

## Re: Security Event Logging and remote WMI connection question

**Source:**

<http://www.tech-archive.net/Archive/Development/microsoft.public.win32.programmer.wmi/2005-01/0221.html>

---

*alexbalaev\_at\_yahoo.com*

**Date:** 01/24/05

Date: 24 Jan 2005 12:16:38 -0800

Hello,

Let me re-phrase the question.

Does any one know on what WMI call these entries are added to remote box security log?

EventID: 538

User Logoff:

User Name:NAME

Domain:DOMAIN

Logon ID: (0x0,0x2FC0A)

Logon Type: 3

For more information, see Help and Support Center at

<http://go.microsoft.com/fwlink/events.asp>.

EventID: 540

Successful Network Logon:

User Name: name

Domain: domain

Logon ID: (0x0,0x1B4755)

Logon Type: 3

Logon Process: NtLmSsp

Authentication Package: NTLM

Workstation Name: boxname

Logon GUID:{00000000-0000-0000-0000-000000000000}

TIA, Alex.

alexbalaev@yahoo.com wrote:

> *Hi there,*

> *So really no one?*

> *Please maybe some MCFT guys that monitor the forum could add any*

> *comments?*

> *TIA, Alex.*

>

> alexbalaev@yahoo.com wrote:  
>> Hello,  
>> Every successful WMI connection to a remote box creates a couple of  
>> entries into Security Event Log on the box: one for successful  
login  
>> and another one for logoff.  
>> I can understand that the information should be logged – all  
>> connections should be tracked.  
>> However if sysadmin monitors (using a sort of notification)  
security  
>> log activity like who and when was logged into a box that could  
> create  
>> a problem. Because the sysadmin will be getting a lot of  
> notifications  
>> from multiple boxes...  
>> Besides if WMI monitors something real-time (like every other time  
>> interval) that could generate a lot of security event log entries  
> too.  
>> So the question is: Is there a way to disable such logging on a box  
> so  
>> that every WMI connection would not generate security event log  
> entry?  
>> Any help would be greatly appreciated,  
>> Thanks, Alex.