

## Re: Single user issue; best troubleshooting

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2006-09/msg01449](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-09/msg01449)

---

- *From:* "Herb Martin" <[news@xxxxxxxxxxxxxxxx](mailto:news@xxxxxxxxxxxxxxxx)>
  - *Date:* Fri, 22 Sep 2006 10:18:22 -0500
- 

Herb, I suspect your comment about the authentication being prompted for versus the credentials configured into Outlook will eventually be proven.

Especially if you have an intermittent network glitch WHICH COULD be cause by that intermediate 'network access' server you are still to be briefed on.

I am guessing the reason for the user being prompted is a secondary server between her workstation and the Exchange server that monitors or controls "network access", but I have not been briefed on our specific network setup yet. This is something I pointed out to my boss yesterday and we are supposed to discuss it today.

As to the...

Is the Exchange server able to pass "NetDiag"? Can all of your DCs pass DCDiag? (Send output to text file, search with text editor for FAIL, WARN, ERROR.)

Unfortunately I do not know the answers to these questions.

If you are not the DOMAIN ADMIN you likely cannot test these anyway, so you will need an Admin's help to complete the troubleshooting of any such DOMAIN problem.

These tools are critical to troubleshooting any domain authentication problem (which usually turns out to be a DNS issue) UNLESS you have a network/firewall outage issue -- which is more likely in your case if you have a goofy network access server with issues.

Re: Single user issue; best troubleshooting

My question to the boss yesterday included an observation that many other organizations I have worked in gave Helpdesk personnel a much higher level of access to server log files and system statuses.

In general I am for minimum access CONSISTENT with doing your job and your knowledge but do frequently recommend "read only" (diagnostic) type access to many places. Win2000 and Win2003 even better can grant things like "read only access to the DNS or DHCP console".

This allows Help desk (etc) to DIAGNOSE or ISOLATE the likely problem before calling an admin who can fix that specific issue (big companies might have different admins for DNS and DHCP servers.)

I hope that I will be able to convincingly prove this would be VERY helpful to us as well in this environment.

Are you allowed to read the Event Viewer on the DCs and servers.

BTW, you do know there is significant logging in Outlook IF you ENABLE it (although I cannot find the option or the view right at the moment so you will need to use Help or Google.)

Thanks for your feedback. I will try and post the eventual outcome in case it is of use to you or anyone else.

Please do.

Remember this is probably MORE than one problem. Maybe related, possibly not.

---

Herb Martin, MCSE, MVP  
Accelerated MCSE  
<http://www.LearnQuick.Com>  
[phone number on web site]

"Dennis the Nerf Herder" <costeaden@xxxxxxxx> wrote in message  
[news:1158927739.874458.46200@xx](mailto:news:1158927739.874458.46200@xx)

Re: Single user issue; best troubleshooting

## Re: Single user issue; best troubleshooting

Herb Martin wrote:

Herb, thanks for the reply. It is helping me to analyze the issue analytically.

The user in this case is (typically) logging in to Outlook 2003 as soon as she has logged onto the desktop. E-mail is an integral part of the person's daily activities, and the profile of her activities includes a shared Calendar (or appointments), at least one public folder in Outlook 2003 and access to several network shared folders which reconnect at logon.

You still haven't indicated which EMAIL SERVER is used. Most email servers other than Exchange will not be using any form of Integrated Authentication and so all of the OUTLOOK generated Password Request boxes would be PURELY outlook based and have nothing to do with AD or logging/authenticating onto the domain.

After launching Outlook the user typically accesses 1 Remote Desktop Connection session to a departmental server, opens Internet Explorer 6.x and launches at least one network-based application. (I need to look at her 'netstat -a' and get a more complete picture of ALL the servers she is connecting to).

Remote Desktops typically pop the logon box every time the connection is lost for more than a few seconds. (There are exceptions but this is normal behavior in general.)

Remote Desktops don't typically use INTEGRATED authentication either but allow the user to possibly logon with differing credentials rather than assuming one identity. So again, separate problem most likely.

The authentication prompts are occurring at "random" intervals and often act as though the password she has entered is wrong and has failed to authenticate (e.g. the login dialog box re-appears almost instantaneously).

For Outlook and SMTP email servers, I think this is a known but irregularly occurring bug, especially if either/both the the

## Re: Single user issue; best troubleshooting

network connection is disconnecting periodically or/and the user is using a different account than they used to logon to the domain.

Notice that "herbm" on some SMTP server is usually not the same as "domain\herbm" on the domain, or even probably "server\herbm" on that SAME server. (This MAY applied to IE and web servers below too.)

And yet on other occasions her password appears to be accepted and the box does not re-appear.

I have seen this in Outlook --- usually when NETWORK connection has FAILED between Outlook and the email server --- I suspect that Outlook assumes a mismatched password when it is really a (temporary) network outage.

Also, Outlook has a known bug wherein the users current logon name (on the domain) will be sent to SMTP servers EVEN THOUGH the user has supplied a different user name and password --- this will fail, and then the one CONFIGURED in Outlook will be used on the next try. (I see regular logon failures on my SMTP servers due to this bug.)

One can easily imagine that the combination of both these problems would produce the logon box: SOMETIMES the network connectivity would fail after the initial logon failure and before the correct credentials are used.

The authentication box is popping up for BOTH her e-mail connection and an Intranet company homepage (as indicated by the server names shown in the title bar of each login dialog box respectively).

Outlook and the web server are probably different problems too.

Which web server do you use (IIS is vastly different in this respect than others)? Do you use IIS with "Integrated Authentication"? Do you use IE SOLELY, as it is the only browser likely to support "integrated authentication"?

Does the app on the intranet server USE this authentication or does it have its own external user database (many apps do, especially if purchased from outside or built by former Unix developers.)?

Re: Single user issue; best troubleshooting

There are many details that are critical be still missing from your analysis.

I also strongly suspect you have MORE than one problem and may need to be very careful about consolidating the symptoms and expecting them to make sense when taken together.

So what I infer from this is either  
her credentials failed to authenticate (incorrect password) or

OR EVEN incorrect ACCOUNT (even if the USER name portion happens to be the same.)

if they are being "cached" (on or off her workstation) that they have 'expired' (for lack of a more accurate word) within a very short period of time. The user can enter her password to connect to the Exchange 5.5 server, read a few e-mails but will get prompted again for her password after about 10 minutes (when she goes to open the next message).

I wish you hadn't buried the reference to Exchange way down here but had indicated that back in the beginning (of the first message.)

Is the Exchange server able to pass "NetDiag"? Can all of your DCs pass DCdiag? (Send output to text file, search with text editor for FAIL, WARN, ERROR.)

I have unchecked "Used Cached Exchange mode" in order to see more detail on what happening, and thinking Outlook would not be suppressing any background events. Maybe this was a bad move and unchecking Cached Exchange mode was the wrong thing to do.

Outlook also has logging you can enable -- see help.

The issue is bugging me and I know the user is itching for it to be resolved, as is her boss!

A more complete list of Event Log events includes:  
1030, 40961, 11197, 63, 40960, 31 and an Outlook error

Re: Single user issue; best troubleshooting

code 0x80040115 which seems to have between 3 and 18 possible causes (or combinations thereof).

Research these at EventID.net which is usually better than search directly at Microsoft even by using Google.

Thanks in advance for considering my additional information.

--  
Herb

"Dennis the Nerf Herder" <costeaden@xxxxxxxx> wrote in message [news:1158845418.863232.306460@xx](mailto:news:1158845418.863232.306460@xx)

Herb Martin wrote:

"Dennis the Nerf Herder"  
<costeaden@xxxxxxxx> wrote in message  
[news:1158807522.640301.175060@xx](mailto:news:1158807522.640301.175060@xx)

Can anyone recommend the best steps for isolating the trouble when a single user account repeatedly prompts for authentication?

Start by figuring out which APPLICATION is causing this.

Once a user logs onto a computer in a domain the user is practically never prompted for authentication credentials again, unless some application is not fully integrated with AD/Windows (i.e., some web servers or some web clients.)

I have devoted considerable time and effort to isolating the cause of a case like this, but have not

Re: Single user issue; best troubleshooting

YET removed the user from  
Active  
Directory  
and recreated her account.

When does it happen precisely? What is the  
precise nature  
of the prompt?

Is the user fully authenticated on the domain  
prior to the prompt?

What is the user doing at the time of the  
prompt? Including the  
application that is running and any servers  
being accessed.

That's not especially my job,  
since the  
user "should not" be having  
a problem to begin with.  
However, I  
have  
backed up her account  
(Outlook 2003 .pst files,  
Favorites and "My  
Documents") and retored  
same to a completely  
re-imaged (Ghost)  
Windows  
XP workstation, and yet the  
problem continues.

Is this happing while accessing Exchange or  
some email server?

IF the email server is not AD Integrated  
(usually Exchange would  
be for most email functions) then this would  
be a common issue  
for Outlook not having her  
username/password stored correctly or  
some (apparent) bugs that Outlook  
experiences.

This occurs most commonly with SMTP or  
POP servers that are  
NOT running Exchange (or other integrated

Re: Single user issue; best troubleshooting

authentication.)

[I have seen this bug and can usually make it go away but I don't know the full story just some of the issues and fixes that seem to work.]

We have seen 40690, 40691, 1030 and other events captured in Event Viewer but as helpdesk technicians are not familiar with "behind the scenes" workings of Active Directory (e.g. we have not been as fully trained as the Admins., etc).

It is unlikely to be an AD issue from what you have written.

If it is a Domain (AD) authentication error then it is likely a DNS issue at heart.

Furthermore I have been casually (not officially) told the user's account must be removed from Active Directory for 24 hours and then restored (or re-created), and this seems a lengthy investment in time and patience for an uncertain outcome. In other words, I would hate to do it and NOT have the problem resolved.

Who told you that and why? (There is no troubleshooting reason of which I am aware. Sounds like

Re: Single user issue; best troubleshooting

superstition.)

So if there exists a checklist of things to examine or a "best practices" page related to things that go wrong with user accounts, I would very much like to know about it.

User platform: Windows XP  
Service Pack level: 2  
Office 2003 level: 2  
Outlook 2003 level: 2  
Environment: Windows Server 2003  
Env. size: 4,000 – 5,000 (users total)  
(with a couple of hundred at the user's building/site)

Kerberos/NTLM authentication seemed to be failing 50% of the time on "Directory" as shown in Outlook 2003's "Connection Status" window, so we switched to "NTLM" alone and the failed attempts dropped to 2 in a 1,000 (also switching to "Mail" from "Directory"). Does this mean something significant?

Any direction on this is very much appreciated. I'm not placing blame or pointing fingers towards any administrator, specific feature of, or inherent quality of Active Directory. I just want to FIX the user

Re: Single user issue; best troubleshooting

and  
KNOW (or learn) what went  
wrong.

Is this possible? It must be.

We need much better specifics on the exact  
problem.

--

Herb Martin, MCSE, MVP  
Accelerated MCSE  
<http://www.LearnQuick.Com>  
[phone number on web site]