

# Re: Disable Kerberos in a Windows Server 2003 Environment

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2007-11/msg01393](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-11/msg01393)

---

- *From:* "Joe Kaplan" <[joseph.e.kaplan@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:joseph.e.kaplan@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Tue, 27 Nov 2007 09:38:43 -0600
- 

Sure thing. I'm going to be away for about a week, so if you post while I'm gone, hopefully someone else can help. There are also some hardcore Kerberos experts who hang out on the activedir.org mailing list that can probably give you good advice as well.

Best of luck!

Joe K.

--

Joe Kaplan-MS MVP Directory Services Programming  
Co-author of "The .NET Developer's Guide to Directory Services Programming"  
<http://www.directoryprogramming.net>

--

"JerryAMWE" <[JerryAMWE@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:JerryAMWE@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)> wrote in message [news:E1F94083-1F3D-4ED2-8E81-A2DBF97D37B0@xxxxxxxxxxxxxxxxxxxx](mailto:news:E1F94083-1F3D-4ED2-8E81-A2DBF97D37B0@xxxxxxxxxxxxxxxxxxxx)

Thanks Joe! I will investigate this further and try to determine if there is a specific service that they are running for single-signon. If this ends up going any further, I will re-post. Thanks again for all of your help, it is very much appreciated.

Thanks  
Gerry

"Joe Kaplan" wrote:

Without more details on what he's doing and what he really needs, I can't give you a satisfying answer. It is definitely possible to prevent Kerberos authentication to a given service by making sure the service principal name (SPN) for the service is not published in the directory. If no SPN

Re: Disable Kerberos in a Windows Server 2003 Environment

exists  
for a given service, Kerberos auth to it is not possible.

However, we don't know enough about what is going on here to know if that might be a viable option.

Joe K.

--

Joe Kaplan—MS MVP Directory Services Programming  
Co—author of "The .NET Developer's Guide to Directory Services  
Programming"  
<http://www.directoryprogramming.net>

--

"JerryAMWE" <JerryAMWE@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in  
message  
<news:21F92E8D-9D75-4996-A830-38EFC9D52F8@xxxxxxxxxxxxxxxxxxxx>

I'm not sure why our HIS system requires NTLM for  
single—signon  
authentication. You have raised an interesting question  
though; can I  
specify his servers/app to use NTLM and leave the rest of my  
environment  
alone? If so, how?

Thanks  
Gerry

"Joe Kaplan" wrote:

Do you have any detailed information about  
why his product requires  
NTLM  
only? Is it possible that this product will  
work if it does NTLM auth  
to  
just those specific apps, but still uses  
Kerberos in general?

I'm not even sure if it is possible, but ou  
really don't want to try  
to  
get  
rid of Kerb across the board.

Joe K.

--

Joe Kaplan—MS MVP Directory Services

Re: Disable Kerberos in a Windows Server 2003 Environment

Programming  
Co-author of "The .NET Developer's Guide  
to Directory Services  
Programming"  
<http://www.directoryprogramming.net>

--  
"JerryAMWE"  
<JerryAMWE@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>  
wrote in message  
<news:7439B34C-0BAB-4FA0-816D-44DB88B14210@xxxxxxxxxxxxxxxxxxxx>

Hi,

We are a hospital running a Microsoft Server 2003 environment with Microsoft Exchange, Citrix and a few other vendor applications that integrate with Active Directory for authentication. We are at the highest possible functional level in our environment. We also have a Hospital Information System which is the most important system we have. Our systems engineer wants to try to get our HIS system to use it's native single-signon capability to authenticate users to AD. The problem is that he wants me to disable Kerberos and only use NTLM authentication. My questions are:

1. Can I disable Kerberos even though my functional level is at its highest level?

Re: Disable Kerberos in a Windows Server 2003 Environment

2. If so, how do I do this?
3. Are there any consequences by me doing this? (i.e. Exchange authentication issues, Citrix authentication issues, time-services, DNS issues, etc....)

Any help/advice would greatly be appreciated.

Thanks,  
Gerry