

# Re: Unexplained User Account Deletion

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2006-12/msg01475](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-12/msg01475)

---

- *From:* "Joe Richards [MVP]" <[humorexpress@xxxxxxxxxxxx](mailto:humorexpress@xxxxxxxxxxxx)>
  - *Date:* Thu, 21 Dec 2006 16:00:40 -0500
- 

Oh I absolutely do not believe it is an event log problem. It doesn't control anything, it simply reports stuff that is submitted to it to report. Both IDs were mucked with, what did it, I can't even guess. I don't believe it was the event log obviously and I am not really of the opinion it is ADUC either. We could guess for days at what it is and never hit it, it will require digging in and looking at the system closely to see if you can find other things that seem to fit the pattern.

—  
Joe Richards Microsoft MVP Windows Server Directory Services  
Author of O'Reilly Active Directory Third Edition  
[www.joeware.net](http://www.joeware.net)

—O'Reilly Active Directory Third Edition now available—

<http://www.joeware.net/win/ad3e.htm>

zexmarquis wrote:

Joe,

Thank you again for your prompt reply, however i do not believe the event log is at the heart of the problem in light of the fact that the event log is no more than a "passive" component of the system whole whose purpose is to display information passed to it in a readable format.

Being of a rational disposition I will not totally dismiss the possibility of an event log "malfunction", but I will also not concede to the idea of the aforementioned "hiccup" until all other avenues have been explored. It is not rational to excuse ADUC from the list of possible culprits based solely on an argument of pure speculation. A statement like, "... I indirectly support millions and i've never seen it so it doesn't exist...", does not constitute an alibi of any considerable merit.

Again, I do thank you and your millions of quasi-clients for your contribution to this effort but the inquiry goes on.

## Re: Unexplained User Account Deletion

Good luck on your Third Edition.

Joe Richards [MVP] wrote:

I have not ever seen a case where you delete one ID and two IDs get deleted. It is possible the GUI could screw up but unlikely if you are talking about ADUC as I would expect to hear a lot of that as I indirectly support millions of users through work and indirectly support multi-millions through joeware questions and newsgroups.

As for the events and how they come in, I don't really study the event logs, I don't much care for the whole system. What I tend to do for work is put provisioning tools into place and no one really manages AD directly, they request things through the tool and everything is logged that way.

--

Joe Richards Microsoft MVP Windows Server Directory Services  
Author of O'Reilly Active Directory Third Edition  
[www.joeware.net](http://www.joeware.net)

---O'Reilly Active Directory Third Edition now available---

<http://www.joeware.net/win/ad3e.htm>

zexmarquis wrote:

Joe,

Thanks for replying. I did not mean for you to take the 'modified GUID' statement literally, however I am referring to the DEL: appended to the beginning of the GUID when generated in the event.

Moving on, in your experience, have you seen the issue i've described or can you provide a viable explanation as to why this may have occurred?

Joe Richards [MVP] wrote:

What you mean generates a modified GUID? The object GUID does not change during a "delete", it is maintained through the tombstone process.

Re: Unexplained User Account Deletion

---

Joe Richards Microsoft MVP Windows  
Server Directory Services  
Author of O'Reilly Active Directory Third  
Edition  
[www.joeware.net](http://www.joeware.net)

---O'Reilly Active Directory Third Edition  
now available---

<http://www.joeware.net/win/ad3e.htm>

michael\_gore718@xxxxxxxxx wrote:

So here's an iffy one. Turns  
out a user account was  
deleted and  
everything is pointing  
towards me. However I  
don't recall deleting the

account, then confirming the  
deletion, and confirming the  
deletion of  
the associated mailbox.  
Heres the info from the  
Event logs, the header

is the same for both events:

Header>>

Date: 12/13/06  
Source: Security  
Time: 4:18:35 PM  
Category: Account Mgmt  
Type: Success A  
Event ID: 630

This is the event in  
question>>

User Account Deleted:  
Target Account Name:  
User1

Re: Unexplained User Account Deletion

Target Domain: DOMAIN  
Target Account ID:  
DOMAIN\User1  
Caller User Name: admin  
Caller Domain: DOMAIN  
Caller Logon ID:  
(0x0,0x64390BE)  
Privileges: -

Here is the account I was  
working on at the time>>

User Account Deleted:  
Target Account Name:  
User2  
Target Domain: DOMAIN  
Target Account ID: User2  
DEL:d006b3a0-09de-45f2-8393-ba47246b8ea8  
Caller User Name: admin  
Caller Domain: DOMAIN  
Caller Logon ID:  
(0x0,0x64390BE)  
Privileges:

Right off the back i'm sure  
you can tell that something  
is missing.  
**WHERE IS THE GUID?** It's  
been my experience that a  
deleted account  
generates a modified GUID.  
Im not sure why the GUID  
was not generated  
in the event. Can anyone  
explain this?

Another bit of information,  
the two events were  
timestamped for exactly

4:18:35 PM. Any help on  
this will be appreciated.

Re: Unexplained User Account Deletion