

Re: Record User Logon/Logoff with Computer Name + Username

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2006-02/msg00094.html>

- *From:* mem0ri <mem0ri@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 20 Feb 2006 11:12:27 -0800
-

Thank you for the info...however, I was unable to find anything that worked on the links provided...and several of them stated specifically to not try the templates on Win2000 Servers (which is what I'm running on).

I will continue to try to work with the system...does anyone else have any ideas?

"YAKETYAK" wrote:

google security templates..

NIST has some, NSA and Microsoft has some too depending on your needs.

Try these..

<http://www.windowsecurity.com/articles/Understanding-Windows-Security-Templates.html>

http://csrc.nist.gov/itsec/download_W2Kpro.html

http://csrc.nist.gov/itsec/guidance_W2Kpro.html

<http://www.sans.org/resources/policies/>

http://www.nsa.gov/forms/site_search_action.cfm

On Fri, 17 Feb 2006 09:25:27 -0800, mem0ri
<mem0ri@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote:

We're running a Windows 2000 server to which many workstations logon throughout the day. The boss would like a record of all remote access successes with a record of the a)incoming computer name, b)username

Re: Record User Logon/Logoff with Computer Name + Username

c)logon
time and logoff time.

I have been attempting to run a record through the Event Viewer and have:

1)Been able to successfully record "Account Logon Events" (672) but these only give me the username that logged on and the time of initial logon. Additionally, to get the information I have to look at the "properties" of each event...as the user is inherently "SYSTEM" when listed in the main Event Log.

This Method is missing: Incoming Computer Name, Logoff Time.

2)Been able to successfully record network Logon/Logoff events (540, 538), though these occur in the thousands (yesterday there were about 18000 of these events) and provide me with virtually no useful information (a logoff occurs virtually simultaneously with a logon when you compare ticket ids). Additionally, though a username is recorded...there is no computer name or reliable way to track times.

It is my understanding that the Security Event Viewer is meant to record things like Account Logons and Logoffs...but nothing seems to be working.

For a short while, I managed to get 682/683 events whenever we tested a VPN access...though those events aren't directly related to a remote access, they did record a username and computer name and time of logon. However...it seems getting these events to show up was more of an accident than an actual recurring and reliable event.

I am desperate for help. Answer needed:

- 1)Username and Computer logged on and Time
- 2)Username and Computer logged off and Time

That's all I need. Can it really be that difficult...heh...(it apparently is for me...)

9/11
Never Forget