

Eytcheson
Software

Multi-Remote Registry Change v4

Rule the Registry!

Multi-Remote Registry Change v4
Copyright © 1998-2004, Eytcheson Software
All Rights Reserved

Contents

1. Overview.....	5
2. Features.....	6
3. System Requirements	7
4. General Instructions	8
5. The Main Window	12
<i>Computer Names List.....</i>	<i>12</i>
<i>The Operations tabs.....</i>	<i>13</i>
<i>The Status Display</i>	<i>13</i>
<i>The Status Bar</i>	<i>14</i>
<i>Data File Location</i>	<i>14</i>
<i>5.a Logging</i>	<i>14</i>
<i>5.b Retry Log</i>	<i>15</i>
<i>5.c Advanced Selections</i>	<i>16</i>
6. Operations.....	17
<i>Note on disabling</i>	<i>17</i>
<i>6.a Change Single Key.....</i>	<i>17</i>
<i>6.b Change Many Keys (Key Group)</i>	<i>18</i>
<i>6.c Check for Key.....</i>	<i>18</i>
<i>6.d Shutdown Systems.....</i>	<i>18</i>
<i>6.e REG File Operations</i>	<i>19</i>
<i>6.f Lookup IP Addresses</i>	<i>20</i>
<i>6.g Change User Rights</i>	<i>20</i>
<i>6.h Apply from File</i>	<i>21</i>
<i>6.i Create "Call" Batch File</i>	<i>22</i>
<i>6.j Registry Security</i>	<i>23</i>
<i>Registry Security Actions List.....</i>	<i>23</i>
<i>Registry Security Detail Dialog</i>	<i>24</i>
<i>Permissions.....</i>	<i>25</i>
<i>Security Object Inheritance</i>	<i>25</i>
<i>6.k Browse Registry</i>	<i>26</i>
<i>6.l Send Message.....</i>	<i>27</i>
<i>6.m Change Service User Info.....</i>	<i>27</i>

6.n Search and Replace	28
6.o Insert into REG_MULTI_SZ	28
6.p Dump Key to .REG File	28
6.q Manage Services.....	29
7. Substitutions.....	30
Registry Substitutions.....	30
Run Query Using Substitutions.....	35
8. Quick Entry	37
9. Tools.....	38
String Conversion.....	38
SID <-> UserName.....	38
10. Options	39
Use Alternate User Credentials	39
Verbose Log Entries.....	39
Open Default Log File Folder.....	39
Retry Log items.....	40
Retry Log Entry Warning Count.....	40
Allow Connect Retries	40
Save n Entries for Reuse.....	40
Set Max Active Threads	40
EVERY USER Options	40
Use Profile Paths for *EVERY USER*	40
Save Tab Settings on Exit	41
Always Update Tab Settings on Exit.....	41
11. Command Line Options	42
12. Troubleshooting, Updates and Support	43
Troubleshooting	43
Updates	44
Support	44
13. Ordering	45
Order Form.....	45

14. License	47
--------------------------	-----------

1. Overview

Multi-Remote Registry Change is the easiest way to manage the registry on multiple remote computers running Windows NT/2000/XP/2003. It is designed for network administrators working with groups of systems requiring the same change(s) on many computers.

Version 3.1 provides support for Windows 95/98, but that support is limited by the capabilities of the operating system. This document will apply only to version 4.

The demo version allows only 10 computers at a time in the Computer Names list. Purchase information is near the bottom of this document.

Caution: *You can very quickly, very easily, and with no warning render a computer (or all of your computers!) completely inoperable using this program. Always double-check your entries before clicking the run button. Any damage you do to any machine is completely and totally your responsibility!*

2. Features

- Zero client configuration.
- Works equally well over the Intranet and Internet.
- "Retry Log" maintains log of failed changes. One click to retry the failed changes.
- Remotely manage registry security and auditing for groups of computers.
- User definable dynamic Substitutions.
- Using Substitutions, extensive reporting capabilities, including saving a list of remote registry values to a file in .CSV format.
- Change user rights.
- Use Alternate Credentials to run any operation as any user.
- Limit the available operations by machine and/or by user to prevent inexperienced users from causing problems.
- Drag-and-Drop keys and values.
- Registry Browser to quickly find keys and values on any computer. Supports Drag-and-Drop to copy keys and values – even between machines.
- Startup parameters allow you to run the program in batch mode or scheduled from the Task Scheduler.
- Quick Entry lets you easily build and save a library of frequently used operations. Less typing means fewer errors.
- Verify the existence of a key and/or value.
- Delete keys (including subkeys) or values.
- The option to change the remote registry for all users of a remote machine – logged on or not.
- Create a simple TAB delimited file to apply many changes to many computers. Includes a method for creating these files with ease.
- Quick Copy a key and all subkeys from one computer to many others.
- Export keys, subkeys and values to .REG file format.
- Apply all changes from .REG files to many computers very quickly.
- User initiated automatic updates let you check for program updates without visiting a web site.
- Shutdown remote systems or groups of remote systems.
- Save logs of Operation Successes, Operation Failures and Failures to Connect and then reselect computers based on these logs.
- Change Service User Information
- Send pop-up messages to your users based upon which machine they are logged in to.
- Multi-Threaded – do many of these operations at once with each operation having multiple threads (two to hundreds)!
- Fast, Fast, Fast! Change literally tens of thousands of keys/values per minute.

3. *System Requirements*

- Microsoft Windows NT® Version 4 or greater, including Windows 2000, Windows XP and Windows Server 2003.
- Works with any O/S option: Workstation, Server or Advanced Server.
- 5 MB Hard Disk Space
- For maximum functionality, user must be a member of the Administrators group on the remote computer or Domain Admins group if the remote computer is part of a domain.

4. General Instructions

The general operation of the program is simple: Select computers from the list, select the operation, fill in the blanks and click RUN!

The first operation on any remote computer can take several seconds. Future operations (during the same session) on the same computer(s) will be *much* faster.

Note: The right-click or context menu is used *extensively* in the program. Many options are available only on the context menu.

Registry terms and instructions as used in this program:

Each registry entry consists of a hive, a key, and zero or more values. Values are in the format "Value Name", "Value Type" and "Value".

Hives:

This program can operate on all remote hives:

HKEY_LOCAL_MACHINE,
HKEY_USERS,
HKEY_CURRENT_USER,
HKEY_CURRENT_CONFIG,
HKEY_CLASSES_ROOT,
and a dual function special option: *EVERY_USER*.

Hives other than HKEY_LOCAL_MACHINE and HKEY_USERS are automatically mapped to their real location in the registry. All hives other than HKEY_LOCAL_MACHINE and HKEY_USERS are in fact subkeys of these two. The other hives that are generally available in REGEDIT and REGEDT32 are located as shown:

HKEY_CURRENT_USER Because Windows NT/2000/XP/2003 can have many "Current Users" (services that logon locally, Terminal Server Clients, etc), Multi-Remote Registry Change uses a complex algorithm to attempt to discover the correct current user of the attached terminal on the remote machine. If it believes it has successfully discovered the correct user, it will map HKEY_CURRENT_USER to the correct S-1* entry under HKEY_USERS.

HKEY_CURRENT_CONFIG is
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Hardware\Profiles\Current

HKEY_CLASSES_ROOT is HKEY_LOCAL_MACHINE\Software\Classes

The "key" is the full path of the entry. For example, the location of the AutoAdminLogon setting is:

Hive: HKEY_LOCAL_MACHINE
Key: \Software\Microsoft\Windows NT\Current Version\WinLogon
Value Name: AutoAdminLogon
ValueType: REG_SZ
Value: 1 (enable autologon) or 0 (disable autologon)

In this case, the key is: \Software\Microsoft\Windows NT\Current Version\WinLogon

The Value Name is a text identifier for the value, or blank for <default>.

Note: When using the **Single Key** or '**Apply from File**' operations, an asterisk (*) in the **Key Path** will be expanded to include all values represented by the asterisk. For example, if you want to change the Screen Saver to sspipes.scr for every user, you would normally have to use regedt32 to manually click through the unique login identifiers (ex. S-1-5-21-47866669-18273647284-182742842194-1837) but with Multi-Remote Registry Change, you would enter:

Hive: HKEY_USERS
Key Path: *\Control Panel\Desktop
Value Name: SCRNSAVE.EXE
Value Type: REG_SZ
Value: C:\Windows\SSPIPES.SCR

(You could also use *EVERY USER*, but this is just an example)

EVERY USER Where logical, *EVERY USER* is available as a **Hive**. Selecting *EVERY USER* causes the program to perform the selected operation on every user hive on each selected remote machine. If you use roaming profiles, or have many people that share a single machine in shifts, this will allow you to run the operation once and be assured of actually changing the HKEY_CURRENT_USER profile for every user, not just those that happen to be logged in at the time.

Values:

Depending on the option, the value type is one of the following:

REG_SZ
REG_DWORD
REG_MULTI_SZ
REG_EXPAND_SZ
REG_BINARY
REG_LINK
REG_FULL_RESOURCE_DESCRIPTOR
REG_RESOURCE_REQUIREMENTS_LIST
REG_QWORD
REG_NONE

DELETE KEY

DELETE VALUE

ADD TO VALUE-START

ADD TO VALUE-END

REMOVE FROM VALUE

Values are entered as follows, or may be dragged/dropped from the **Registry Browser**:

REG_SZ: Enter the text directly in the **Value** box.

REG_DWORD: Enter the integer number directly in the **Value** box. Alternatively, to enter the value as hex, enter the hex value preceded by a '\$'. For example, to enter the hex value 0x4AD39F enter \$4AD39F

REG_MULTI_SZ: Enter the values separated by a semicolon. For example Item1;Item2;Item Number 3;Item 4 is next;Item 5 ...

REG_EXPAND_SZ: Enter the item directly in the **Value** box. Programs that read values of type REG_EXPAND_SZ expect to find a system variable as part of the value, for example %WINDIR%\System32.

REG_BINARY,
REG_LINK,
REG_FULL_RESOURCE_DESCRIPTOR,
REG_RESOURCE_REQUIREMENTS_LIST,
REG_QWORD,

REG_NONE: May be entered as a string of hex values. Each hex value must consist of exactly two characters, and may be separated by a comma. The best way to accomplish this is to find the value in the

Registry Browser and drag and drop the value onto the form. It will automatically decode the binary value in the registry into a string of hex values. You may also use the String Conversion Tool to create your hex string from a regular string.

***DELETE_KEY*:** Enter the Hive and the Key. The key entered and all subkeys will be deleted.

***DELETE_VALUE*:** Enter Hive, Key and Value Name to delete this value from the registry.

***ADD TO VALUE-START*:** Enter Hive, Key, Value Name and the exact text to add to the beginning of the text already in the registry.

***ADD TO VALUE-END*:** Enter Hive, Key, Value Name and the exact text to add to the end of the text already in the registry.

***REMOVE FROM VALUE*:** Enter Hive, Key, Value Name and the exact text to match and remove from the registry

The ***ADD TO VALUE START***, ***ADD TO VALUE END*** and ***REMOVE FROM VALUE*** options are handy for values that contain things like paths or other delimited strings. If you use one of the Add to Value or Remove from Value options, please remember to include whatever delimiter the reading program(s) expect. For example, if it expects a list of semicolon separated strings like this C:\;C:\Windows;C:\Windows\System and you want to remove the C:\Windows entry, make sure you enter it as C:\Windows; so the value doesn't end up with two consecutive delimiters.

Note: For those forms with a small picture of a mouse in the upper right hand corner of the screen, you can click and drag the values from the selected form to any other form that accepts dropped keys/values. To use this functionality, fill in the blanks normally, then click and drag the picture of the mouse to add these values to another form.

5. The Main Window

The main window consists of the Computer Names list, the Operations tabs area, the Status Display Area, and the Status Bar.

Computer Names List

The Computer Names list is a persistent list of the computers in your organization. In the demo version, this list can contain a maximum of 10 computer names. When you purchase the program, the limit will be the number of computer names you purchase.

The list is divided into three columns, the Computer Name (or NetBIOS name), the FQDN or DNS Name and the IP address. The columns can be rearranged by dragging the column header to the desired location. To sort the list, click on the column header of the column to be sorted.

Computer Names can be added to the list by searching the network using *Edit-Search Network* or by importing items (Computer Names, IP Addresses or FQDN), one per line, using *Edit-Import Computer Names*. When new names are placed in the list, only one of the columns will be filled in. The next time you start the program, it will attempt to fill in the remaining columns with the correct information. To force the program to fill in the remaining columns without restarting, choose *Operations-Lookup Missing Grid Info*. Items can also be edited in place by clicking an item to select it, waiting a second or so and then clicking again to activate the in-place editor. When editing is complete, click away from the edited item to save changes.

To expand the view to show more information, select *Edit-Expand Window*.

The Computer Names list will remember your selections from session to session, and has options to temporarily remember a set of selections and to save and restore selections from permanent groups.

To delete items from the list, highlight the ones you want to delete, right-click and choose Delete Selection. You can multi-select items in the list using CTRL -Click to select individual items and SHIFT-click to select consecutive items. Also, selecting an item then holding down SHIFT and using the arrows will extend the selection up or down. To select the entire computer names list, click on the first, hold the SHIFT key and press the End key.

Operations Tabs Area

To the right of the Computer Names list is the Operations tabs area. Most new operations will show up here as a tab. If you need to monitor several operations at once, you can drag the tabs off of the area by clicking on the tab and dragging them off of the main window. When not docked with the main window, the operations tabs become standard windows.

By default, the program will automatically save the tab layout on exit and restore it the next time the program starts. You also have the option to arrange the tabs as you prefer, and have the program automatically restore your preferred layout at startup. To do this:

1. Open the operations windows for the operations you use most.
2. Drag all tabs off the main window except the one you wish to show as the first tab.
3. Drag your preferred windows back onto the main window in the order you wish to have them displayed.
4. When you have the tabs arranged as you prefer (Make sure the tab you wish to have displayed first is selected and active), select *Options-Save Tab Settings Now*.
5. To keep these new saved settings from being overwritten on exit, also make sure *Options-Always Update Tab Settings on Exit* is NOT checked.

Double clicking on the status bar of any operation will show dynamically updated windows with both the computers on which the operation has failed, as well as those on which the operation is still active. This is very useful in quickly determining which computers the operation failed on, as well as those the program is waiting on to finish.

Status Display Area

The status area displays the status of all active operations. You can save the status log to a file by selecting *File-Save Log to File* or clear the log with *File-Clear Log*. By default, the log will be saved in the <Data File Location> \Logs\ with a name beginning with the current date and time, followed by the text 'Registry Update.log'.

By default, everything logged in the Status Display area is saved to a file. To view this file, select *Options-Open Default Log File Folder* and then locate and open the "StatLogHistory.txt" file.

To allow time for inspection during active operations the status display may be paused by clicking on the Status Bar (see below).

Status Bar

The status bar at the bottom of the window shows: a) the number of computers in the Computer Names list; b) the number of computers currently selected; c) the number of worker threads currently active (you will not be able to exit the program if there are active worker threads); d) the status of logging in the status display area. Click on the status bar to toggle logging active and paused.

Data File Location

The default location of the data files that Multi-Remote Registry Change creates and maintains is in the sub-directory \Multi-Remote Registry Change\4.x under the value specified in the registry in the key:

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
Value Name: AppData

If you would prefer to have your data files maintained elsewhere, you may specify a different default path by entering a new location in the Key:

Hive: HKEY_CURRENT_USER
Key: \Software\Eytcheson\Multi-Remote Registry Change\4.x\Options
Value Name: User File Path
Value Type: REG_SZ
Value: (Full path to the new default location)

5.a Logging

The Logging form offers the option to log or not log the status of each operation in a standard delimited text file of your choice. You may choose the delimiter to use by selecting *Options-Set Log Delimiter*. Possible Options are COMMA, TAB, or SPACE. If you choose COMMA for the log delimiter, the program formats the log in a standard Comma Separated Value (.CSV) formatted file that you can open in Excel or nearly any spreadsheet or database. The default is TAB because it is easier to read in a standard text file. You can view or clear (delete) the log file with the option buttons for each log.

The 'On Failure to Connect' log will log any failure to connect to the indicated file. Failure to connect normally only happens when the computer is not powered on and/or attached to the network.

The 'On Operation Failure' log is used to indicate a key or value could not be changed for some reason. This could be because the computer is not

powered on or refused to accept your authority, or, in the case of changing user rights, the user you are trying to assign the rights to does not exist.

The 'On Operation Success' log keeps track of all operations that complete successfully.

The log files created with the logging tab can be used to reselect computers. Choose *Edit-Select from Log File* then choose the name of the log file. All computers in the log will be selected.

5.b Retry Log

The Retry Log maintains a log of all failed operations along with all information required to try the operation(s) again with a couple of mouse clicks. You do not need to be concerned with which machines an operation failed on as long as you regularly process the retry log. See the section on processing the retry log from the command line for information on processing these changes.

By default, the program saves the retry log in the same location as log files as part of the user profile. This allows multiple administrators to use the same machine without accidentally applying other administrators' changes. The retry log has different error types corresponding to the various types of operations supported by Multi-Remote Registry Change.

When a Retry Log item is sent to the appropriate thread manager to be processed, its record is marked as deleted. If processing fails, a new record will be created.

For errors that use a .REG file, the program will create a copy of the .REG file and save it in the \<Data File Location>\REGFILES subdirectory. The filename will be recorded in the Key Path column of the Retry Log. If there are no REGEDIT4 File Errors in the Retry Log, it is safe to delete the \REGFILES subdirectory.

For Registry Security errors, the program will create a copy of the .SEC file and save it in the \<Data File Location>\SECFILES subdirectory. The file name will be recorded in the Key Path column of the Retry Log. If there are no Registry Security File Errors in the Retry Log, it is safe to delete the \SECFILES subdirectory.

Many operations support **right** clicking on the Run button for the operation to add an entry to the Retry Log for each selected computer, just as if you had attempted to run the operation and all selected computers were unavailable.

From either the Edit Menu or the Right-Click Context Menu, you have the option to:

- **Toggle Deleted:** Toggles the selected record(s) deleted status. Records with a deleted status will not be processed. They will remain in the display until the program is closed or they are removed using the Remove Deleted option.
- **Remove Deleted:** Removes all records marked as deleted. When a deleted record is removed, either as a result of selecting Remove Deleted, or when the program is closed, associated .REG or .SEC files will also be deleted.
- **Clear All Entries:** Removes all Retries (and their associated .REG or .SEC file if one exists).

5.c Advanced Selections

The Advanced Selections dialog (*Edit-Advanced Selections* or shortcut CTRL-ALT-S) provides a way to select computers in the computer names list by their role or their operating system version. Selecting computers by role is very fast because role information is stored in the master browsers browse list. Selecting by operating system is much slower since each machine must be queried individually about its operating system version. These options are not exclusive. For example, by using both the Roles and the OS Version tabs you can choose to select all of the Windows Server 2003 machines that are also SQL Servers.

Note: *To quickly select all of the computers in the computer names list that are currently active on your network, open the Advanced Selections dialog and click Find without selecting a role or OS version.*

6. Operations

Note on disabling operations

It is possible to disable any and/or all Multi-Remote Registry Change operation(s) by creating registry entries. This is useful if you have administrators that require the read-only functions such as Query using Substitutions or Check for Key or Value, or if you wish to limit Multi-Remote Registry Change use across your domain.

To limit use of Multi-Remote Registry Change, use the file included with the installation of the program named “disableoperations.reg” and update the values with “00000001” for the items you wish to disable.

There is an option to allow override in HKCU to allow you to disable the use of Multi-Remote Registry Change on your computers for all except certain users. To use this option, set the value “Allow Override in HKCU” to 00000001 and override the entries using the same method with the second set of entries in the “disableoperations.reg” file.

6.a Change Single Key

The Single Key form is used to change a single key on many computers. Simply select the computers you want to change, complete each entry as shown in the General instructions above and click run. To stop before the action completes, click the *Stop* button (it may take several seconds or even minutes for the stop operation to complete.)

For example, to remove a service from selected computers you would enter:

Hive: HKEY_LOCAL_MACHINE
Key: \SYSTEM\CurrentControlSet\Services\ServiceName
Value Name: DeleteFlag
Value Type: REG_SZ
Value: 1
(Also Select *Ignore Entry*)

The Create Key/Ignore Entry option allows you to choose to create a value only if the key already exists. If you select Create Key, the Key and/or Value will always be created. If you select Ignore Entry, the Value will be entered only if the Key exists

6.b Change Many Keys (Key Group)

The Key Group tab is used to copy a key and all subkeys from a source computer to the selected computers. The key can be copied to the same location on the remote computer as on the source, or to any other location. If you select *Delete Destination Key Before Copying*, the program will delete any key at the destination before copying in the new one.

For example, to copy the Office XP settings from computer COMPNAME to several others, you would enter:

Source Computer:	COMPNAME
Source Hive:	HKEY_LOCAL_MACHINE
Source Key:	\SOFTWARE\Microsoft\Office\10.0
Destination Hive:	*SAME AS SOURCE*
Destination Key:	*SAME AS SOURCE*

If you wanted to place these settings in a different location (to back them up for example) you could use:

Source Computer:	COMPNAME
Source Hive:	HKEY_LOCAL_MACHINE
Source Key:	\SOFTWARE\Microsoft\Office\10.0
Destination Hive:	HKEY_LOCAL_MACHINE
Destination Key:	\SOFTWARE\Backup\Microsoft\Office\10.0

6.c Check for Key

The Check for Key window allows you to query the registry on remote computers to confirm the existence of a key or value. The existence or non-existence will be logged or ignored based on the selections you make. If you do not select Ignore Value, you will be asked if you would like to save the actual values to a file. If you choose "Yes", you will be prompted for a filename for the actual values to be saved in. When the operation is complete, the file will be automatically displayed.

6.d Shutdown Systems

Shutdown or abort shutdown on selected computers. Options include: a) send a shutdown message; b) select the shutdown timeout; c) choose to force applications to close; d) Force the computer to reboot after shutdown.

If you begin a shutdown and later change your mind, you have the option

to abort a shutdown in progress. This has no effect on a computer that is not shutting down.

Note: The cancel button will stop the current operation only. It will not issue an Abort Shutdown to a computer that has already accepted shutdown; you must use the Abort button for this.

6.e REG File Operations

One of the more powerful features of Multi-Remote Registry Change is its ability to create and use standard REGEDIT4 formatted files.

With this you can:

1. Create a REGEDIT4 formatted file from the local computer or a remote computer. The file will include all keys, subkeys and values from the selected key of the source computer.

Instructions: Type in the name of the source computer in the 'Source Computer' box. Select the Root Key. Enter the Key Path to examine. For example: '\Software\Microsoft\Windows'. Then select *Edit - Create from Computer*. (Depending on the size of the key, the window may appear to freeze for several seconds—or minutes.)

2. Apply changes from any REGEDIT4 formatted file - including those created with REGEDIT.EXE - to selected computers on the network.

Instructions: Choose *File - Load* from the menu. This will load the selected file into the window. You may edit it or make changes to the destination key (see below) before applying it to the selected computers.

3. Make a change in destination root key and/or key path. This will allow you to "copy" a key from one area of the registry to another.

Instructions: To make the changes at the time the file is created, simply follow the instructions in step one, but before selecting "Create From Computer" check the "Change Destination" box and enter the changes you would like made.

To change a file after it is loaded, in the 'Source Computer' area, select the Root Key and Key Path as they are currently displayed in the file. Check the "Change Destination" box and enter the changes.

For Example, you create an export file with REGEDIT.EXE exporting the key:

[HKEY_USERS\DEFAULT\Software\Eytcheson]

and want to place it on remote computers as:

[HKEY_LOCAL_MACHINE\Software\SomethingElse]

You would select HKEY_USERS in the Source Root Key box, and enter \DEFAULT\Software\Eytcheson in the Source Root Path. Then, check the "Change Destination" box, select HKEY_LOCAL_MACHINE in the Destination Root Key and enter \Software\SomethingElse in the Destination Path.

After you have made your selections, select *Edit - Change Destination* from the menu.

4. Apply the changes from the window to all selected computers.

Instructions: When the text in the right window is exactly what you want to insert into the registry of the remote computers, Select *Apply - Apply to Selected Computers*.

6.f Lookup IP Addresses

The Lookup IP Addresses menu option will query the DNS, WINS or the selected computer to attempt to find its IP Address. The IP Address will be added to the Computer Names list. The reason for this is simple: After the IP Address is added to the Computer Names list, you can use Group Select and Group Deselect to select all (or none) of the computers within a specific range.

6.g Change User Rights

One of the most annoying things about Windows NT's default user rights was that you cannot set the system time from a user's login script. Changing this was a manual process that took lots of time and clicking. With Multi-Remote Registry Change you can quickly grant or revoke any of the user rights available in User Manager.

This feature is also handy in a classroom environment where you would like instructors to be able to remotely shutdown all of the computers in a computer lab at the end of the day.

For example, to grant ProfessorA the authority to shutdown all of the

computers in Computer Lab 9 you would select all of the computers in Lab 9 from the Computer Names List then select *Edit-Change User Rights* and enter:

User Domain or PDC Name:	*AUTO*
User or Group Name:	ProfessorA
Right to Grant/Revoke:	Force shutdown from a remote system
Grant/Revoke:	Grant

And click Run. Revoking the right is as simple as repeating the steps above but selecting Revoke instead of Grant in the Grant/Revoke box.

When entering the User Domain PDC Name, you can use the default *AUTO*, which will attempt to locate the user account by first searching the Primary Domain Controller (PDC) to which you are attached, then the PDC's in all trusted domains.

If you choose to enter the PDC name for the user, be sure to preface it with "\\". This will inform the program that you want it to only search the PDC entered.

The User or Group Name can be any valid User or Group Name on your domain or any trusted domain.

6.h Apply from File

When you need to change several keys on remote computers, instead of changing them one at a time, you can create a file containing the keys and values to be added or changed and use this file as a sort of script. The script file must be plain text; TAB delimited with the following format:

Hive<TAB>Key Path<TAB>Value Name<TAB>Value Type<TAB>Value

(An example file called import.txt is included in the application installation directory)

To change the default value (listed as <No Name> in REGEDT32) use a '@' for the Value Name.

The script file accepts all Value Types as shown in the General Instructions, including *DELETE KEY* and *DELETE VALUE*. It also accepts an asterisk in the Key Path as indicated in the General Instructions. Value Name and Value may be blank, but the TABs must be maintained. For example, to delete a key:

Hive<TAB>Key Path<TAB><TAB>*DELETE KEY*<TAB>

You can have as many entries in this file as you wish, but it will process a little faster if you keep like HIVE's together (ex: all HKEY_LOCAL_MACHINE then all HKEY_USERS.)

Any line in the file that does not begin with "HKEY_" or "*EVERY_USER*" is considered a comment and will be ignored.

To make it simple to create these import files, the menu option *Edit>Create 'Apply from File'* will show a dialog where you may enter the keys into a file and know the format is correct. The keys are entered exactly as you would enter them in the Single Key form. After making the changes to the selections on the left, click Add to insert the line into the file. When you are done, assign the file a name in the box at the top and click save.

6.i Create "Call" Batch File

Batch files provide an amazingly powerful way to administer remote Windows NT computers.

The solution provided here relies on two batch files. One created by this program, the other created by you. The program will create a batch file with the following format:

CALLCOMP.CMD

```
CALL %1 COMPUTER1 <OPTIONAL PARAMS>
CALL %1 COMPUTER2 <OPTIONAL PARAMS>
CALL %1 COMPUTER3 <OPTIONAL PARAMS>
CALL %1 COMPUTER4 <OPTIONAL PARAMS>
CALL %1 COMPUTER5 <OPTIONAL PARAMS>
...
```

Used in conjunction with another batch file, you can easily create directories and copy files. If you have the Windows NT Resource Kit, you can use its command line utilities to set file/directory rights and security as well as a host of other uses.

The second batch file can contain any valid Windows NT command line that is capable of supporting remote computers. An example of a batch file to copy files from your computer to another is:

CPYFILES.CMD

```
MD \\%1\C$\NEWDIR
COPY C:\MYDIR\*. * \\%1\C$\NEWDIR
```

To activate these batch files, on a command line you would enter:

```
CALLCOMP CPYFILES.CMD
```

For each entry in CALLCOMP.CMD, CPYFILES.CMD would be called receiving its parameters from CALLCOMP.CMD.

6.j Registry Security

Multi-Remote Registry Change includes a very powerful means for manipulating registry security. More than any other feature of the program, this option, if used incorrectly, has the potential to render your computers unusable. This functionality is intended for experienced NT administrators with a firm grasp of the specifics of NT security. There are many excellent references available if you need more information about NT Security.

Acronyms used in this section:

ACE: Access Control Entry

ACL: Access Control List. Consists of 0 or more Access Control Entries (ACE).

Registry Security Actions List

Registry Security Action items are added to the list by choosing Edit-Add or by clicking on the add button on the tool bar.

Each Registry Security Action item consists of:

- a) One or more user and/or group names.
- b) A set of one or more permissions.
- c) A set of zero or more ACE flags.
- d) An action type (Allow, Deny or Audit).
- e) A Remove/Revoke flag.
- f) An Apply to Subkeys flag.
- g) A Take Ownership flag.

Each of these is explained in more detail in the section “Registry Security Detail Dialog” below.

Actions are applied in the order they are listed to the registries of selected computers. To adjust the order of the items in the list, select the item you wish to move, and click the up or down arrow button on the toolbar.

Editing an item causes it to be temporarily removed from the list. It will be added back to the end of the list when changes are complete or canceled.

Registry Security Detail Dialog

User/Group Name:

Enter the User and or Group names separated by semi-colons. If necessary, preface the user/group name with the domain name. For example, to indicate the group Everyone in domain ABCCorp, enter as: “ABCCorp\Everyone”

Permissions Dropdown List:

Provides a quick way to select the most common types of access. If you wish to provide a set of permissions other than the common Read or Full Control, select Special Access and then set the specific permissions you need in the Individual Permissions box.

Type of Access

Access Allowed:

Adds (or removes if Revoke/Remove is checked) an ACE to the Access Allowed ACL for each listed user or group.

Access Denied:

Adds (or removes if Revoke/Remove is checked) an ACE to the Access Denied ACL for each listed user or group. Access Denied has higher priority than Access Allowed, therefore, a user denied Full Control in the Access Denied ACL, and allowed Full Control in the Access Allowed ACL would not be able to access the key.

Please note, Windows NT's version of REGEDT32.EXE cannot edit security on keys that contain an Access Denied ACL. This does not mean the OS will not enforce the

security, only that you cannot change the security settings later using REGEDT32.EXE. The version of REGEDT32 in Windows 2000 and Windows XP does not have this limitation.

Audit Access:

Adds (or removes if Revoke/Remove is checked) an ACE to the Audit Access ACL for each listed user or group. Depending on the type of Audit Access entry added, Audit Access entries cause an entry to be made in the event log whenever the key is successfully accessed, or when an attempt to access the key fails. See Security Object Inheritance below.

Permissions

Query Value: Permission to query the value

Set Value: Permission to change the value

Create Subkey: Permission to create subkeys

Enumerate Subkeys: Permission to enumerate (list) subkeys

Notify: Permission to audit the notification events

Create Link: Permission to create a symbolic link in a particular key

Delete: Permission to delete the key

Write DAC: Permission to gain access to a key for the purpose of writing to the discretionary access control list

Write Owner: Permission to take ownership of the key

Read Control: Permission to gain access to the security information for the selected key.

Full Control: All of the above.

Security Object Inheritance

Container Inherit: Container objects, such as Registry Keys inherit

the access item object.

Inherit Only: The access item object does not apply to the container object, but to objects contained by it.

Object Inherit: The access item object is inherited by non container objects, such as values created within the key to which the access item object is assigned.

No Propagate: The Object Inherit and Container Inherit flags are not propagated to inherited access control entries.

Success Audit: Used with access items that belong to System Audit list to indicate a message is generated for successful access attempts.

Fail Audit: Used with access items that belong to System Audit list to indicate a message is generated for failed access attempts.

6.k Browse Registry

Browsing the registry is the easiest way to find the key you wish to change. Double clicking on a computer name in the Computer Names list will open a Registry Browser window. To view the registry of more than one computer at a time, simply double-click on another computer name.

The Registry Browser is a (mostly) view only clone of the ones installed by default with Windows called REGEDIT.

The majority of Multi-Remote Registry Change operations windows will accept keys and/or values dropped from the Registry Browser to fill in the blanks on the operations forms. Simply SHIFT-Click and drag the key or value onto the desired operation form.

Another advantage with the registry browser included with Multi-Remote Registry Change, is that you can drag-and-drop keys and values in the same browser window or between different browser windows, and different computers.

Since it is so easy to copy keys from one computer to another (and possibly render the target computer inoperable in the process), the drag-and-drop functionality in Multi-Remote Registry Change is implemented a little differently. For all drag-and-drop operations, you must **SHIFT-click** and drag the key or value you wish to drag-and-drop.

6.l Send Message

This option will send your message to all selected computers. The message will be displayed on the remote machine as popup dialog box containing the message, just as if you had issued a "NET SEND" from the command line.

6.m Change Service User Info

Each Service entry on a Windows NT computer must either use the System Account or have a valid Windows NT account (username/password) associated with it. In the event that the account information used for this service must be changed, the username/password on for the service must also be changed.

On the Change Service User Info form, you have the option to change the service username, the service password or both.

The Change Service User Info form contains the following:

Change for All Services: Applies the changes to the password for all services with the user name specified below. The Service Name is ignored. For example, if you are using Microsoft Exchange Server and have the Exchange services running as "ExchangeServiceAccount", to change the service start password for the service (make sure you change the actual password for the actual account too!), checkmark Change for All Services, enter the Service User Name as ExchangeServiceAccount and then enter the new password in both password boxes and click Run.

Service Name: Enter the service name as it appears in the services Control Panel. Click the button with the ellipses next to the entry box to browse for a service on the local or a remote computer.

Change Service User Name check box: If the username for the service must be changed, select this box and enter a new username for the service. Click the button with the ellipses next to the entry box to browse for a service on the local or a remote computer.

Note: This should not be the name of a group. If you enter the name of a group in the box, the program will quite happily make the change for you, but it is a good bet the service will not work properly.

Change Service Password check box: If the password for the service must be changed, select this box and enter the new password for the service in each of the following boxes. *Note: passwords are case sensitive.*

Attempting to change service user information for a service that does not exist on the remote computer will not result in any error; the attempt will simply be ignored.

For security reasons, operations of this type are not entered into the Retry Log when they fail.

6.n Search and Replace

The Search and Replace function is NOT designed to do a full search and replace across a Hive or even a large key. It should work, but it will be anything but fast.

You have the option to:

- a) Check only Data (Value)
- b) Check only Key Names
- c) Check only Value Names
- d) Make the search Case Sensitive
- e) Any combination of the above.

Once again: this is NOT intended to be a full scale, cross-hive search and replace.

6.o Insert into REG_MULTI_SZ

REG_MULTI_SZ values are stored as a series of NULL terminated strings. With the REG_MULTI_SZ functionality in Multi-Remote Registry Change, you can manipulate this series of NULL terminated strings by adding and removing items from the list, as well as sorting and reverse sorting the series.

6.p Dump Key to .REG File

This operation allows you to select computers and create individual .REG files for a key/subkeys, or to create a single file with the REGEDIT4 entries for all selected computers. The "One Per Computer" option will create a separate REGEDIT4 file for each selected computer in the selected directory named as ComputerName.REG for non-user hives, and

ComputerName-UserName.REG for HKEY_CURRENT_USER hives. If "Single File" is selected, the REGEDIT4 entries for each computer will be saved one after the other into the selected file in the order that they complete. The entries will be separated by a line containing the computer name (ex: // EYTCHNT). For user hives, the entries will be separated by a line containing the computer name and the username (ex: // EYTCHNT User: greg).

6.q Manage Services

Used to Start or Stop, Change the Startup type or Delete Services. Enter or select the service to control and then select from the available options.

7. *Substitutions*

Substitutions are the most unique and powerful part of Multi-Remote Registry Change. Things that are usually impossible without hiring a programmer are simple to accomplish using Substitutions. Using a simple form, you can set-up a virtually unlimited number of substitution items. Substitutions work by dynamically querying the registry of the target computer or an INI file and replacing the text you enter with the value contained at the specified location.

A Registry Substitution item consists of:

Substitution Name: Any text, of any length, used to uniquely identify the substitution.

Substitution Location: The Hive, Key Name and Value Name of the value to be retrieved.

An INIFILE Substitution item consists of:

Substitution Name: Any text, of any length, used to uniquely identify the substitution.

File name: The name of the file containing the INI File substitution items.

Section: The section in the INI file that pertains to this specific substitution.

The Substitution INI file is a standard Windows INI file and is therefore limited by Windows to the maximum INI file size of 32KB. You may use as many different INI files as required, but not more than one file per substitution item. You may have more than one substitution item in each file as long as the file size does not exceed 32KB.

The items under the section are represented as name=value pairs where the name is the computer name and the value is the text you wish the replacement text to be replaced with.

When you use the Multi-Remote Registry Change “Create New INI File” button to create the new INI file, it will ask for the section name and the name of the file to create. When provided, it will create a new file with a new section and a list containing all selected computer names, as well as two special named entries which are

commented out by default:

ALL=Replace this text with the entry you wish to be applied to ALL computers -- Ignoring the computer name entry below

DEFAULT=Replace this text with the entry you wish to be applied to computers with no entry below

To use the special entries you must remove the semicolon from the beginning of the line in the INI file.

The remaining items will be the computer names, formatted as in this example:

```
LAB2XP01=
LAB2XP02=
LAB2XP03=
LAB2XP04=
LAB2XP05=
```

Make changes to the file as necessary to provide unique entries for the computers that require them. For example:

```
;*ALL*=
*DEFAULT*=Standard Computer Configuration
LAB2XP01=
LAB2XP02=
LAB2XP03=This is Lab2XP Machine number 3
LAB2XP04= WinXP/P3-933/512MB RAM
LAB2XP05=
```

Once you have defined a Substitution Item, you may enter the Substitution Name anywhere in any of the operations. The Substitution Name **is case sensitive**, and must be surrounded by the Substitution Delimiter you choose, the default is the ampersand (&).

A few facts about Substitutions

- A substitution can point to any type of value, even binary values.
- Substitutions are recursive – you may use a substitution inside of another substitution, inside of another substitution...
- All operations support substitutions. Substitutions will work virtually any place you can enter text -- even in REGEDIT4 formatted files.

- Having large numbers of Substitution Items in the list has very little impact on performance.
- Static Substitutions are applied before User Substitutions.
- User Substitutions are applied in alphabetical order.
- To disable a Substitution, remove the check mark from its entry.
- By default, if any substitution fails on a remote machine (because the location it is trying to find is not available, or because there is no current user, etc), then the entire transaction for the remote machine is aborted. The exception to this is the “Run Query Using Substitutions” option below.
- For INI based substitutions, there is no limit to the number of INI files you can use, but the limit to the size of each file is 32KB (as imposed by Windows). You may have multiple sections within a single INI file as long as the file size remains within this limitation.
- You may mix and match registry based and INI File based substitutions at will, even as parts of each other.

Now that those basics are out of the way, the best way to explain this is by example:

Example 1: Change the logon banner to display your company specific text along with the computer name.

1. Open the Substitutions dialog by selecting *Substitutions – View/Change Substitutions* from the main window.
2. Enter “computername” in the box labeled ‘Replace this text’
3. Select HKEY_LOCAL_MACHINE for the Hive
4. Enter “\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName” in the box labeled ‘Key Path’
5. Enter “ComputerName” in the box labeled ‘Value Name’
6. Click the ‘Add/Update’ button.

The Substitution Entry is now complete

Now to apply the text to all selected machines:

1. Select the Single Key Operation.
2. Hive: HKEY_LOCAL_MACHINE
3. Key: \Software\Microsoft\Windows NT\CurrentVersion\Winlogon
4. Value Name: LegalNoticeText
5. Value Type: REG_SZ
6. Value: You are logging on to Biggie Corp Computer: &computername&
7. Click run to apply to all selected machines.

Now, for example, the user logging on to computer “THOR” will see: “You are logging on to Biggie Corp Computer: THOR”

Example 2: Change the default TCP/IP gateway.

Because the TCP/IP parameters are stored as part of the network card parameters, changing the default gateway for a set of computers can be quite a problem.

To start with, you need to know the name of the service of the primary network card:

1. Open the Substitutions dialog by selecting *Substitutions – View/Change Substitutions* from the main window.
2. Enter “PrimaryNetServiceName” in the box labeled ‘Replace this text’
3. Select HKEY_LOCAL_MACHINE for the Hive
4. Enter “\Software\Microsoft\Windows NT\CurrentVersion\NetworkCards\1” in the box labeled ‘Key Path’
5. Enter “ServiceName” in the box labeled ‘Value Name’
6. Click the ‘Add/Update’ button.

To change the Default Gateway:

1. Select the Single Key Operation.
2. Hive: HKEY_LOCAL_MACHINE
3. Key:
 \SYSTEM\CurrentControlSet\Services\&PrimaryNetServiceName&\Parameters\TCP
 P
4. Value Name: DefaultGateway
5. Value Type: REG_MULTI_SZ
6. Value: 123.234.235.1
7. Click run to apply to all selected machines.

Example 3: Backup a value before changing it.

For obvious reasons, sometimes it is imperative that you be able to create a backup of a key before you change it. This example illustrates using a Substitution within a Substitution, and assumes you have created the Substitution in Example 2. To backup a value before changing it:

For example, to backup the TCP/IP address before changing it:

1. Open the Substitutions dialog by selecting *Substitutions – View/Change Substitutions* from the main window.
2. Enter “OldIP” in the box labeled ‘Replace this text’
3. Select HKEY_LOCAL_MACHINE for the Hive
4. Enter :
 \SYSTEM\CurrentControlSet\Services\&PrimaryNetServiceName&\Parameters\TCP
 P in the box labeled ‘Key Path’
5. Enter “IPAddress” in the box labeled ‘Value Name’

6. Click the 'Add/Update' button.

To change the copy the old IP Address to another value:

1. Select the Single Key Operation.
2. Hive: HKEY_LOCAL_MACHINE
3. Key:
 \SYSTEM\CurrentControlSet\Services\&PrimaryNetServiceName\Parameters\TCPIP
4. Value Name: OldIPAddress
5. Value Type: REG_MULTI_SZ
6. Value: &OldIP&
7. Click run to apply to all selected machines.

Then, if the value must be restored, create a new substitution entry that points to the Value Named 'OldIPAddress'

1. Open the Substitutions dialog by selecting *Substitutions – View/Change Substitutions* from the main window.
2. Enter "RestoreIP" in the box labeled 'Replace this text'
3. Select HKEY_LOCAL_MACHINE for the Hive
4. Enter :
 \SYSTEM\CurrentControlSet\Services\&PrimaryNetServiceName\Parameters\TCPIP in the box labeled 'Key Path'
5. Enter "OldIPAddress" in the box labeled 'Value Name'
6. Click the 'Add/Update' button.

To restore the value to its original location:

1. Select the Single Key Operation.
2. Hive: HKEY_LOCAL_MACHINE
3. Key:
 \SYSTEM\CurrentControlSet\Services\&PrimaryNetServiceName\Parameters\TCPIP
4. Value Name: IPAddress
5. Value Type: REG_MULTI_SZ
6. Value: &RestoreIP&
7. Click run to apply to all selected machines.

Although the examples above use only the Single Key Operation, Substitutions work equally well in all operations.

Static Substitutions

For several items that are difficult or impossible to do reliably simply by querying the registry, Multi-Remote Registry Change includes pre-defined "Static Substitutions". Help for each Static Substitution is available by double clicking on the entry. If you have an idea for a static substitution not already included with the program, please forward it to

support@eytcheson.com. We cannot guarantee that every suggestion will be implemented, but we will do our best.

Run Query Using Substitutions

For the ultimate in reporting flexibility, Multi-Remote Registry Change includes the ability to do a free form query using Substitutions.

For example, to list the hard drive types for all of your computers, you can create the following four Substitution Items:

Replace This Text: **HardDisk0**
Hive: **HKEY_LOCAL_MACHINE**
Key Path: **\HARDWARE\DEVICEMAP\Scsi\Scsi Port 0\Scsi Bus 0\Target Id 0\Logical Unit Id 0**
Value Name: **Identifier**

Replace This Text: **HardDisk1**
Hive: **HKEY_LOCAL_MACHINE**
Key Path: **\HARDWARE\DEVICEMAP\Scsi\Scsi Port 0\Scsi Bus 0\Target Id 1\Logical Unit Id 0**
Value Name: **Identifier**

Replace This Text: **HardDisk2**
Hive: **HKEY_LOCAL_MACHINE**
Key Path: **\HARDWARE\DEVICEMAP\Scsi\Scsi Port 1\Scsi Bus 0\Target Id 0\Logical Unit Id 0**
Value Name: **Identifier**

Replace This Text: **HardDisk3**
Hive: **HKEY_LOCAL_MACHINE**
Key Path: **\HARDWARE\DEVICEMAP\Scsi\Scsi Port 1\Scsi Bus 0\Target Id 1\Logical Unit Id 0**
Value Name: **Identifier**

After these entries are created, select “Run Query Using Substitutions” from the Substitutions menu.

In the text box, enter your free form query (wrapped for readability only):

“On machine: &computername&, the current user is: &username&. The hard drives are: HD0 – &HardDisk0&, HD1 - &HardDisk1& , HD2 - &HardDisk2&, HD3 - &HardDisk3&”

This can easily be used to produce a Comma Separated Value (CSV) file for import into Excel or another program, simply enter the text in the box exactly as you wish it to be saved:

&computername&,&HardDisk1&,&HardDisk2&,&HardDisk3&,&UserName
&

Another example is just to list the current user on each selected machine. Simply enter &UserName& in the text box.

An example of the output of this is:

COMP1	CharlieH
COMP2	Ysmith
COMP3	HowardH
SERVER1	Administrator

8. Quick Entry

Quick Entry gives administrators a simple way to store operation entries for easy reuse.

To create a new Quick Entry item, complete an operation form as usual. When the operation form is filled with the entries that you wish to save, choose “*Quick Entry - Create Quick Entry*” from the main menu (or use the keyboard shortcut CTRL-ALT-Q). The Create Quick Entry dialog is displayed. In this dialog, you may enter a Category, Name and Description for the Quick Entry item as well as update any of the settings for the item in the Settings box. When the item is done, click Add.

To view or use a previously saved Quick Entry item, choose “*Quick Entry - View Quick Entry List*” from the main menu (keyboard shortcut: CTRL-Q). The list of previously created Quick Entry items will be displayed. To use an item, double-click on its entry in the list.

To sort the items in the list, click on the column header of the column to sort.

The Right-Click context menu is the primary means of interacting with the items in the Quick Entry list. From this menu you can Use or Delete the items.

Also available from context menu are the options for saving the current Quick Entry file and/or loading a different file, as well as the option to import new items from a different file.

To change a Quick Entry item's settings, it is necessary to double click on it to open its settings on its operation form, make the required changes and then save it as a new item. After it is saved you can delete the original item.

9. Tools

a. String Conversion:

The String Conversion tool converts to and from all of: Simple String, Binary String (0101010), and Hexadecimal strings simultaneously. This makes it easy to see exactly what all of those hex values in the REGEDIT4 files really say – just paste in the hex text and it appears as a string value in the top box.

b. SID <-> UserName

Have you ever wondered who or what that SID represents? Just enter the SID in the box and click the button. You can also find out what a user's SID is by entering their username in the top box. If the user's account is a domain account, preface the name with the domain name like this: CORP\USERNAME. If the username is local to a specific machine, enter the username in the Username box, and the name of the computer to search in the bottom box. If the user is on a different domain or Active Directory tree than your computer, make sure you include the computer name of a domain controller in their domain to run the query against. It doesn't work for every SID, but it does a pretty good job with most.

10. Options

In addition to the Logging Options, the Options Menu contains several items to allow you to customize the performance and operation of the program to meet your needs.

Use Alternate User Credentials: Specify an alternate account username and password under which to run operation threads. When this is selected, an explicit IPC\$ connection will be made with the supplied credentials to the remote computer(s) prior to the worker threads doing any work. The connection is maintained for a short period (default is 10 minutes) after the operation completes and then is explicitly removed. If another operation is required on a computer that already has a connection, that connection will be used and the timer reset. These explicit connections and disconnections incur a significant performance penalty within the program, but they allow you to run operations from user accounts which would not normally have the correct permissions to access all features of the remote registry/computer. After connections are explicitly removed, subsequent operations must incur the performance penalty of reconnecting.

For security reasons, the password for alternate credentials is not saved between sessions and must be re-entered each time the program is started.

Note: Because of the way Windows API's work, if the credentials you enter fail, the credentials of the account you are running the program under may be used to attempt the change.

Note: You can also run the entire program (instead of just each operation) under alternate credentials under Windows 2000/XP/2003 by creating a shortcut to the program, then right-clicking on the shortcut and navigating to the Shortcut tab, then selecting Advanced and check-marking "Run with Different Credentials". Each time you use this shortcut, Windows will prompt you for a username and password to run the program as. Using this option removes all of the performance penalties incurred by the Multi-Remote Registry Change Alternate User Credentials option.

Verbose Log Entries: Additional information will be entered in the log. The default is off.

Set Log Delimiter: The logs are formatted to make it easy to open them using a spreadsheet. If your spreadsheet requires a different delimiter, please select from COMMA, TAB or SPACE. The default is TAB.

Open Default Log File Folder: Opens the default log file location in

Windows Explorer.

Retry Log items: See section 5b for information on using the Retry Log

Retry Log Entry Warning Count: As the Retry Log grows, the action of inserting new items becomes more “expensive” in terms of computer performance. The setting allows you to set a threshold after which a warning will be displayed when the program is started. The default is 40,000.

Allow Connect Retries: Used on slow networks, it will attempt several times to connect to the remote computer. When this is NOT checked the timeout period when attempting to connect to remote computers is reduced by approximately two-thirds. The default is on. The recommended setting is off after confirming that it works correctly in your environment.

Save n Entries for Reuse: Allows you to determine how many of your prior entries are saved from session to session in the drop-down boxes. Set this number as high as you think might be useful. The default is eight.

Set Max Active Threads: Multi-Remote Registry Change is capable of managing a -very- large number of simultaneous threads. The number of threads that can run well on a given configuration depends on the speed of the computer, the speed of the network, and the operation being run. On a moderately fast (P-II/450 or greater) computer running the Single Key operation in a switched environment, 100 threads is a very reasonable number. The same computer running the Dump to Reg File operation would do better with 20 or fewer threads.

The default Max Active Threads for Windows NT/2000/XP is 50. The number can be changed to increase Max Active Threads while an operation is active, but you should never decrease the number while an *EVERY USER* operation is active. Because of the way the threads are allocated in *EVERY USER* operations, reducing the number during an active operation can cause a resource contention deadlock that may result in the program hanging. A confirmation dialog will be shown if you attempt to reduce the number of Max Active Threads while any operation is active.

EVERY USER Options: See the section on *EVERY USER* for more information.

Use Profile Paths for *EVERY USER*: If your organization uses Roaming Profiles, the Profile Paths option allows you to make changes to the roaming profiles of your users. There are a few simple steps to use Profile Paths:

1. Make sure the computer name of the computer you are using is in the computer names list.
2. Choose Options -> Use Profile Paths for *EVERY USER*
3. Choose Options -> *EVERY USER* Profile Paths
4. Click the Search Paths button and enter the path to the user profiles RELATIVE TO YOUR COMPUTER. (ex: \\ServerName\UserProfiles) Add it to the list and then Apply and close that dialog.
5. Click the Search button.
6. Edit and add/delete the listed profiles as necessary.
7. Apply and then close the dialog.

The only option in any of the Hive boxes on the operations tab should now be *EVERY USER*. Other than that, the program should work like if it wasn't using profile paths -- except much slower. All of the profiles will be loaded, one-by-one, onto your computer, edited and then unloaded.

Save Tab Settings on Exit: Saves the layout of the operations tabs automatically upon exiting the program. The next time the program starts, the tab layout will be reloaded and the same operations will be immediately available.

Always Update Tab Settings on Exit: Persistent version of the item above.

11. Command Line Options

The command line options offer the opportunity to run repetitive operations from a batch file or to schedule high bandwidth or lengthy tasks to run overnight or on weekends when the impact on the network will be reduced.

The feature requires you to complete two steps in advance of running the task from the command line or as a scheduled task in Windows Task Scheduler:

- 1) Create a group (Edit->Save Group) that contains the computers that should receive the operation (remember the name of the group!).
- 2) Create a Quick Entry with the operation settings to be applied (remember the name of the Quick Entry!).

Once these two items are in place they are used as arguments on the command line of the program in this format:

MREGCHG "Group Name" "Quick Entry Name" RUN

Where:

- **"Group Name"** is the name of the group you created in step (1) above (or **"*ALL*"** to select all computers in the computer names list)
- **"Quick Entry Name"** is the name of the Quick Entry you created in step (2) above
- **RUN** is an optional parameter that tells the program to really execute. If you do not include this parameter then the computer names will be selected and the Quick Entry will be loaded and ready to go, but the operation WILL NOT EXECUTE.

Within about 60 seconds of when the last thread finishes, the program will exit on its own. Even if you did not include the RUN parameter the program will still exit after about 60 seconds! This should give sufficient time to check the entries to confirm they are the ones desired.

If you decide to schedule multiple consecutive tasks or run them from a batch file, please allow **ample** time for the prior task to complete before the next task begins, the program still only allows a single copy of itself to execute at one time. Additionally, if you are scheduling the program as a task, it must run under the credentials of a user authorized to make the changes and it also may be necessary to allow it to interact with the desktop.

12. Troubleshooting, Updates and Support

Troubleshooting

Failures within the program usually fall into one of two areas: Unable to connect or incorrect operation entries.

The inability to connect to a remote machine can be caused by any number of problems on your computer, the network, or the remote computer. In general, if you can connect to the computer using REGEDIT to change the key then you should be able to connect with Multi-Remote Registry Change. Sometimes just clicking Run a second time to try the operation again is enough to get past whatever caused the initial failure. One quick way to test connectivity is to open a command prompt and type "net use IPC\$ \\Computername". If you get a reply that the command completed successfully then everything should be working. If it prompts for a user name then you probably have security issues. If it fails then you may have network connectivity issues (is the remote computer even switched on?).

Incorrect operation entries can be much harder for you as the user to diagnose. It can *look* right and still not be what you expect. Newer users are especially susceptible to this since they may be unfamiliar with the syntax the program uses. At least 98% of the time when we are contacted with a "It runs but doesn't create(/delete/copy,etc) the key as expected" problem it turns out to be an incorrect entry in the Key Path part of the operation. To better double check your entries, hit CTRL-ALT-Q when the operation window has focus and look at the text the program is using in the Quick Entry settings box. If everything looks right and you still cannot get it to work, please take a screenshot of the operation screen and email it to support@eytcheson.com. The screenshot will help us identify what is causing the problem.

Another category of failures that you may encounter when using Multi-Remote Registry Change are entries in the Status log that start with "The error (some error name) has occurred in the program..." Normally these are not cause for concern. When you see the notice in the status log, it means the program has handled the error and is moving along to other things. It could be that the data type was not what was expected or that the network connection to the computer was unexpectedly terminated or that a user logged off in the middle of a HKCU operation. You only need to report the problem if it has kept the program from working as expected.

If you are in the middle of an operation and see one of the Windows dialogs pop up that says that "an error has occurred and that the program must be closed", WAIT! Chances are that the error that Windows is

objecting to occurred in just one of the threads and the program will still complete the operation correctly. There are some Windows API errors that simply cannot be handled by the calling program.

Finally, if you have trouble with the program, please don't hesitate to send your questions or problems to support@eytcheson.com! Your question will be answered quickly, and by someone who knows the program inside and out.

Updates

The program has built-in self update feature. Use the option on the help menu to start the process. If your network uses a proxy server, enter the settings for the proxy server prior to running the update.

Support

For technical support, to report a bug or make a suggestion, please send e-mail to:

support@eytcheson.com

Please check the Eytcheson Software web site at <http://www.eytcheson.com> for other program updates or additional information.

13. Ordering

Order Form

Name: _____

Company: _____

Address: _____

City: _____

State: _____

Postal/ZIP Code: _____

(Country): _____

Daytime Phone #: _____

FAX #: _____

Email: _____

Multi-Remote Registry Change 4

Registration number received via Internet e-mail:

	Num.	Price	Total
Administrators	_____	X_\$35.00__	= _____
Computer Names in Computer Names List	_____	X*_____	= _____
Hard Copy Documentation with CD--	_____	X_\$35.00__	= _____
--US Add \$3.85 for Priority Mail			= _____
--Outside US add \$9.00 for Global Priority Mail			= _____
		Total =	_____

*Computer Names are priced as follows:

Computers	%Discount**	Price Each
1-99	0	\$2.00
100-249	5	\$1.90
250-499	10	\$1.80
500-999	20	\$1.60
1000-1499	30	\$1.40
1500-1999	35	\$1.30
2000-2999	40	\$1.20
3000-3999	45	\$1.10
4000-	50	\$1.00

** %Discount is off regular \$2.00 each price.

For Example: If your organization has 2 administrators and 700 Computers, your price would be:

Administrators:	2 X \$35.00	=	\$70.00
Computer Names:	700 X \$1.60	=	\$1120.00
	Total	=	\$1190.00

Method of Payment

☐ Check (US Funds drawn on US Bank)
☐ Purchase Order (Terms NET 30)
☐ Electronic Funds Transfer (*\$10 additional fee required)
☐ Credit Card

Name on Card: _____

Billing Address: _____

Card Type: ☐ Visa ☐ MasterCard ☐ American Express

Card Number: _____

Expiration Month: _____ Year: _____

Please make remittance payable to Eytcheson Software.

Prices and terms subject to change without notice.

Mail or FAX this form to:

Eytcheson Software
608 S. 4th St.
Independence, KS 67301 USA
Fax (620)331-4471

Ordering is also available via a secure web site - Click Help-Secure Online Order. (Or go to <http://www.eytcheson.com/secureorder.htm>)

*Contact sales@eytcheson.com for more information.

14. License

THE INFORMATION AND CODE PROVIDED IS PROVIDED AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DAMAGES WHATSOEVER INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF THE AUTHOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THIS PROGRAM CAN QUICKLY AND EASILY MAKE EVERY COMPUTER IN YOUR ORGANIZATION UNUSEABLE. IT IS INTENDED FOR USE BY EXPERIENCED NETWORK ADMINISTRATORS ONLY. THE USER IS RESPONSIBLE FOR ENSURING THE ACCURACY OF THEIR ENTRIES. **NO WARNING WILL EVER BE GIVEN.**

15. Index

DELETE KEY	10, 21, 22
DELETE VALUE	10, 21
EVERY USER	9
EVERY USER Options	40
8. Quick Entry	37
ADD TO VALUE-END	10, 11
ADD TO VALUE-START	10, 11
Advanced Selections	16
Allow Connect Retries	40
<u>Alternate User Credentials</u>	39
<u>Always Update Tab Settings on Exit</u>	41
Apply from File	21
Browse Registry	26
Change Many Keys (Key Group)	18
Change Service User Info	27
Change Single Key	17
Change User Rights	20
Check for Key	18
Command Line Options	42
<u>Computer Names List</u>	12
Create "Call" Batch File	22
<u>Credentials</u>	
Alternate User	See Alternate User Credentials
<u>Data File Location</u>	14
<u>Default Log File Folder</u>	39
DELETE_KEY	11
DELETE_VALUE	11
Dump Key to .REG File	28
Features	6
General Instructions	8
HKEY_CLASSES_ROOT	8, 9
HKEY_CURRENT_CONFIG	8
HKEY_CURRENT_USER	8
HKEY_LOCAL_MACHINE	8, 9, 17, 18, 20, 22
HKEY_USERS	8, 9, 20, 22
Insert into REG_MULTI_SZ	28
License	47
Logging	14
Lookup IP Addresses	20
Manage Services	29
Open Default Log File Folder	39

Operations	17
Disabling.....	17
<u>Operations tabs</u>	13
Ordering	45
Order Form.....	45
Other/Miscellaneous.....	39
Allow Connect Retries.....	40
Open Default Log File Folder	39
Save n Entries for Reuse.....	40
Set Log Delimiter	39
Verbose Log Entries.....	39
Overview	5
<u>Password</u>	See Alternate User Credentials
REG File Operations	19
REG_BINARY	10
REG_DWORD	10
REG_EXPAND_SZ.....	10
REG_FULL_RESOURCE_DESCRIPTOR	10
REG_LINK.....	10
REG_MULTI_SZ	10, 28
REG_NONE	10
REG_QWORD	10
REG_RESOURCE_REQUIREMENTS_LIST.....	10
REG_SZ	9, 10, 17
Registry Security.....	23
Permissions	25
Registry Security Actions List	23
Registry Security Detail Dialog	24
Security Object Inheritance.....	25
REMOVE FROM VALUE.....	10, 11
Retry Log	15
<u>Retry Log Entry Warning Count</u>	40
<u>Retry Log items</u>	40
Save n Entries for Reuse.....	40
<u>Save Tab Settings on Exit</u>	41
Search and Replace	28
Send Message	27
Set Log Delimiter.....	39
Shutdown Systems	18
<u>Status Bar</u>	12, 14
<u>Status Display</u>	13
Substitution Items	30
Substitutions	30
Examples	32
INIFILE.....	30
Registry	30
Static.....	34
Support	44
Web Site	44
System Requirements	7
The Main Window	12
Tools	38

SID <-> UserName.....	38
String Conversion.....	38
Troubleshooting	43
Updates.....	44
<u>Use Profile Paths for *EVERY USER*</u>	40
Verbose Log Entries.....	39