

## Re: Security Event Id 552

**Source:**

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2005-02/7704.html>

---

**From:** CharlieFoxytrot (*CharlieFoxytrot\_at\_discussions.microsoft.com*)

**Date:** 02/24/05

Date: Thu, 24 Feb 2005 15:13:02 -0800

One more thing that may be significant: all of these spurious events seem to have the same GUID

"CharlieFoxytrot" wrote:

> okay, the system administrator's GUID doesn't match the GUID in the event log.

>

> also, the GUID in the event log doesn't appear in a registry search.

>

>

> "Cris Hanna [SBS-MVP]" wrote:

>

>> well did you check the renamed accounts GUID?

>>

>> Also search the registry for the GUID in event log

>>

>> --

>> Cris Hanna [SBS-MVP]

>> Small Business Server Specialist

>> The Trinity Companies – Microsoft Gold Partner

>> St. Louis, MO

>> [www.trinitycos.com](http://www.trinitycos.com)

>>

---

>> Please only respond in the newsgroup and not to me directly so that all can benefit from the information

>> SBS 2003 – [microsoft.public.windows.server.sbs](mailto:microsoft.public.windows.server.sbs)

>> SBS 2000 – [microsoft.public.backoffice.smallbiz2000](mailto:microsoft.public.backoffice.smallbiz2000)

>> SBS 4.5 – [microsoft.public.backoffice.smallbiz](mailto:microsoft.public.backoffice.smallbiz)

>> "CharlieFoxytrot" <[CharlieFoxytrot@discussions.microsoft.com](mailto:CharlieFoxytrot@discussions.microsoft.com)> wrote in message <news:3465542E-2258-45D9-BD1C-A7B8F58FCEB3@microsoft.com...>

>> Cris,

>> Thanks for the reply...

>> We have installed the Res kit and registered the Acctinfo.dll. However, the

>> Administrator account doesn't appear in the SBSUsers folder since we renamed

>> the account. Administrator does appear in the Builtin folder, but the

>> "additional account info" tab doesn't show up on that window. Any other way

>> to check the Administrator GUID? Would I have to reverse the renaming?

>>

>> *I should have mentioned before that these events are appearing in the security folder at a rate of about \*8 per second\* on a 30 node network.*

>>

>> *Thanks again,*

>> *bill*

>>

>> *"Cris Hanna [SBS-MVP]" wrote:*

>>

>>> *do you have access to the Windows Server 2003 resource kit?*

>>>

>>> *If not you can download it here*

>>>

<http://www.microsoft.com/downloads/details.aspx?familyid=9d467a69-57ff-4ae7-96ee-b18c4790cffd&displaylang>

>>>

>>>

>>> *There is a neat tool in there called Acctinfo.dll*

>>> *among other things when you look at the properties of a user (Administrator for instance) you can see the Logon GUID. Match that with what your seeing in the event log.*

>>>

>>> *This could be a System Account for a service*

>>>

>>> *--*

>>> *Cris Hanna [SBS-MVP]*

>>> *Small Business Server Specialist*

>>> *The Trinity Companies – Microsoft Gold Partner*

>>> *St. Louis, MO*

>>> *www.trinitycos.com*

>>>

-----  
>>> *Please only respond in the newsgoup and not to me directly so that all can benefit from the information*

>>> *SBS 2003 – microsoft.public.windows.server.sbs*

>>> *SBS 2000 – microsoft.public.backoffice.smallbiz2000*

>>> *SBS 4.5 – microsoft.public.backoffice.smallbiz*

>>> *"CharlieFoxytrot" <CharlieFoxytrot@discussions.microsoft.com> wrote in message news:4D4B596F-6B61-4C8B-A7ED-0E791A5F39DC@microsoft.com...*

>>> *This may be an issue but I clearly don't have a clue...*

>>>

>>> *I'm getting numerous events like this one:*

>>> *Category: Logon/Logoff Type: Success A Event ID 552*

>>> *User: WSDBW\System Administrator*

>>>

>>> *Logon attempt using explicit credentials:*

>>> *Logged on user:*

>>> *User Name: System Administrator*

>>> *Domain: WSDBW*

>>> *Logon ID: (0x0,0x98CC38)*

>>> *Logon GUID: {0099da6c-7849-b704-7725-5e0f89f7e02a}*

>>> *User whose credentials were used:*

>>> *Target User Name: Guest*

>>> *Target Domain: WSDBW*

> > > *Target Logon GUID: –*  
> > >  
> > > *Target Server Name: ns1.Worldlan.com*  
> > > *Target Server Info: ns1.Worldlan.com*  
> > > *Caller Process ID: 4*  
> > > *Source Network Address: –*  
> > > *Source Port: –*  
> > >  
> > > *We have renamed the Guest and Administrator account per article 816109.*  
> > > *Should I worry about this? Are we vulnerable? Should I unplug the router and*  
> > > *call it a day?*  
> > >  
> > > *Thanks for your advice!*  
> > > *Bill*