

# Re: audit user activity

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2006-03/msg03329.html>

---

- *From:* [v-criminal@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:v-criminal@xxxxxxxxxxxxxxxxxxxxxxxx) ("Crina Li")
  - *Date:* Wed, 15 Mar 2006 08:11:05 GMT
- 

Hi Andrea,

Thanks for your update.

After you have set the needed file auditing for create and delete events, you can set filter to view the Security log for a particular user.

To filter Security log events, follow these steps:

1. Open Event Viewer snap-in through Administrator Tools.
2. In the console tree, expand Event Viewer, and then right click the Security and select Properties.
3. Click Filter tab and then specify the filter options that you want (the user name), and then click OK.

Only events that match your filter criteria are displayed in the details pane.

To return the view to display all log entries, click Filter on the View menu, and then click Restore Defaults.

To see if a user moves a file from a folder to another of shares that you are monitoring, you can see the copy and delete logs for the file.

If you have any question, please feel free to let me know.

I appreciate your time and look forward to hearing from you.

Best regards,

Crina Li (MSFT)

Microsoft CSS Online Newsgroup Support

Get Secure! – [www.microsoft.com/security](http://www.microsoft.com/security)

=====  
This newsgroup only focuses on SBS technical issues. If you have issues

Re: audit user activity

regarding other Microsoft products, you'd better post in the corresponding newsgroups so that they can be resolved in an efficient and timely manner. You can locate the newsgroup here:

<http://www.microsoft.com/communities/newsgroups/en-us/default.aspx>

When opening a new thread via the web interface, we recommend you check the "Notify me of replies" box to receive e-mail notifications when there are any updates in your thread. When responding to posts via your newsreader, please "Reply to Group" so that others may learn and benefit from your issue.

Microsoft engineers can only focus on one issue per thread. Although we provide other information for your reference, we recommend you post different incidents in different threads to keep the thread clean. In doing so, it will ensure your issues are resolved in a timely manner.

For urgent issues, you may want to contact Microsoft CSS directly. Please check <http://support.microsoft.com> for regional support phone numbers.

Any input or comments in this thread are highly appreciated.

=====

This posting is provided "AS IS" with no warranties, and confers no rights.

-----  
| Reply-To: "Andrea Racca" <raccaNOSPAMlibero.it>  
| From: "Andrea Racca" <raccaNOSPAMlibero.it>  
| References: <OsrkQxrRGHA.5900@xxxxxxxxxxxxxxxxxxxxxx>  
<h2K0RPzRGHA.5524@xxxxxxxxxxxxxxxxxxxxxx>  
| Subject: Re: audit user activity  
| Date: Tue, 14 Mar 2006 16:11:02 +0100  
| Lines: 146  
| X-Priority: 3  
| X-MSMail-Priority: Normal  
| X-Newsreader: Microsoft Outlook Express 6.00.2900.2180  
| X-RFC2646: Format=Flowed; Original  
| X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2180  
| Message-ID: <uOxYIm3RGHA.5552@xxxxxxxxxxxxxxxxxxxxxx>  
| Newsgroups: microsoft.public.windows.server.sbs  
| NNTP-Posting-Host: host2-152.pool8020.interbusiness.it 80.20.152.2  
| Path: TK2MSFTNGXA03.phx.gbl!TK2MSFTNGP08.phx.gbl!TK2MSFTNGP14.phx.gbl  
| Xref: TK2MSFTNGXA03.phx.gbl microsoft.public.windows.server.sbs:252551  
| X-Tomcat-NG: microsoft.public.windows.server.sbs  
|  
| Hi,  
| thank you very much for your documentation.  
| I followed your step and now I'd like to see if a user move a file from a  
| folder to another of shares that I'm monitoring..  
| It's possible??  
| Where I can read this?  
| hi

Re: audit user activity

Re: audit user activity

|  
| ""Crina Li"" <v-crinal@xxxxxxxxxxxxxxxxxxxxxx> ha scritto nel messaggio  
| [news:h2K0RPzRGHA.5524@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:h2K0RPzRGHA.5524@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)  
| > Hi Andrea,  
| >  
| > Thank you for posting in SBS newsgroup.  
| >  
| > According to your description, I understand that you would like to know  
| > how  
| > to log the access or change to the shared folders on SBS. If I have  
| > misunderstood your concerns, please do not hesitate to let me know.  
| >  
| > As I know, you can enable Audit log in Event log on SBS:  
| >  
| > 1. Click Start, click Run, type "gpmmc.msc" and click OK.  
| > 2. Expand Domains -> your domain -> Domain Controllers.  
| > 3. Right-click Small Business Server Auditing Policy and click Edit.  
| > 4. Expand Computer Configuration -> Windows Settings -> Security  
Settings  
| > -> Local Policies -> Audit Policy.  
| > 5. In the right pane, double-click "Audit object access".  
| > 6. To audit successful access of specified files, folders, select the  
| > Success check box.  
| > 7. To audit unsuccessful access to these objects, select the Failure  
check  
| > box.  
| > 8. To enable auditing of both, select both check boxes.  
| > 9. Click OK.  
| > 10. Run "gpupdate /force" or restart the computer so that the policy  
takes  
| > effect on SBS.  
| >  
| > After you enable auditing, you need to specify the files, folders that  
you  
| > want audited. To do so:  
| >  
| > 1. In Windows Explorer, locate the file or folder you want to audit.  
| > 2. Right-click the file, folder that you want to audit, and then click  
| > Properties.  
| > 3. Click the Security tab, and then click Advanced.  
| > 4. Click the Auditing tab, and then click Add.  
| > 5. In the "Enter the object name to select" box, type the name of the  
user  
| > or group whose access you want to audit. You can browse the computer for  
| > names by clicking Advanced, and then clicking Find Now in the "Select  
User  
| > or Group" dialog box.  
| > 6. Click OK.  
| > 7. Select the Successful or Failed check boxes for the actions you want  
to  
| > audit, and then click OK.

Re: audit user activity

Re: audit user activity

|> 8. Click OK, and then click OK.  
|>  
|> After that, you may check the Security event log to find the info you  
|> want.  
|>  
|> Please Note: Frankly, checking the security event log to track which  
user  
|> update certain public folder is not an easy way since there are bunch of  
|> logs there.  
|>  
|> More information:  
|>  
|> 174073 Auditing User Authentication  
|> <http://support.microsoft.com/?id=174073>  
|>  
|> Securing Your Windows Small Business Server 2003 Network  
|>  
[http://www.microsoft.com/downloads/details.aspx?familyid=f62b2722-267c-4642-](http://www.microsoft.com/downloads/details.aspx?familyid=f62b2722-267c-4642-b287-c31115ef10a4&displaylang=en)  
|> [b287-c31115ef10a4&displaylang=en](http://www.microsoft.com/downloads/details.aspx?familyid=f62b2722-267c-4642-b287-c31115ef10a4&displaylang=en)  
|>  
|> Using Audit Policies to Secure Your Windows 2000 Network  
|>  
<http://whidbey.msdn.microsoft.com/library/default.asp?url=/library/en-us/dne>  
|> [xnt00/html/ewn0054.asp](http://whidbey.msdn.microsoft.com/library/default.asp?url=/library/en-us/dne)  
|>  
|> I hope the above information helps. If you have any questions or  
concerns,  
|> please do not hesitate to let me know.  
|>  
|> Thanks for your time and I look forward to your reply.  
|>  
|> Best regards,  
|>  
|> Crina Li (MSFT)  
|>  
|> Microsoft CSS Online Newsgroup Support  
|>  
|> Get Secure! – [www.microsoft.com/security](http://www.microsoft.com/security)  
|>  
|> =====  
|> This newsgroup only focuses on SBS technical issues. If you have issues  
|> regarding other Microsoft products, you'd better post in the  
corresponding  
|> newsgroups so that they can be resolved in an efficient and timely  
manner.  
|> You can locate the newsgroup here:  
|> <http://www.microsoft.com/communities/newsgroups/en-us/default.aspx>  
|>  
|> When opening a new thread via the web interface, we recommend you check  
|> the  
|> "Notify me of replies" box to receive e-mail notifications when there

Re: audit user activity

Re: audit user activity

are

> any updates in your thread. When responding to posts via your newsreader,

> please "Reply to Group" so that others may learn and benefit from your issue.

>

> Microsoft engineers can only focus on one issue per thread. Although we

> provide other information for your reference, we recommend you post

> different incidents in different threads to keep the thread clean. In

> doing

> so, it will ensure your issues are resolved in a timely manner.

>

> For urgent issues, you may want to contact Microsoft CSS directly.

Please

> check <http://support.microsoft.com> for regional support phone numbers.

>

> Any input or comments in this thread are highly appreciated.

>

> =====

>

> This posting is provided "AS IS" with no warranties, and confers no

> rights.

> -----

> | Reply-To: "Andrea Racca" <raccaNOSPAMlibero.it>

> | From: "Andrea Racca" <raccaNOSPAMlibero.it>

> | Subject: audit user activity

> | Date: Mon, 13 Mar 2006 17:36:42 +0100

> | Lines: 9

> | X-Priority: 3

> | X-MSMail-Priority: Normal

> | X-Newsreader: Microsoft Outlook Express 6.00.2900.2180

> | X-RFC2646: Format=Flowed; Original

> | X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2180

> | Message-ID: <OsrkQxrRGHA.5900@xxxxxxxxxxxxxxxxxxxxxx>

> | Newsgroups: microsoft.public.windows.server.sbs

> | NNTP-Posting-Host: host2-152.pool8020.interbusiness.it 80.20.152.2

> | Path: TK2MSFTNGXA03.phx.gbl!TK2MSFTNGP08.phx.gbl!tk2msftngp13.phx.gbl

> | Xref: TK2MSFTNGXA03.phx.gbl microsoft.public.windows.server.sbs:252193

> | X-Tomcat-NG: microsoft.public.windows.server.sbs

> |

> | Hi,

> | I need to audit user activity on SBS 2003. My problem is that i like

to

> | understand who move files, delete file from network share.

> | Is there any tools to do it? And also: performance risk to go down if

I

> | active it? Thank's a lot..

> |

> | andrea

> |

> |

Re: audit user activity

Re: audit user activity

|> |  
|>  
|  
|  
|  
.