# LAPS Local Admin Password Solution

Thursday, November 16, 2017   2:28 PM

Having one local administrator password across our domain was identified as a major vulnerability. This vulnerability provides attackers with a single point of failure to target; one password affords access to nearly every machine in our domain. The LAPS tool sets a randomized password for the local admin account on each individual computer. It should also be noted that this randomized password periodically changes as computers sync with Active Directory.

There are a few methods that we can use to view this random password:

Method 1of3

1. Open Active Directory Users and Computers and expand gmaccm.com->Berkadia->Workstations locate and expand the correct site OU, then highlight the OU. In this case I'm going to use my own laptop for example so I'm highlighting the PAHOR OU to scroll down and locate "PAAMBTSIEBER2L." Unfortunately, if you simply perform a search for the computer name, this process will fail as we will not be able to view an additional tab called "Attribute Editor."
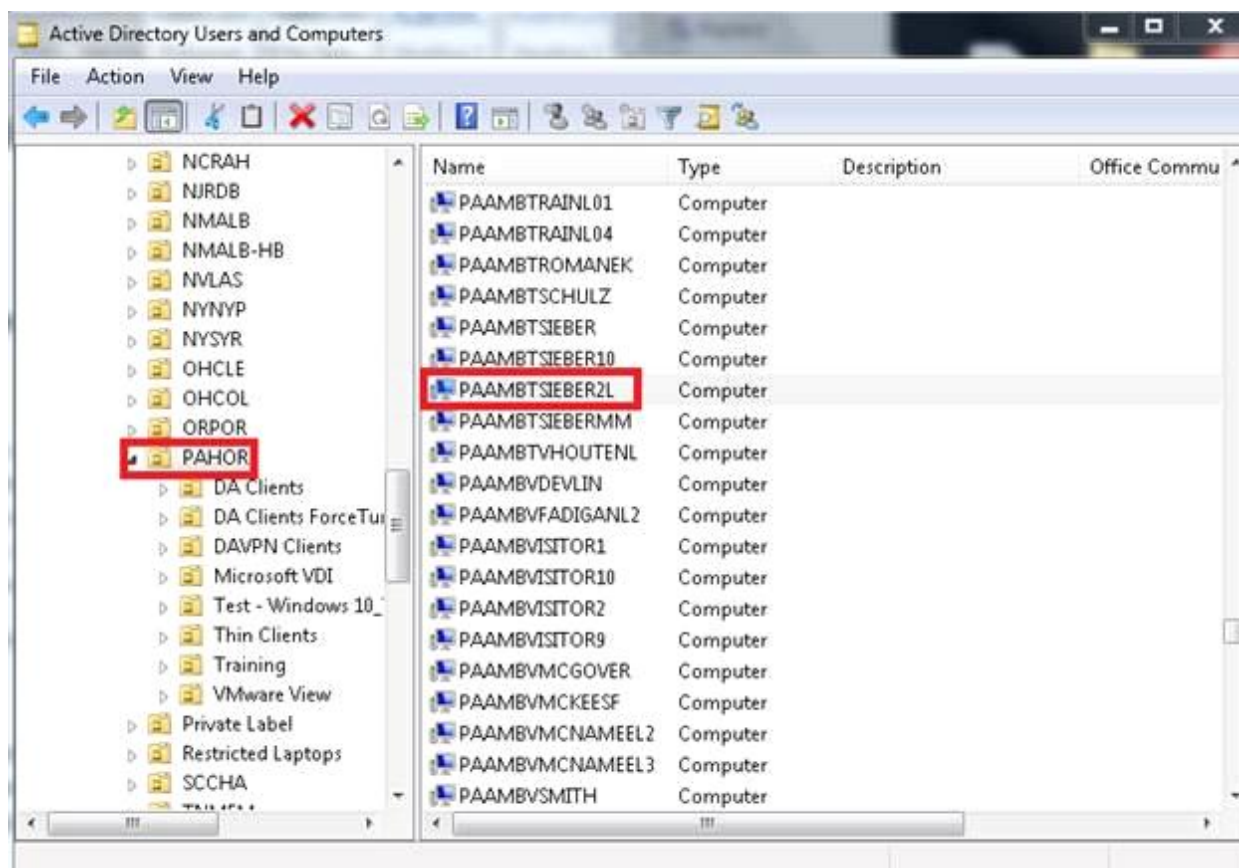

2. Double click the computer name, a new window will open. Select the "Attribute Editor" tab and then look for the "ms-Mcs-AdmPwd" field. This is the new current local admin password for the computer in question.
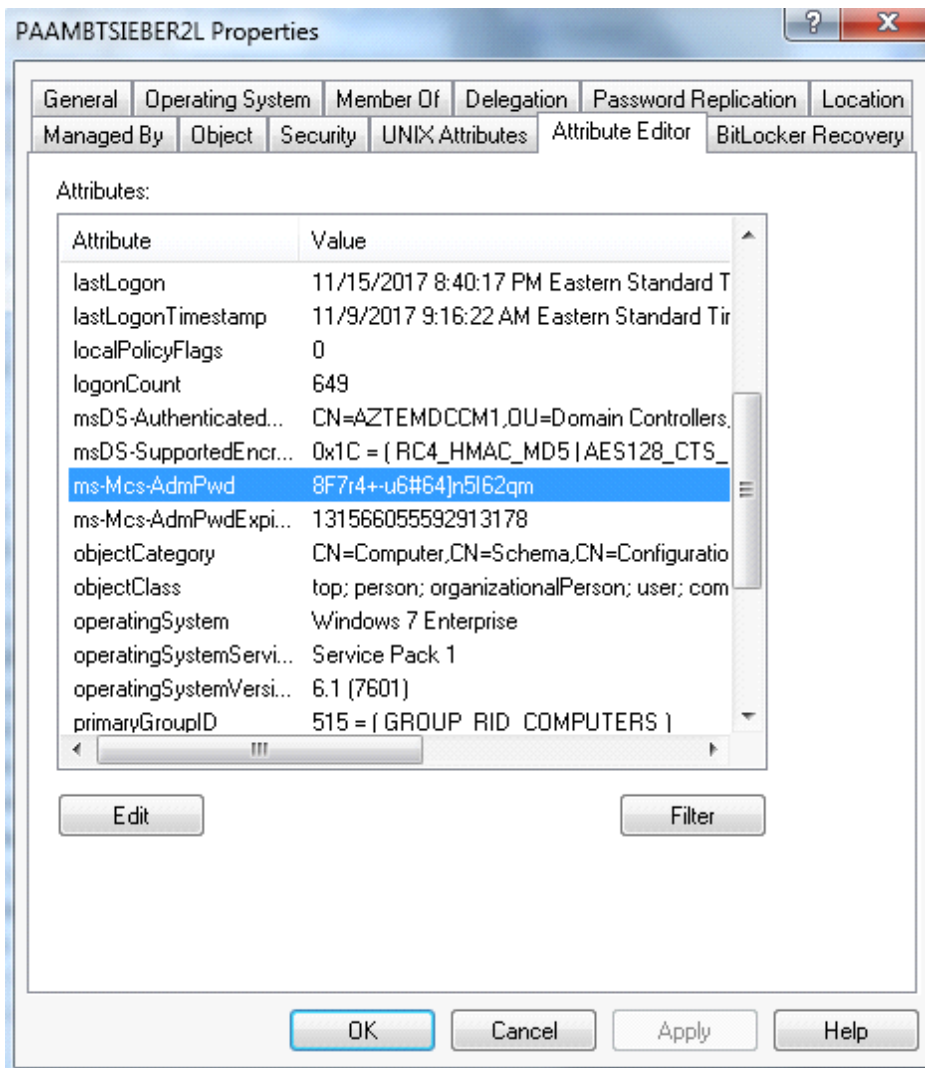
3. If you do not see the Attribute Editor tab, please ensure you have "Advanced Features" selected under view tab on the main AD Users and Computers window.
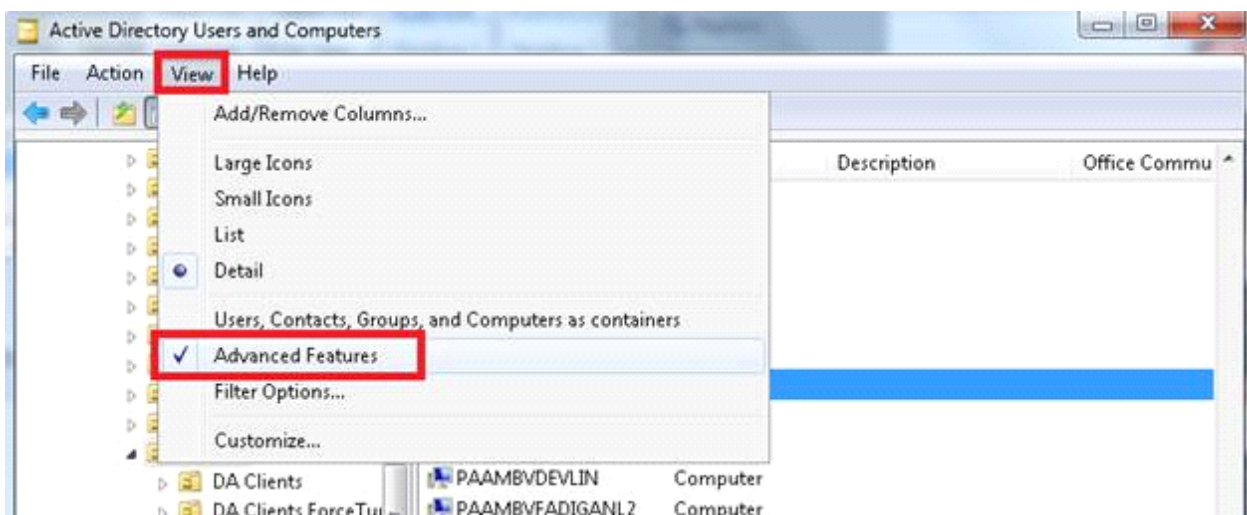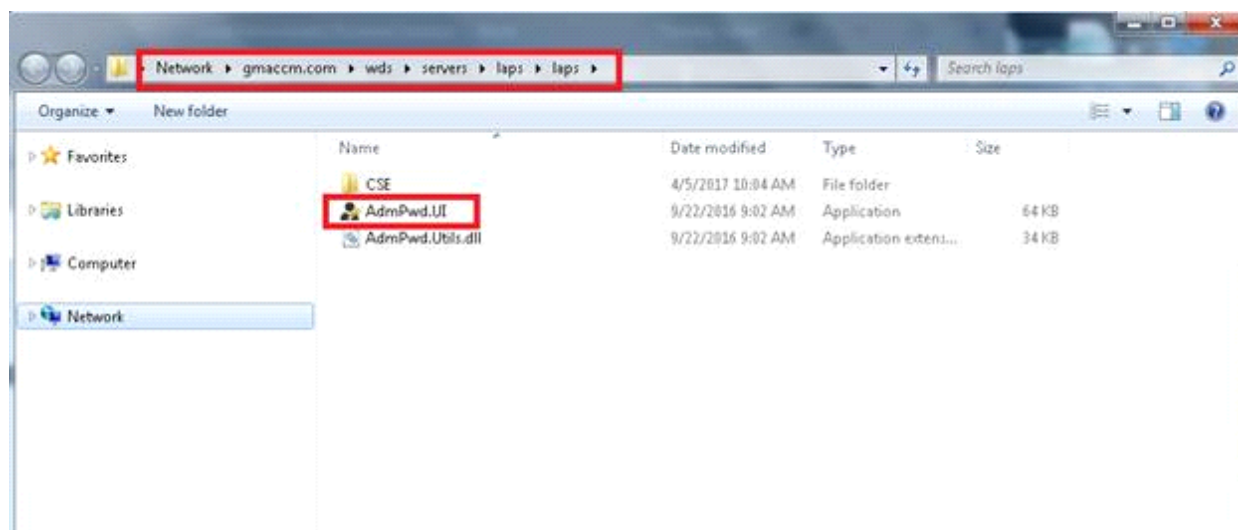

4. To make finding the "ms-Mcs-AdmPwd" field easier, select "Filter" while still in the Attribute Editor window. From there select "Show only attributes that have values." This will eliminate excess fields to look through and speed up the process.
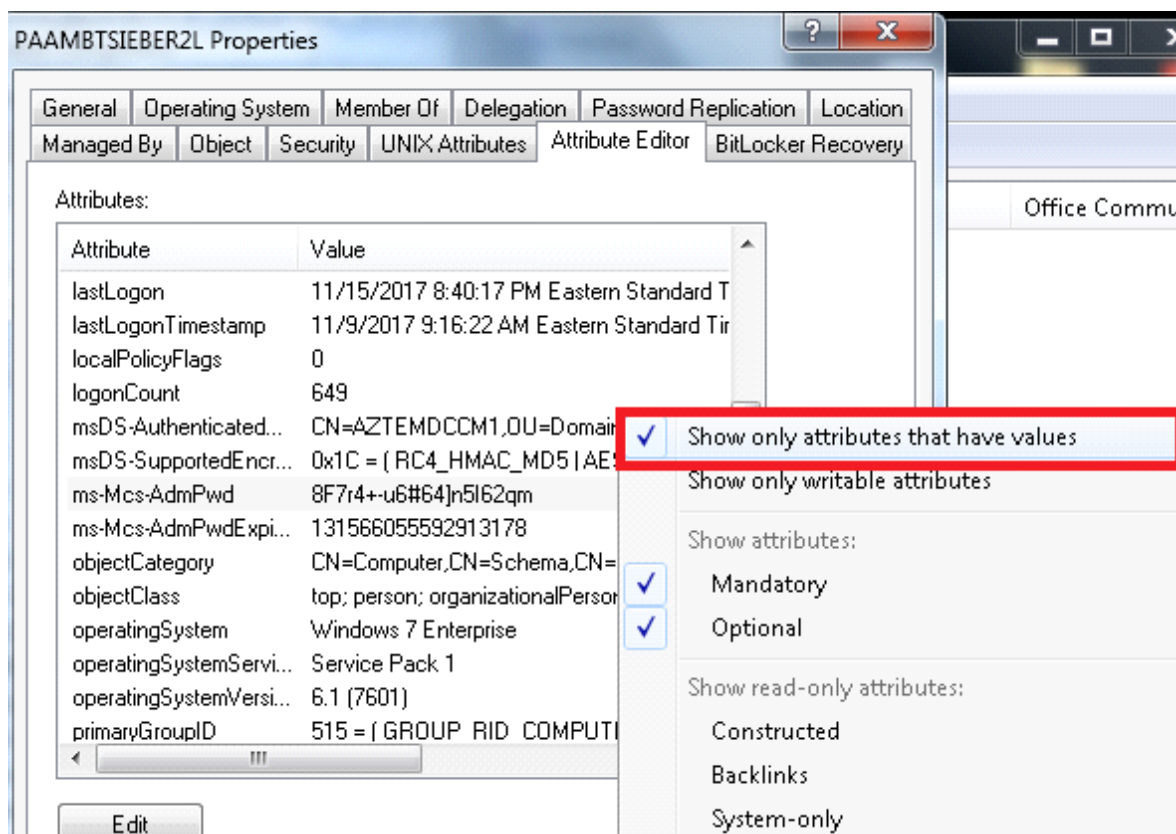
Method 2of3

1. Browse to \\gmaccm.com\wds\servers\laps\laps\
2. Launch AdmPwd.UI.exe **using your -adm account**

3. You'll see the following box pop up, enter the computer name, then select Search. As an added bonus of this particular tool, you'll also see when this temporary password is due to be refreshed.