

Application Note: Removing Obsolete Machine Accounts with User Manager Pro

Rev 1 – December 3, 2003

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

Abstract

This white paper provides step by step instructions to remove obsolete machine accounts with Lieberman Software's **User Manager Pro**

Contents

1. Introduction	3
2. Background	3
3. Locating Dead Machine Accounts	4
4. Going Further: Reviewing the List with Team Members	6
5. Deleting Dead Machine Accounts	8
6. Quick Tip to Delete Machines Accounts Really Fast	9
7. Conclusion	10

1. Introduction

Managing Machine Accounts in a Windows domain is a frustrating task and in some environments, completely impossible. Every time a Windows computer joins a domain or has its name changed, a Machine Account is automatically created on the Domain Controller. Microsoft has not provided an automated solution for managing or removing these accounts, so every time a computer is decommissioned or renamed, an obsolete Machine Account is left behind in the Domain.

Obsolete Machine Accounts are both a security risk and a management nightmare. By default, Windows changes Active Machine Account passwords regularly to keep them secure; obsolete Machine Account passwords are never changed, leaving them vulnerable. Without a current list of Domain members, a system administrator cannot accurately report on the state of the Domain. For example, they would not be able to ensure that all machines in an environment have the latest security patches installed.

This application note demonstrates, step-by-step, how Lieberman Software's **User Manager Pro** can find and delete these obsolete machine accounts in even the most populous domain.

2. Background

Intra-Machine relationships in Microsoft Domains are managed through Trust Accounts. Domain Servers use Trust Accounts to determine which computers can have access to network resources. Machine Accounts are one type of Trust Account; the other types are Server and Inter-Domain Trust Accounts.

Trust Account types are set when the accounts are created, and cannot be changed. Trust Account names are always Machine Name (or Domain Name for domain trusts) plus a dollar sign. For example, the Machine Account for a computer named FINE would be FINE\$.

Machine and Server Trust Account passwords are managed by Windows; by default they are changed by the Domain Controller about every 30 days. To accomplish this password management, Windows tracks and stores the age of Trust Account passwords. **User Manager Pro** exposes Trust Account password age to system administrators, allowing them to report on and use this valuable and otherwise hidden data.

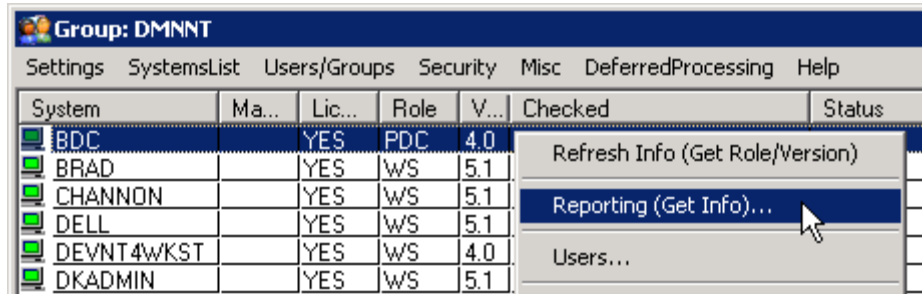
Reporting on Machine and Server Trust Account password age allows computers that have not been in contact with the Domain Controller for an extended period of time to be identified. In most environments, a password age of greater than 60 days on a Machine or Server Trust Account would indicate that a computer has been renamed or removed from the environment, leaving an orphaned Trust Account behind.

Inter-domain Account passwords must be managed manually by domain administrators, so password age on Inter-domain Trust Accounts cannot be managed using this method.

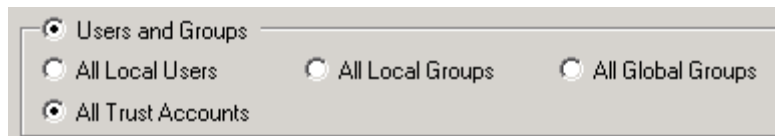
User Manager Pro makes it possible for system administrators to discover all Machine and Server Trust Accounts with a password age greater than 60 days (for example), and delete them in a few easy steps.

3. Locating Dead Machine Accounts

1. [] Start **User Manager Pro** (Version 4.67 or later) and bring up a machine group that contains the primary domain controller (NT 4) or PDC emulator (W2K or 2003).
2. [] Highlight the domain controller entry and right-click to bring up the context menu. Select the "Reporting (Get Info)..." entry from the menu.



3. [] Set the group radio buttons on "Users and Groups" and "All Trust Accounts".



4. [] Click on the "Report" button to retrieve all of the machine/server and domain trust accounts.



5. [] Sort the resulting list by the password age (descending) by clicking on the "Password age" header.
6. [] Highlight the accounts that are obviously no longer active. Important! Verify the entries in the "Type" field to avoid deleting a domain trust account.

System	Username	Type	Password Age
BDC	BDC\$	Server	670 Days 00:29:41
BDC	VAID\$	Workstation	499 Days 07:49:59
BDC	TRAINING7\$	Workstation	297 Days 13:43:57
BDC	TRAINING8\$	Workstation	292 Days 14:27:59
BDC	INTEL90\$	Workstation	214 Days 20:53:24
BDC	TRAINING2\$	Workstation	181 Days 05:08:17
BDC	TRAINING4\$	Workstation	138 Days 13:46:59
BDC	TRAINING5\$	Workstation	138 Days 08:29:26
BDC	JAMEY\$	Workstation	50 Days 12:07:44

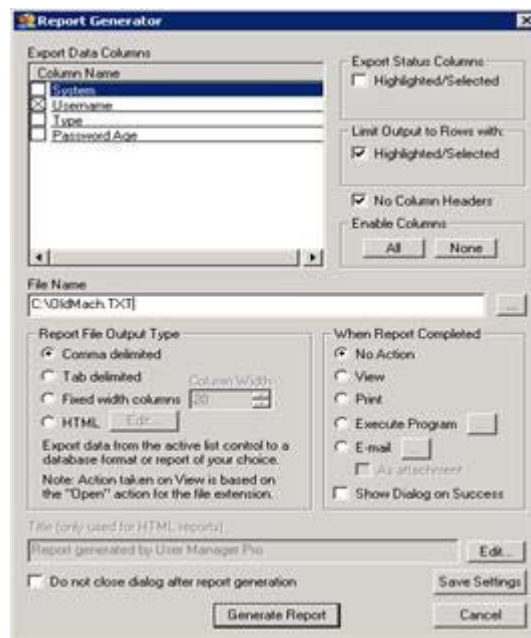
NOTE: If you are ready to delete the machine accounts immediately, you can go directly to step 6.4"

7. [] After highlighting the appropriate entries, click on the “Export Report” button.

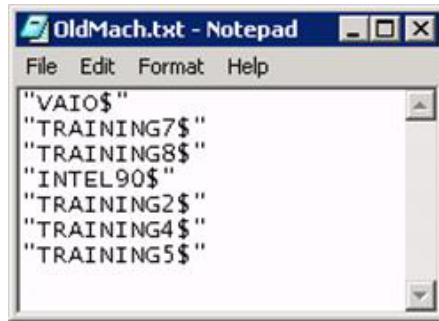


This will trigger the display of the “Report Generator” dialog.

8. [] Uncheck all “Export Data Columns” except “Username” so that the exported report will only contain the names of the machine accounts.
9. [] Set the checkbox in “Limit Output to Rows: with Highlighted/Selected” so that only the highlighted entries with very old passwords will be deleted.
10. [] Set the checkbox in “No Column Headers” so that the name of the column (Username) is not the first entry in the account list.
11. [] Create a “File Name” that is easy to find. It is recommended to create a text file by using a “.TXT” extension on the file.
12. [] Set the “Report File Output Type” to “Comma Delimited”. Set the “When Report Completed” to “No Action” since only the file generated is needed.
13. [] Finally, click on the “Generate Report” button at the bottom of the dialog.

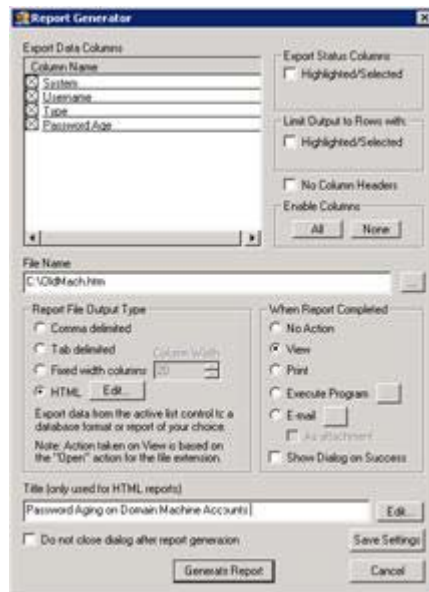


The generated file can be reviewed by opening it in Notepad. Notice that each machine account is on a line by itself.



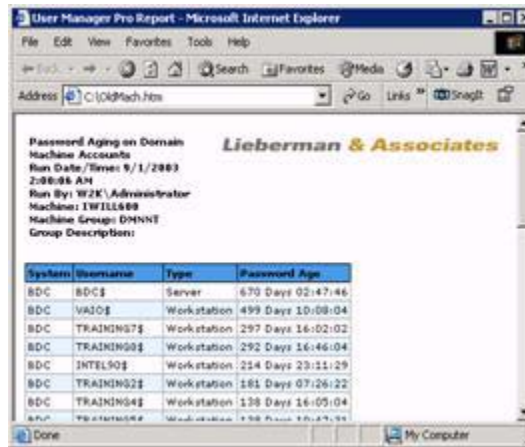
4. Going Further: Reviewing the List with Team Members

1. [] To circulate the account deletion list prior to actual deletion, repeat the previous steps, but change the “Report Generator” dialog so that all fields in the “Exported Columns” are checked, and the “Report File Output Type” is HTML.

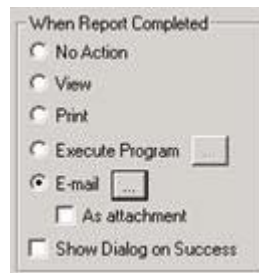


2. [] Set the “When Report Completed” to “View”.
3. [] Note that the file name now has an extension of “.HTM”.
4. [] Click on the “Generate Report” button.

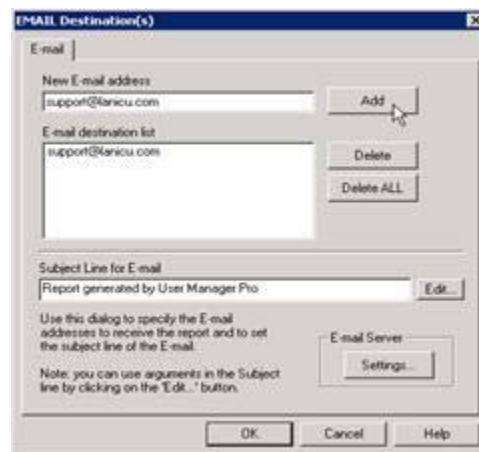
5. [] The report can be viewed with your Web browser.



6. [] If desired, a report can be sent to your team members. Attach the file in the “Address” field to an outgoing E-mail. Alternately, if an SMTP mail server is available, go back to the Report Generator and select the “E-mail” option and click on the “...” button.

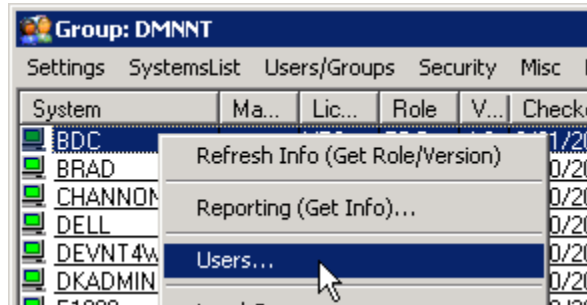


7. [] Set the destination E-mail list and configure the SMTP settings by clicking on the “Settings” button.

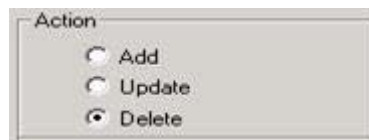


5. Deleting Dead Machine Accounts

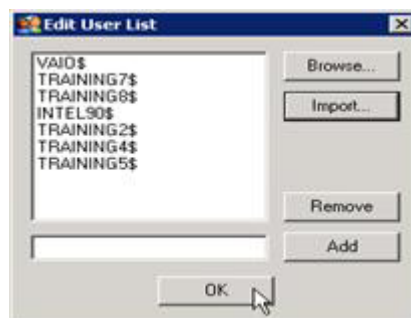
1. [] Now that the file containing a list of machine accounts to delete has been created, select the Domain Controller holding the machine accounts.
2. [] Right-click on the Domain Controller entry and select the “Users...” menu option.



3. [] Select the “Delete” radio button in the “Action” group.

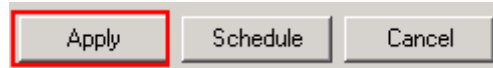


4. [] Click on the “...” button to the right of the “User Name (Original)” field to enter the list of accounts to delete.
5. [] Click on the “Import...” button to specify the file containing the list of machine account names to delete.
6. [] Verify that the list of accounts is correct. To delete an entry, highlight it and click on the “Remove” button.
7. [] If everything is OK with the list, click on the “OK” button.



8. [] Notice that the “User Name (Original)” field now says “[multiple]” if there is more than one machine account in the list.

9. [] Click on the “Apply” button at the bottom of the dialog to start the deletion action.



6. Quick Tip to Delete Machines Accounts Really Fast

The following steps eliminate the need to export a list of machine accounts into a file, import the list into the Users dialog, and finally use the Delete User option.

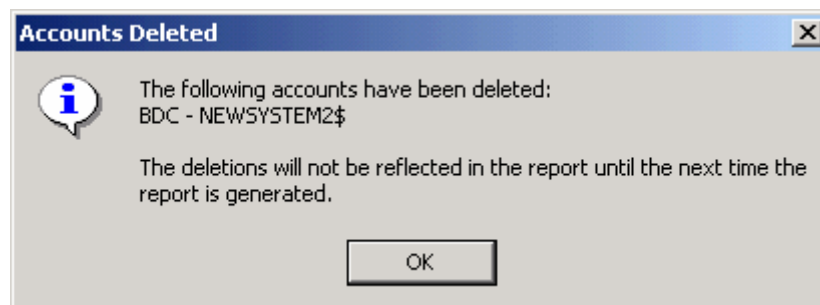
1. [] Generate a report of the machine trust accounts (as previously described).
2. [] Sort the resulting list by password age.
3. [] Highlight all of the machine accounts to delete (usually older than 60 days).
4. [] Right-click on the highlighted entries. You will then see the following context menu:

BDC	PENT4\$	Workstation	46 Days 16:07:55
BDC	NEWSYSTEM2\$	Workstation	102 Days 05:18:49
BDC	PLAYGROUND\$	Interdomain	131 Days 03:34:47
BDC	TELEQUAL03\$	W	
BDC	JAMEY\$	W	
BDC	TRAINING5\$	W	
BDC	TRAINING4\$	Workstation	231 Days 12:14:18

Delete User(s)

Create New Group with Selected Systems

5. [] Left-click on the "Delete User(s)" menu option
6. [] After the accounts have been deleted you should see a pop-up similar to the following:



7. [] That's all there is to deleting the obsolete machine accounts.

7. Conclusion

A secure and manageable Domain Controller must have an accurate list of Machine Accounts. However, in most situations the accuracy of the Account list deteriorates because it takes too much time and energy to keep track of the obsolete Machine Accounts.

User Manager Pro has been specifically optimized to give system administrators the power to keep their Machine Account lists up-to-date, easily and in just a few minutes.

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

