

White Paper: Solving the “Common Administrator Account Configuration Problem” with the User Manager Pro Random Password Generator Module

Rev 1 October 16, 2002

Written by Philip Lieberman (phil@lanicu.com)
Lieberman Software Corporation
<http://www.lanicu.com>

Abstract

It is a common practice to assign the same local administrator name and password to every workstation in a Window's domain. If a hacker decrypts this password, they will have full administrator access to every machine with the same password. This document describes how Lieberman Software Corporation' Random Password Generator can mitigate this flaw found on almost all Windows NT, 2000, XP, and Server 2003 systems, by enabling a domain administrator to periodically (and unattended if desired) randomize all local administrator passwords.

Contents

1. Introduction	3
2. Best Practices	3
3. Product Installation	4
4. Verification of Feature Enable	4
5. Generating Random Passwords	5
6. Saving Randomly Created Passwords	5
7. Setting Password Complexity	6
8. Backward Compatibility	6
9. Password Length	6
10. Password Must Contain	7
11. Generate Sample	7
12. Scheduling a Regular Random Password Change	7
13. Creating an Account with a Random Password	7
14. Recovering Random Password Settings	8
15. Menu Option: View Single Entry	8
16. Menu Option: Report Generator	9
17. Menu Option: Delete Entries	10
18. Menu Option: Changing Recovery Console Password	10
19. Menu Option: Refreshing List	10

1. Introduction

The common practice of assigning the same local administrator name and password to every workstation in a domain is the largest security hole any company can have. If someone decrypts this common account's password (there are tools out there to do so such as L0phtCrack), they would have full administrator access to all other machines in the organization with that same account.

To solve the "common administrator account configuration problem", we created the optional **Random Password Generator Module for User Manager Pro**.

With this add-on component, a domain administrator can periodically (and unattended if desired) randomize all local administrator passwords on even the largest domain in just a few minutes. The new passwords can be automatically stored in secure database within the program for later review if necessary.

When randomization has been completed, cracking the local password on any single machine does not provide any clue as to what credentials will work on other machines.

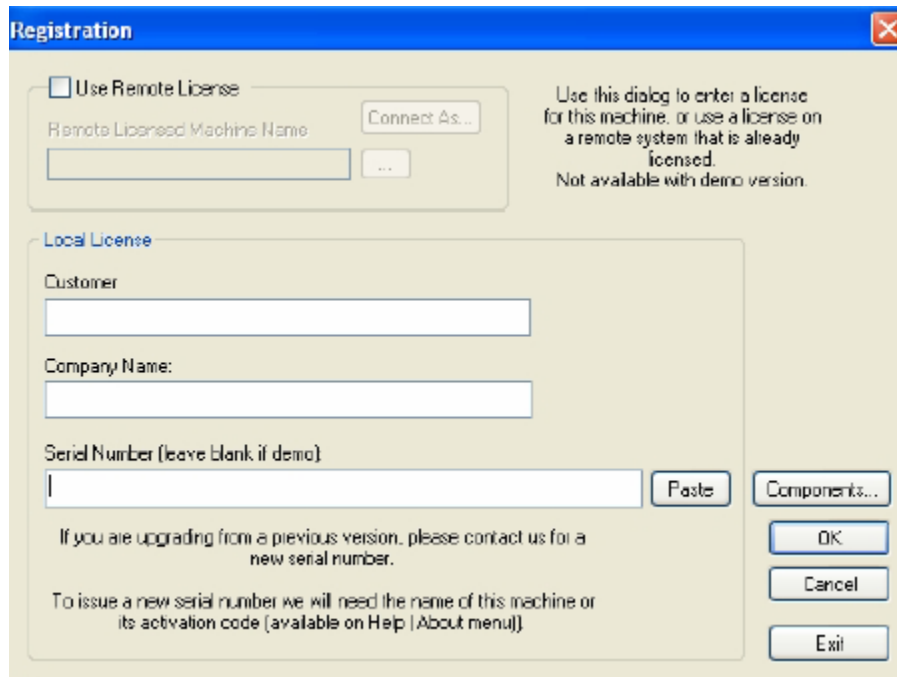
2. Best Practices

Administrators should change the built-in administrator password on all of their workstations/servers at regular intervals (at least every 30 days). The common local machine administrator passwords should also be changed immediately when there is turnover in the pool of machine administrators.

If the local administrator password is common to all machines, but is changed regularly and is cryptographically complex (more than 8 characters, then brute force password cracking tools will take longer to crack the password than the interval between password changes. In that case, cracking passwords is a useless exercise. If the administrator fails to change the passwords frequently enough, or uses passwords for the common account that are too simple, then it would be possible to successfully crack the password and gain unauthorized access.

3. Product Installation

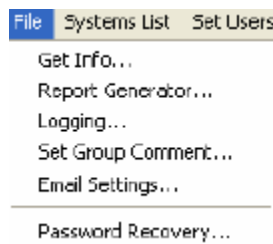
This product requires version 3.09 or later of User Manager Pro. The feature is enabled when the proper licensed serial number is entered. To enter the serial number provided to you when you purchase this add-on, go to the menu option: **Help | Register** located in the initial main dialog.



Enter your serial number in the “Serial Number” field and click on the “OK” button.

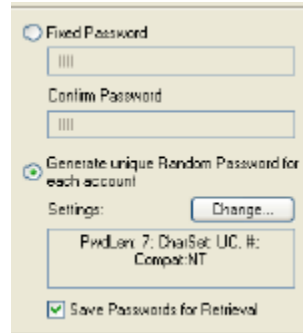
4. Verification of Feature Enable

You can confirm the enablement of this add-on by opening any group of machines and going to the File menu pull down. If you see the entry “Password Recovery” at the bottom of the list, you have the add-on enabled.



5. Generating Random Passwords

Highlight a single machine and click on the “Users” button. Look at the bottom of the Users dialog and focus on the password area.



You can select either “Fixed Password” or “Generate Random Password for each account” when creating or updating an account. The first option: “Fixed Password” sets the account to the password manually entered and confirmed. The second option: “Generate Random Password/System” automatically generates a different random password for the account on each machine (add or update modes). You would want to use the second mode to assure that every workstation has a different password for the built-in administrator account.

6. Saving Randomly Created Passwords

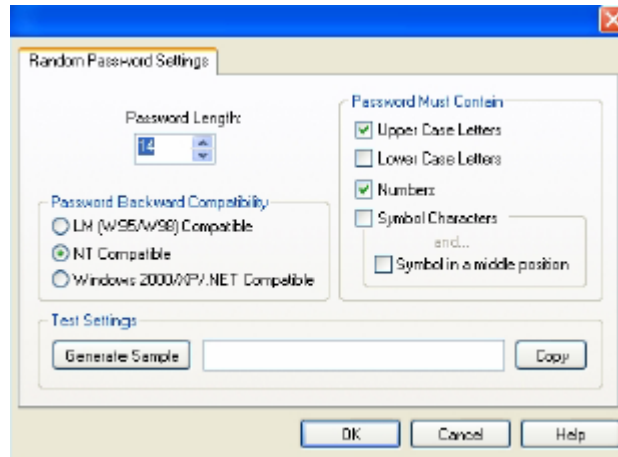
The “Save in Database” checkbox keeps a local copy of each random password by machine and account created/updated. Access to the randomly created passwords is password controlled. All data is stored in an encrypted format within the registry of the machine running User Manager Pro. The information is further ACL controlled so that only administrators have access to the encrypted data in the registry.

If you are concerned about the level of encryption of the passwords, you can choose to not store the encrypted passwords. If at some point in the future you wish to gain access to a specific machine, you can set the password to a known value. Remember that you should still be able to administer all machines, even those with unknown passwords, since the local Administrators group of each machine should still contain entry for the Domain Admins group.

WARNING: If your environment does not assure that you are in a group that is seen as a local administrator of every modified machine, you should always check the “Save Passwords for Retrieval” check box.

7 Setting Password Complexity

The complexity of passwords generated can be modified to suit your organization's standards. To change the password complexity, click on the "Change..." button



8. Backward Compatibility

The "Password Backward Compatibility" radio buttons control the characteristics of password generated by the program so that peer-to-peer access will be possible and appropriate.

The "LM Compatible" option is necessary when you wish to assure that Windows 95/98/ME and OS/2 machines can access the account. The password generated will be sufficiently simple for these downlevel clients to access the machines. This is not a good choice for creating unbreakable passwords.

The "NT Compatible" is the most common option and generates passwords up to 14 characters in length. This length of password can be theoretically broken given enough computer power and time, but with a length of 14 characters (maximum length for this platform type) and with a sufficiently complex character set, this would be unlikely. However, it is recommended that the password be updated regularly anyway.

The "Windows 2000/XP/.NET Compatible" option allows you to create passwords that are greater than 14 character in length. With longer passwords it becomes virtually impossible to crack the password using a brute force attack. The password length can be up to 127 characters in length for this option. Anything over 14 characters will create very strong passwords. Beware that by using this option, Windows NT machines will be unable to use the accounts remotely since NT physically enforces a maximum entry of 14 characters for the password.

9. Password Length

The password length is set by entering the length manually or by using the spin button adjacent to the "Password Length" field. A minimum of eight characters should be used for randomly generated passwords. The absolute minimum password length is dependent on how many checkboxes are checked in the "Password Must Contain".

10. Password Must Contain

This group contains checkboxes of characters the **MUST ALL** occur in the generated password. An added optional bonus is the characteristic of making sure that a symbol character must occur within the password, but not as the first or last character.

The program always checks the complexity of the randomly generated password. If the generated password does not conform to all of the checked boxes, it is discarded and new ones are continuously generated until one is found that matches all of the character set requirements.

11. Generate Sample

You can try out the random password generator and all of the previously discussed characteristics by clicking on the “Generate Sample” button. The resulting password can be copied to the clipboard and used wherever you need a truly random password.

12. Scheduling a Regular Random Password Change

To schedule a regular password change of an existing account:

1. Set the “Action” radio button to “Update”
2. Enter the user name in “User Name (Original) field
3. Set the “Update” checkbox to the left of the password options
4. Set the radio button: “Generate Random Password/System”
5. Check the “Save in Database” if you want a record of the passwords used
6. Click on the “Schedule” button to set the frequency of updates

If you don’t know or are not sure of the name of the built-in administrator account, you can use the value of “*A” in the “User Name” field to look up the account name per machine.

Make sure that no other update checkboxes are set if all you wish to do is change the password.

13. Creating an Account with a Random Password

To schedule a regular password change of an existing account:

1. Set the “Action” radio button to “Add”
2. Enter the user name in “User Name (Original) field
3. Fill-in all fields and options according to your needs
4. Set the radio button: “Generate Random Password/System”
5. Check the “Save in Database” if you want a record of the passwords used

6. Click on the “Apply” button to create the account immediately

14. Recovering Random Password Settings

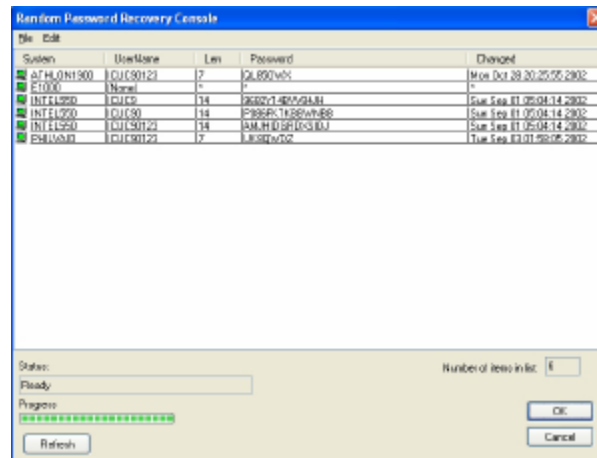
To retrieve the current list of passwords for the current group,

1. Go to the menu option:

Users/Groups | Password Recovery

2. Enter the password for password recovery (default is: **MI4GUYC** (all caps)). You can change this password once you have successfully entered the default password.

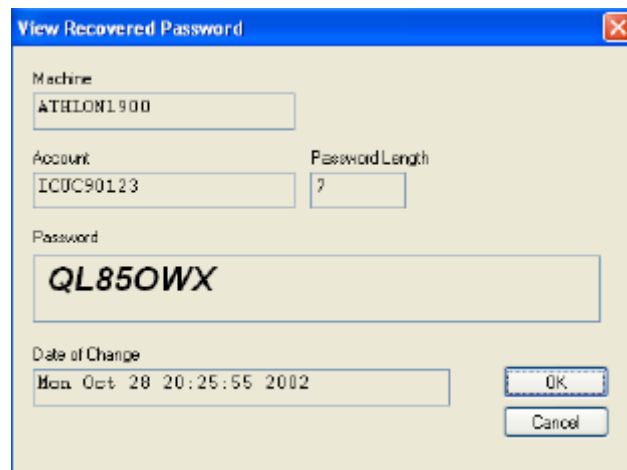
If you have entered the correct password, you will see a dialog similar to the following:



15. Menu Option: View Single Entry

You can double-click on any entry, or use the menu option:

Edit | View Single Entry... to see a larger version:

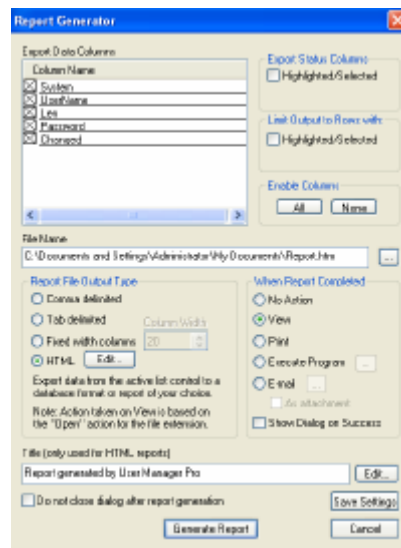


16. Menu Option: Report Generator

You can use the built-in report generator in the menu:

File | Report Generator.

Via the menu, you can create comma-delimited output or HTML and send it to a variety of different destinations.



This is an example of an HTML output report from the Report Generator:

Report generated by User Manager Pro
 Run Date/Time: 10/29/2002 12:21:59 PM
 Run By: ATHLON1900\Administrator
 Machine: ATHLON1900
 Machine Group: abc
 Group Description:

System	UserName	Len	Password	Changed
ATHLON1900	ICUC90123	7	QL850WX	Mon Oct 28 20:25:55 2002
E1000	(None)	*	*	*
INTEL550	ICUC9	14	9682Y148VV84JH	Sun Sep 01 05:04:14 2002
INTEL550	ICUC90	14	P086FKTK8BWNBB	Sun Sep 01 05:04:14 2002
INTEL550	ICUC90123	14	AMJHIDGRDXXSDJ	Sun Sep 01 05:04:14 2002
PHILVADO	ICUC90123	7	UK8QWDE	Tue Sep 03 01:58:05 2002

17. Menu Option: Delete Entries

If you remove machines or accounts, the password retrieval console will still have the old password information. If you wish to delete some or all of the recovery information, you can select the entries to delete, followed by using the menu option:

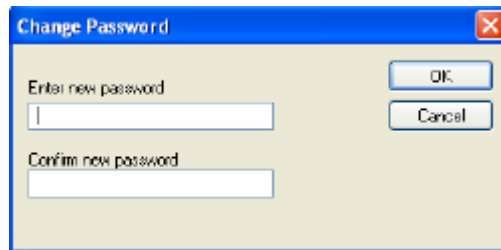
Edit | Delete Entries

18. Menu Option: Changing Recovery Console Password

To change the password used to access the password recovery console, use the menu option:

Edit | Change Recovery Access Password

Then enter the new password twice. It would be a good idea to write down this new password and place it in a secure location. If you forget this password, you will be unable to recover the passwords or get to this console.



19. Menu Option: Refreshing List

When you first open the recovery console, the list is refreshed with the most up-to-date information available. If you are running scheduled updates, and leave this list on your screen for an extended period of time, the information will not automatically update unless you click on the "Refresh" button, or leave and reenter this screen (password required).

Our support staff is available to answer your technical questions whether you are a customer or not.

Voice: 800.829.6263 (USA/Canada) Voice: (01) 310.550.8575 (Worldwide) Fax: (01) 310.550.1152 (Worldwide)
Web: www.lanicu.com Email: support@lanicu.com

