

# Re: Bad login alerts

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2007-08/msg02481.html>

---

- *From:* "Teneo" <not@xxxxxxx>
  - *Date:* Fri, 17 Aug 2007 15:25:04 +0100
- 

Hello Robert

Thank you for your post.

I think there is a little confusion, I am aware of a RDP unsuccessful attempt but my post was enquiring about the log entry with the DOC MAIL in the security log.

I am wondering what type of connection my original example is as there is very little information presented. My second example showed an unsuccessful RDP connection which gives us a lot of useful information and I would like to add that an external unsuccessful RDP connection does give the source network address. This has been very useful tracking down infected server/pcs.

"Robert Li [MSFT]" <v-robali@xxxxxxxxxxxxxxxxxxxxxx> wrote in message <news:7IC5mTM4HHA.2340@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Hi Sasha,

Thanks for sharing your wonderful experience here.

When a unsuccessful RWW or RDP logon occurs, Event ID 529 is recorded in the Security log. In the logs, you can see the following content:

Logon Failure:  
Reason: Unknown user name or bad password  
User Name: DOC-MAIL\$  
Domain: DOC  
Logon Type: 3  
Logon Process: NtLmSsp  
Authentication Package: NTLM  
Workstation Name: DOC-MAIL  
Caller User Name: -  
Caller Domain: -

## Re: Bad login alerts

Caller Logon ID: –  
Caller Process ID: –  
Transited Services: –  
Source Network Address: –  
Source Port: –

When you RDP to server from Internet, this is expected behavior, because the firewall get rid of the information of Source Network Address, Source Port and so on. When you RDP from internal, you can see Source Network Address, Source Port, because the traffic doesn't pass firewall.

Logon Failure:  
Reason: Unknown user name or bad password  
User Name: aaaaaaaaa  
Domain: SERVER  
Logon Type: 3  
Logon Process: Advapi  
Authentication Package: Negotiate  
Workstation Name: SERVER  
Caller User Name: IUSR\_SERVER

The RWW depends on IIS, all the logon attempt starts from IIS, not from client workstation, so you can see the server is SERVER and user name is IUSR\_SERVER.

I'd like to give you more information on the process NTLMSSP and Advapi.

NTLMSSP is a security support provider that is available on all versions of DCOM. It uses the Microsoft Windows NT LAN Manager (NTLM) protocol for authentication. NTLM never actually transmits the user's password to the server during authentication.

More info:

NTLMSSP  
<http://msdn2.microsoft.com/en-us/library/ms691272.aspx>

Process Advapi is triggered by a call to LogonUser; LogonUser calls LsaLogonUser, and one of the arguments to LsaLogonUser, OriginName, identifies the origin of the logon attempt.

More info:

How to troubleshoot Kerberos-related issues in IIS  
<http://support.microsoft.com/kb/326985>

Hope this helps.

If you have any concern on this issue, please don't hesitate to let me know.

Re: Bad login alerts

Best regards,

Robert 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 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.

-----  
<From: "Sasha" <news@xxxxxxxxxx>  
<Subject: Bad login alerts  
<Date: Thu, 16 Aug 2007 19:27:23 +0100  
<Lines: 40  
<X-Priority: 3  
<X-MSMail-Priority: Normal  
<X-Newsreader: Microsoft Outlook Express 6.00.2900.3138  
<X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.3138  
<X-RFC2646: Format=Flowed; Original  
<Message-ID: <Ow4ZWMD4HHA.1824@xxxxxxxxxxxxxxxxxxxxxxxx>

Re: Bad login alerts

<Newsgroups: microsoft.public.windows.server.sbs  
<NNTP-Posting-Host: mail.sxcomputers.co.uk 217.34.35.237  
<Path: TK2MSFTNGHUB02.phx.gbl!TK2MSFTNGP01.phx.gbl!TK2MSFTNGP04.phx.gbl  
<Xref: TK2MSFTNGHUB02.phx.gbl microsoft.public.windows.server.sbs:56935  
<X-Tomcat-NG: microsoft.public.windows.server.sbs  
<  
<Hi all  
<If someone tries an unsuccessful RDP attempt on server much helpful info  
is  
<recorded, especially IP address.  
<Seeing some login alerts of the below where limited info is recorded..  
Its  
<this NtLMSsp logon process  
<  
<Logon Failure:  
<Reason: Unknown user name or bad password  
<User Name: DOC-MAIL\$  
<Domain: DOC  
<Logon Type: 3  
<Logon Process: NtLmSsp  
<Authentication Package: NTLM  
<Workstation Name: DOC-MAIL  
<Caller User Name: -  
<Caller Domain: -  
<Caller Logon ID: -  
<Caller Process ID: -  
<Transited Services: -  
<Source Network Address: -  
<Source Port: -  
<  
<Username / Domain and workstation name have no relation to site where  
server  
<recorded this.  
<  
<I thought it maybe an RWW attempt but this gives:-  
<Logon Failure:  
<Reason: Unknown user name or bad password  
<User Name: aaaaaaaa  
<Domain: SERVER  
<Logon Type: 3  
<Logon Process: Advapi  
<Authentication Package: Negotiate  
<Workstation Name: SERVER  
<Caller User Name: IUSR\_SERVER  
<  
<TIA, have a great day / night depending wherever you are... ;-)  
<  
<  
<  
<

Re: Bad login alerts