists
Define which template to use for the users restrictions
Actually add the user or perform a test run
Whether or not to append the created.rpt file generated for this run to a master report file (master.rpt)

Once these options are specified, MUM will add the user according to the criterion you have set. These new features allowing you to manage individual users as well as users "en masse" and should substantially reduce your need to use other utilities (e.g. SysCon) to supplement MUM. These options are also saved in the massuser.ini file allowing you to customize MUM to your particular needs.

4.2 How MUM Adds Users from a List

Mass User Management uses a template to connect Novell server groups and restrictions to a particular user while adding or modifying users. When adding or modifying from a list, templates are matched with a field in the text file representing the department identifier. Templates allow you to define which server groups the user belongs to; it also allows you to specify volume restrictions, home directory locations, login scripts to use, and account restrictions, etc. See Managing Templates for more information.

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 simply an ASCII file created from a database, spreadsheet or word processing program. Tabs, commas or spaces are used to delineate categories. MUM uses a previously defined template to connect Novell account restrictions to the department references in the text file.

Table 1. Database or Spreadsheet data:

Last Name	First Name	Middle	Department (Template name)	
Holmstead		S.	Bruce	Development
Holmstead		Shawn	Matthew	Development
McClellan	Ron	A	Marketing	
Crandal	John	H.	Sales Group	
Doe	Jane		Tech Support	

Once you have created your ASCII file you have the following options when adding users.

Use a personalized user name algorithm or supply your own user name
Use a password algorithm or supply your own password
Define what to do if the account exists
Define which template to use for the users restrictions
Actually add the user or perform a test run
Define the format of your ASCII file (e.g. tabs, commas or spaces)
Whether or not to append the created.rpt file generated for this run to a master report

file (master.rpt)

When you are ready to perform the operation press OK and MUM will display the users as they are processed. In addition, MUM will generate reports for users that were created, not created or modified during the adding run. Any errors will be written to an error report log (ERRORLOG.RPT). You may view all these report files using the View Menu.

Related Topics
Text File Format for Adding Users
Creating Templates
Examples of Adding Users

User name and Full Name Options
Password Options
Type of Run Options
Modifying Existing Accounts While Adding

Viewing Reports

4.3 User name 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, MUM will modify the account if you selected the "Apply Template" option. Otherwise, an account will not be made for that user. If the full name doesn't exist, a unique user name will be generated using the current user name algorithm and the account will be added.

All full names are generated from first, middle and last name text file fields.

If you choose the "**User name**" option, MUM will use data from the user name field in your text file for the user name. If the user name already exists on the server or if a user name is not found in the 5th field of the text file, the user will not be added. If you selected the "Apply Template" option, however, the account will be modified.

Related Topics
Password Options
Account Exists Options
Type of Run Options

4.4 Password Options

If you choose the "**Same as User name**" option, MUM will make the passwords identical to the user name with one exception. If the user name is shorter than the required password length, extra random numbers will be added to the end of the password until the password is the same length as the required password length. (ie. If the user name is LEEB and the required password length is six, the actual password might be LEEB56.)

If you choose the "**Password Algorithm**" option, MUM will generate a password using up to the first four characters of the user name and four random numbers. For example, if the user name is HOLMSTES, the password will be essentially HOLM8324. If the generated password is shorter than the minimum password length, random numbers will be added until the password is the correct length. For example, if the user name is LA and the minimum password length is 6, the password might be LA23456 (Full user name + 4 random numbers +1 extra random number).

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 user names) 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.

Related Topics
User name and Full Name Options
Account Exists Options
Type of Run Options

4.5 Account Exists Options

If you choose the "**Don't Modify**" option, MUM will not modify the user account if a duplicate fullname or user name is found on the server. The users whose accounts already exist will appear in the modified.rpt file to show that their accounts already exist (even though the account wasn't modified).

If you choose the "**Apply Template**" option, MUM will modify the user account if a duplicate fullname or user name is found on the server. The users whose accounts already exist will appear in the modified.rpt file to show that their accounts already exist.

When modifying user accounts, if a particular restriction of the existing account has a higher restriction than the template, MUM will leave the current restriction. If the template is higher than the existing restriction, MUM will modify that restriction to match the template. For example, say the account DOEJ already exists with the following restrictions (in part):

No account expiration
2 Concurrent Logins
Disk restriction of 512 K on the SYS volume

The template matching user DOEJ during the add run has the following restrictions (in part):

Account expiration of 1/1/95
No Limit to the number of concurrent logins
Disk restriction of 2048 K on the SYS volume

User DOEJ will have the following restrictions (in part) after being modified:

No account expiration
No Limit to the number of concurrent logins
Disk restriction of 2048 K on the SYS volume

NOTE:
The algorithm used to modify accounts while adding is different than the algorithm used with the "Modify" menu items. The "Modify" menu items do not compare restrictions, but force the account restrictions to be the restrictions you specify. Thus, you can modify existing accounts in two different ways by either using the "Modify" menu items or by doing an Add Run and specifying the "Apply Template" option.

Related Topics
User name and Full Name Options
Password Options
Type of Run Options

4.6 Type of Run Options--Adding

MUM will show you exactly the data it is working on and tell you if it encounters an error in the text file format. This may go by quite rapidly, so you can view the error report log (ERRORLOG.RPT) afterwards to see what error's were associated with which users.

If you choose the "**Mock Run**" option, MUM will run continuously and show you data it read for each user in the text file showing you the data read as well as the user name 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, notcreat.rpt and modified.rpt reports will also be filled with data for the users in the text file, but accounts will NOT be created or modified for the users.

If you choose the "**Add New Users**" option, MUM will run continuously and show you data it read for each user in the text file showing you the data read as well as the user name 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, notcreat.rpt, and modified.rpt reports will also be filled with data for the users in the text file, and accounts will be created and modified (if selected) for the users.

Related Topics
User name and Full Name Options
Password Options
Account Exists Options
Type of Run Options

4.7 Text File Format for Adding Users

Text files utilized to add users should use either tabs, commas or spaces 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) User name -- optional
6) Password -- optional
7) Extra Data -- optional

The fields can be separated by tabs, commas or a number of spaces. You can enter blank fields when delimiting with tabs or commas, but the field still needs to be there. For example, if John Doe does not have a middle name and you are delimiting with commas, your text file could look like the following:

Doe,John,,Template Name

If you use tabs instead of commas, make sure there are two tabs between "John" and "Template Name" as follows:

Doe	John		Template Name

WARNING:
You CANNOT enter blank fields when delimiting with spaces. MUM looks for at least the number of spaces you specify to separate fields. If you have blank fields, MUM will end up using erroneous information when adding users.

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 will not create or modify the account but will put the user's information in the notcreat.rpt report and put an error message in errorlog.rpt.

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

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 user name and password , the 5th column should include the user name, and the 6th column should include the password.

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 6--depending on the user name/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.

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.

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

4.8 Example of Adding Users 'en masse'

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 while maintaining all these changing accounts!

Table 2. Requirements for users.

Department Listing	Server Groups Home Directory Login Script
Mechanical Engineering	DEVELOP, 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 and faculty, 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 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 user name (if not provided) and adds the user according to the given requirements. If a matching template is not found, the user is not created and an error is generated in the errorlog.rpt report.

For example, John Crandall, who is in the sales group, would be assigned to the *Sales Group* template. The template would link John with the SALES and PRODUCT_GROUP server groups; he would be given a home directory in the USER:SALES directory so that the path to his directory would be something like: f:\sales\CRANDALJ. 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
How MUM Adds Users
Text File Format for Adding Users
Creating Templates

4.9 Personalizing a User name Algorithm

Overview of the User name Algorithm

Since many people like to use varying user name algorithms, we have provided a means to customize an algorithm for the creation of user names from a users first, middle and last name.

Defining a user name algorithm involves defining:

1) the number of characters to use from each name (referred to as name fragments)
2) the order of the name fragments
3) the name fragment replaced if a duplicate name is found (only the first character of the selected name fragment is replaced)

To aid in creating a user name algorithm, MUM displays what two sample users' user name would look like using the currently defined algorithm.

The *Next User name* button will indicate what user name will be used if a duplicate user name is found on the system. The *Standard Algorithm* button sets the user name algorithm to the algorithm used in previous versions of MUM.

Defining the Number of Characters in Each Name Fragment

Again, a name fragment is a portion of a given users first, middle and last name.

User names are composed of name fragments from the first, middle and last name of the user. You may have a maximum of 8 characters in the user name, so you can decide how many characters of each name to use.

Defining the Order of Name Fragments

Next, you will need to decide what order the name fragments should appear in the user name. Some people prefer the first name fragment at the first of the user name and some prefer it at the end.

Order the first, middle and last name fragments with values 1, 2 or 3. You must order all fragments even if you do not intend to use a particular fragment.

Defining the Name Fragment to be Replaced

The Name to be Replaced field indicates which name fragment will be replaced if a duplicate user name is found on the system. If the name fragment indicated is longer than one character, only the first character of the fragment will be replaced with a new character.

Using the *Next User name* button will help you get a feel for which character is being replaced.

Related Topics

Adding Users

4.10 Running Batch Files

Selecting the Run Batch Files menu item launches a DOS program that takes a created.rpt file as input and then runs any batch file associated with what department and matching template the user is in. The batch file will begin in the users home directory.

You will need to specify two things:
1) identify the created.rpt file
2) identify a drive letter MUM can use temporarily to map a drive to the users home directory. If that drive is already mapped, the current mapping will be saved and restored after runbatch.exe is finished executing.

Note: Make sure the drive letter specify for MUM to temporarily use is not the same drive letter as the one defined in the template identifying the location of the batch file. For example, if you specified the batch file to be at f:\users\sales.bat, do NOT use drive F for MUM to temporarily map to the user's home directory.

MUM needs a drive letter to use temporarily to map a drive in order to run the batch file and will restore the drive letter to it's original state when finished. MUM will map root the drive letter to the user's home directory. If the home directory doesn't exist, MUM will generate and error and will not run the batch file.

Your batch file can use assume two input fields %1 for the user name and %2 for the userid (corresponds to the users mail directory). A sample batch file could be as follows:

```
REM Copy Windows files to the user's home directory
md windows
cd windows
xcopy f:\users\setup\windows\*.* *.* /s

REM For testing the batch file, put in pause statements to view batch file output
pause

REM Set a user name variable
SET USERNAME=%1

REM Copy news reading files to the user's mail directory
map g:=sys:mail\%2
copy f:\users\setup\news\*.* g:
map del g:
```

The output of runbatch.exe will be saved in the runbatch.rpt file. You can view this file under the View menu. The output from the batch file will not be saved in this file. Only the output from runbatch.exe itself is saved in this file.

Related Topics
Adding Users

Part 5: Deleting Users

5.1 Overview

Mass User Management allows system managers with supervisory status to delete users in five ways: by file, by group, by individual, by disabled account status and by last login status. MUM will output three text files for you when you delete users. It creates the Deleted.rpt, Notdelet.rpt and Errorlog.rpt files. The Deleted.rpt file lists users that were deleted, the Notdelet.rpt lists users that were not deleted and the ErrorLog.rpt reports any errors encountered when deleting users.

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 user names are still listed in the Deleted.rpt file when you run the "Delete Directories" option, MUM will ignore them.

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 and it's tree structure. 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 (e.g. 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

We recommend running Bindfix quarterly to clean up your bindery or after adding or deleting large numbers of users.

Related Topics

Deleting an Individual User
Deleting Members of a Group
Deleting Disabled Accounts
Deleting Expired Accounts
Deleting Users using a File
Deleting Directories
Type of Run Options
Viewing Deleted and Not Deleted Reports

5.2 Deleting an Individual User

When the option to delete an individual user is chosen, MUM will prompt you for a search criterion to identify the a particular user. Since some systems have many thousands of users, we wanted to alleviate the need to unnecessarily display all of the users on your network. As many of you know this becomes very tedious and time consuming. Instead we will display only the users matching the search criterion you enter. If you want to list all users enter the wild card character '*' for the search criterion. If you want to list all the users beginning with B enter "B*" and press *Search*. If you know the name of the user you wish to delete, you can also enter the user name in the "User Name" edit box.

When you have identified the user you wish to delete, press the delete button. You will then be given 'Are you sure' prompts to verify your choice. The user's trustee directory assignments will be saved in a file with the user name as the title. For example, if you delete user DOEJ, the user's trustee directory assignments will be saved in a file called DOEJ.RPT. Use the "Delete Directories" option on this file to delete the user's trustee directory assignments.

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

5.3 Deleting Members of a Group

Deleting members of a group is as easy as selecting a group name. MUM will generate a report in the Deleted.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. See Type of Run Options--Deleting for more details.

Related Topics
Deleting an Individual User
Deleting Disabled Accounts
Deleting Expired Accounts
Deleting Users using a File
Deleting Directories

5.4 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 Deleted.rpt file that lists the users deleted, and a file called Notdelet.rpt that lists users that could not be deleted.

Note: Users who have never logged in ARE deleted with this option.

This option supports both real and mock runs. See Type of Run Options--Deleting for more details.

Related Topics
Deleting an Individual User
Deleting Members of a Group
Deleting Expired Accounts
Deleting Users using a File
Deleting Directories

5.5 Deleting Expired Accounts

This option prompts you for a 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 Deleted.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. See Type of Run Options--Deleting for more details.

Related Topics
Deleting an Individual User
Deleting Members of a Group
Deleting Disabled Accounts
Deleting Users using a File
Deleting Directories

5.6 Deleting Users using a File

To delete using a text file, Mass User Management only requires that the user name 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 user name. 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: APPS

USER NAME	FULL NAME	ACCT EXP	ACCT DISAB
BRUCE	S. Bruce Holmstead	None	Enabled
SHAWN	Shawn Holmstead	None	Enabled
RON	Ron A McClellan	None	Enabled
JANE	Jane Doe	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 and Notdelet.rpt. A mock run will only generate Deleted.rpt and Notdelet.rpt files but not actually delete the user.

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.

Related Topics
Deleting an Individual User
Deleting Members of a Group
Deleting Disabled Accounts
Deleting Expired Accounts
Deleting Directories

5.7 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 are still listed in the Deleted.rpt file when you run the "Delete Directories" option, MUM will ignore them.

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 and it's tree structure. 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 (e.g. 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

We recommend running Bindfix quarterly to clean up your bindery or after adding or deleting large numbers of users.

Related Topics
Overview
Deleting Directories
Type of Run Options

5.8 Type of Run Options--Deleting

MUM allows system managers to do a real or mock run for deleting users.

If you choose the "**Mock 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. 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. Any errors will appear in the Errorlog.rpt file, while all other information concerning users deleted and not deleted will be reported in the Deleted.rpt and Notdelet.rpt files.

Related Topics
Overview
Viewing Deleted and Not Deleted Reports

Part 6: Modifying User Restrictions

6.1 Overview

Mass User Management allows system managers to modify restriction for: an individual user, all users, members of a certain group, users with old expiration dates, users with old login dates, users with disabled accounts, and users in a text file. 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.

Instead of having to enter account restrictions each time you modify, you may select a template of restrictions and then customize those restrictions to fit your immediate need for modifying users.

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.

Related Topics
User Restrictions that can be Modified
Modifying an Individual User
Modifying All Users
Modifying Members of a Group
Modifying by Expiration Dates
Modifying by Login Dates
Modifying Disabled User Accounts
Modifying Users Listed in a File

6.2 User Restrictions that can be Modified

The Current Settings windows reflects a summary of the account restrictions for the current template. To edit these restrictions choose the appropriate button in the Edit Settings section of the window.

(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. You can also enter the number of days before the account will expire, and MUM will determine the appropriate expiration date. The "Days Before Account Expires" is not saved anywhere in the Bindery -- it is only for convenience while running MUM. Only the "Account Expiration Date" or "No Expiration" fields are saved in the Bindery.

Enable/Disable/Remain Same Buttons: Check whether to enable or disable the account (default is to remain same). If you choose "Remain Same", the account status will remain the same as it is currently configured for each user.

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.

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.

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.

Change Password: You may change the password if you are modifying an individual user. Press the "Change Password" button and then enter the new password. Retype the password to make sure you entered the correct password.

Require Password: Check the "Require Password" checkbox to force the users to have a password. If the users are not forced to have a password, they may still have a password however.

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

Unique Passwords Required: Check the "Unique Passwords Required" checkbox to force the users to supply a unique password when they change their password.

Require Periodic Change: Check the "Require Periodic Change" checkbox to force the users to supply a new password periodically. The length of this period is defined in the "Days Between Change" edit box.

Days Between Change: Enter the number of days between forced password changes. When you enter the number of days between changes, the password expiration date is automatically calculated for you. You can uncheck the "Require Periodic Change" checkbox to make the password never expire.

Password Expiration Date: Enter the month, day and year you wish the password to expire or uncheck the "Require Periodic Change" box to make the password never expire. The password expiration date does not have to match the "Days Between Change" edit box. You can set the password to expire earlier or later than the "Days Between Change". Once the password has expired, the "Days Between Change" will calculate the next password expiration date.

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.

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).

Volume Restrictions: Highlight the volume name and press "Edit" to set the space restriction for that volume. Indicate whether or not to limit space; if space is limited, indicate the limitation.

Remove Other Volume Restrictions: Check the "Remove Other Volume Restrictions" checkbox to not limit volume space on the volumes you do not explicitly specify. For instance, if you only specify to limit the SYS volume and then check the "Remove Other Volume Restrictions" checkbox, the users will only have a volume restriction on the SYS volume. Any volume restrictions on other volumes will be removed. Do not check the "Remove Other Volume Restrictions" checkbox to limit only certain volumes and to leave the other volume restrictions as they are. For instance, to limit the SYS volume and leave the other volume restrictions intact, do not check the "Remove Other Volume Restrictions" checkbox.

Groups Belonged To: The "Groups Belonged To" are shown on the left list box, and the other "Available Groups" are displayed on the right list box. To make the users belong to a group displayed in the "Available Groups", either highlight the group in the "Available Groups" list box and press the "Insert" button or double click on the group. To remove a group from the "Groups Belonged To", either highlight the group and press the "Delete" button or double click on the group.

Remove Other Groups Belonged To: Check the "Remove Other Groups Belonged To" checkbox to make the users only belong to the groups you

specify. If you do not check the "Remove Other Groups Belonged To" checkbox, the groups shown in the "Groups Belonged To" list box will be added to the user's list of groups belonged to. For instance, if you want to make sure the users you are modifying are in the APPS group, double click on the APPS group in the "Available Groups" list box so the group is displayed in the "Groups Belonged To" list box. By leaving the "Remove Other Groups Belonged To" checkbox unchecked, the users modified will belong to all groups they previously belonged to plus be added to the APPS group.

Create Group: MUM gives you the ability to create a new group on the fly. Just press the "Create Group" button and enter the new group name. The recently created group will then appear in the "Available Groups" list box.

Related Topics
Modifying an Individual User
Modifying All Users
Modifying Members of a Group
Modifying by Expiration Dates
Modifying by Login Dates
Modifying Disabled User Accounts
Modifying Users Listed in a File

6.3 Modifying an Individual User

When the option to modify an individual user is chosen, MUM will prompt you for a search criterion to identify the a particular user. Since some systems have many thousands of users, we wanted to alleviate the need to unnecessarily display all of the users on your network. As many of you know this becomes very tedious and time consuming. Instead we will display only the users matching the search criterion you enter. If you want to list all users enter the wild card character '*' for the search criterion. If you know the name of the user you wish to modify, you can also enter the user name in the "User Name" edit box.

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 the user specified.

Related Topics
User Restrictions that can be Modified

6.4 Modifying 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.

Note: The SUPERVISOR user will not be modified. The only way to modify the SUPERVISOR user is to modify an individual user and select the SUPERVISOR user.

Related Topics
User Restrictions that can be Modified

6.5 Modifying Members of a Group

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.

Note: The SUPERVISOR user will not be modified. The only way to modify the SUPERVISOR user is to modify an individual user and select the SUPERVISOR user.

Related Topics
User Restrictions that can be Modified

6.6 Modifying Users by Expiration Date

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. Users with no expiration date will not be modified. 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.

Note: The SUPERVISOR user will not be modified. The only way to modify the SUPERVISOR user is to modify an individual user and select the SUPERVISOR user.

Related Topics
User Restrictions that can be Modified

6.7 Modifying Users by Login Date

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. Users who have never logged in will be modified. 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.

Note: The SUPERVISOR user will not be modified. The only way to modify the SUPERVISOR user is to modify an individual user and select the SUPERVISOR user.

Related Topics
User Restrictions that can be Modified

6.8 Modifying Disabled User Accounts

When this option is selected, managers may modify all disabled accounts. 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.

Note: The SUPERVISOR user will not be modified. The only way to modify the SUPERVISOR user is to modify an individual user and select the SUPERVISOR user.

Related Topics
User Restrictions that can be Modified

6.9 Modifying Users Listed in a File

When this option is selected, managers may identify a text file containing user names to be modified. The text file must list each user name 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.

Related Topics
User Restrictions that can be Modified

Part 7: Generating Lists of User Restrictions

7.1 Overview

Mass User Management allows system managers to generate restriction information for: an individual user, all users, members of a certain group, old expiration dates, old login dates, disabled accounts, and users in a text file. 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.

Related Topics
User Restrictions that can be Displayed
Reports for an Individual User
Reports for All Users
Reports for a Group of Users
Reports by Expiration Dates
Reports by Login Dates
Reports for Disabled User Accounts
Reports for Users Listed in a File

7.2 User Restrictions that can be Displayed

Press the "Select All Restrictions" button to easily check all checkboxes. Press the "Clear All Restrictions" button to easily uncheck all checkboxes.

Full Name: The users full name.

Account Expiration Date: The month, day and year the account expires.

Account Disabled/Enabled: Whether the account is enabled or disabled.

Account Balance--Low Limit: The account balance and low limit for the users.

Password Required: Whether the account is forced to have a password.

Password Expiration Date: The month, day and year the password expires.

Minimum Password Length: The minimum length of login passwords.

Days Between Password Change: The number of days before the password is forced to change.

Unique Passwords Required: Whether unique passwords are required when a user changes their password.

Maximum Connection: The number of connections a user may simultaneously login to.

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.

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.

Groups Belonged To: All of the groups the user belongs to.

Related Topics
Reports for an Individual User
Reports for All Users
Reports for a Group of Users
Reports by Expiration Dates
Reports by Login Dates
Reports for Disabled User Accounts
Reports for Users Listed in a File

7.3 Generating Reports for an Individual User

When the option to generate a report for an individual user is chosen, MUM will prompt you for a search criterion to identify the a particular user. Since some systems have many thousands of users, we wanted to alleviate the need to unnecessarily display all of the users on your network. As many of you know this becomes very tedious and time consuming. Instead we will display only the users matching the search criterion you enter. If you want to list all users enter the wild card character '*' for the search criterion. If you know the name of the user you wish to view, you can also enter the user name in the "User Name" edit box.

When this option is selected, managers are shown the standard modify dialog. However, all buttons to modify the account are disabled. The manager can only view the account restrictions for the selected user.

Related Topics
User Restrictions that can be Displayed

7.4 Generating Reports 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

7.5 Generating Reports Lists for a Group of Users

When this option is selected, managers are prompted for 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.

Related Topics
User Restrictions that can be Displayed

7.6 Generating Reports by Expiration and 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. Users with no expiration date will not be displayed. However, users who have never logged in will be displayed. 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.

Related Topics
User Restrictions that can be Displayed

7.7 Generating Reports for Disabled User Accounts

When this option is selected, managers may get a list of disabled accounts. Managers are 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

7.8 Generating Reports for Users Listed in a File

When this option is selected, managers may identify a text file containing user names to generate lists for. The text file must list each user name 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.

Related Topics
User Restrictions that can be Displayed

Part 8: Viewing Report Files

8.1 Overview

Mass User Management allows system managers to easily view the report files generated by MUM or any ASCII text file. Below is a list of the files you can view with MUM and a short explanation of each file:

Users Created	Displays the created.rpt file showing all users created during the last real or mock adding run. This file contains the user name, last name, first name, middle name, department identifier, password, server name, and any extra data.
Users Not Created	Displays the notcreat.rpt file showing all users not created during the last real or mock adding run. View the "Error Report" to see why these users were not added. This file contains the user name, last name, first name, middle name, department identifier, password, server name, and any extra data.
Users Modified during Add	Displays the modified.rpt file showing all users whose accounts were modified during the last real or mock adding run. View the "Error Report" to see if there were any errors modifying these accounts. This file contains the user name, last name, first name, middle name, department identifier, password, server name, and any extra data.
Batch File Report	Displays the runbatch.rpt file showing the messages generated by RUNBATCH.EXE during the last batch file run. The runbatch.rpt file does not show what the actual batch file did however, only status and error messages generated by RUNBATCH.EXE. To view the output of the actual batch file, put pause messages in the batch file at key points so you can read the output. Once the batch files are running the way you want them to, make sure to remove these pause messages to allow the batch files to run without waiting for you to press a key.
Users Deleted	Displays the deleted.rpt file showing all users deleted and their trustee directories during the last real or mock deleting run. This file contains the user name and that user's trustee directories. Use the "Delete Directories" option to delete the user's trustee directories (and their files).
Users NOT Deleted	Displays the notdelet.rpt file showing all users not deleted during the last real or mock deleting run. This file contains the user name of the users not deleted. View the "Error Report" to see why these users were not deleted.
Deleted Directories	Displays the deldirs.rpt file showing all trustee directories (and their files) deleted during the last delete directories run. View the "Error Report" to see if any errors occurred during the delete directories run.
Modify/List Report	Displays the passit.fil file containing the data generated during the last modify or list run. A subsequent modify or list run will overwrite this file. View the "Error Report" to see if any errors occurred during the modify or list run.
Error Report	Displays the errorlog.rpt file containing any errors and a possible explanation that occurred any time during program execution. This file is overwritten every time any kind of run is executed, so only the most recent error messages are displayed. If an error occurred outside of a run (such as when

	creating a group or changing a password), you are generally given the option to view the error log.
A File	Displays any ASCII text file. You are given a browse dialog to help you choose the file you would like to view.

Related Topics

Controls While Viewing Files

8.2 Controls While Viewing Files

When viewing any files with MUM, you are given a standard set of controls. In the bottom right corner of the dialog shows the current page out of the total number of pages (such as Page 3/5). If there is more than one page, the following controls are available for use:

Prev	Takes you to the previous page.
Next	Takes you to the next page.
Beg	Takes you to the first page.
End	Takes you to the last page.
Goto	Gives you the option to go to any page you specify.

Related Topics
Viewing Report Files

Part 9: Getting Help

9.1 How to Get Help With MUM

If you have any questions about how MUM works, there are three ways you can get help:

1. You can e-mail us at partners@world.std.com. We generally try to answer all e-mail questions the same day.
2. You can write to us at:
   Holmstead Partners
   P.O. Box 50452
   Provo, UT 84605-0452
3. You can call us at: (801) 375-8890. If we do not answer the phone, leave a message and we will try to get right back to you.

Part 10: Lists of Menus

10.1 Quick Menu Search

File Menu
New Templates
Load Templates
Edit Templates

Change Server

Exit

Add Menu
Individual User
From a List

Delete Menu
Individual User
Members of a Group

Disabled Accounts
Expired Accounts

From a File

Directories

Modify Menu
Individual User
All Users
Members of a Group

By Expiration Date
By Last Login Date
Disabled Accounts

From a File

Lists Menu
Individual User
All Users
Members of a Group

By Expiration Date
By Last Login Date
Disabled Accounts

From a File

View Menu
Viewing Report Files
Users Created

Users NOT Created
Users Modified during Add
Batch File Report

Users Deleted
Users NOT Deleted
Deleted Directories

Modify/List Report
Error Report

A File

Table 1. Database or Spreadsheet data:

Last Name	First Name	Middle	Department (Template name)	
Holmstead		S.	Bruce	Development
Holmstead		Shawn	Matthew	Development
McClellan	Ron	A	Marketing	
Crandal	John	H.	Sales Group	
Doe	Jane		Tech Support	

User name Option. Database or Spreadsheet data:

Last Name	First Name	Middle	Department	User name	
Holmstead		S.	Bruce	Development	bruce
Holmstead		Shawn	Matthew	Development	shawn
McClellan	Ron	A	Marketing	ron	
Crandal	John	H.	Sales Group	john	
Doe	Jane		Tech Support	jane	

Fullname option and Password Supplied. Database or Spreadsheet data:

Last Name	First Name	Middle	Department	Password	
Holmstead		S.	Bruce	Development	bruce234
Holmstead		Shawn	Matthew	Development	shawn234
McClellan	Ron	A	Marketing	ron234	
Crandal	John	H.	Sales Group	john234	
Doe	Jane		Tech Support	jane234	

User name option and Password Supplied. Database or Spreadsheet data:

Last Name	First Name	Middle	Department	User name	Password
Holmstead		S.	Bruce	Development	bruce bruce234
Holmstead		Shawn	Matthew	Development	shawn shawn234
McClellan	Ron	A	Marketing	ron	ron234
Crandal	John	H.	Sales Group	john	john234
Doe	Jane		Tech Support	jane	jane234

Ordering Information

(Print this form using the Print Topic menu item under the File menu.)

Mass User Management (MUM) for 386 NetWare is available on a per server licensing agreement with site licenses available. You will need a license for each server you do work on using MUM.

We accept company, government, and university Purchase Orders. We also accept check, money orders, VISA and Master Card.

To contact Holmstead Partners concerning ordering questions, please call:
(801) 375-8890
You may also contact Holmstead Partners via e-mail at:
partners@world.std.com
Finally, you can contact Holmstead Partners via regular mail at:
HOLMSTEAD PARTNERS
P.O. Box 50452
Provo, UT 84605-0452
USA

Company Information:

Contact Name _____

Company Name _____

Street Address _____

Additional Mailing Information _____

City _____ State/Province _____

Country _____ Zip/Postal Code _____

Telephone Number _____

E-mail address to send updates: _____

Department name to appear in license agreement:

_____

Ordering Worksheet:

** Note: Prices subject to change without notification. Contact Holmstead Partners to verify pricing. **

Individual Purchases:

Quantity	Price	Cost
_____	$390.00 ea.	_____

	Sub Total	_____
Educational Discount	- 20%	_____
(Utah Residents add 6.25%)	Tax	_____
	Total	_____

If no sales tax: Tax Exemption No. _____

Site License:

Type of Institution	Price	Check One
Education:		
College in a University(< 20 servers) (or small Academy/University)*	$1190.00	_____
Multiple Colleges (20 - 40 servers)	$2380.00	_____
> 40 servers contact Holmstead Partners		
Yearly Renewel Fee	1/4 of purchase price	
Business:		
Company Department (< 20 servers)	$1700.00	_____
Multiple Departments (20 - 40 servers)	$3400.00	_____
> 40 servers contact Holmstead Partners		
Yearly Renewel Fee	1/4 of purchase price	

	Sub Total	_____
(Utah Residents add 6.25%)	Tax	_____
	Total	_____

If no sales tax: Tax Exemption No. _____

*Contact Holmstead Partners to see if you qualify
Note that the price on site licenses for education reflects a 30% discount

If ordering with VISA or Master Card, please fill in the following information:

Card Holder's Name _____

Card Number _____ Expiration Date _____

Card Holder's Signature _____

Send Check, Money Order, Purchase Order or this form with VISA and Master Card information to:

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

You can also call in VISA and Master Card orders to (please have all of this information ready when you call):

Holmstead Partners

(801) 375-8890

- All prices may be subject to change without notification.
- For information about site licenses (or any other questions) write to the above address, call the above number, or send E-mail to:

PARTNERS@world.std.com