

Re: Add Windows User to ADAM Role using LDIFDE.exe

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-01/msg01583

- *From:* "Joe Richards [MVP]" <humorexpress@xxxxxxxxxxxx>
 - *Date:* Fri, 19 Jan 2007 19:22:23 -0500
-

Note you can use admod to do this right at the command line without the encoding.

```
admod -h server:port -b group_dn "member:+:<SID=Blah>"
```

Joe Richards Microsoft MVP Windows Server Directory Services
Author of O'Reilly Active Directory Third Edition
www.joeware.net

---O'Reilly Active Directory Third Edition now available---

<http://www.joeware.net/win/ad3e.htm>

Jeremy Wiebe wrote:

Hi Lee,

Thanks for the response. I missed the part that you have to encode the "<SID=XYZ>". I gave that a quick try and that works!

As to the existing foreignSecurityPrincipal collision, I don't think that should ever be an issue because I'm always importing into a brand new application partition.

Thanks for the help!

Jeremy Wiebe

On Jan 19, 3:20 pm, "Lee Flight" <l...@xxxxxxxxxxxxxxxx> wrote:

Hi

unfortunately <SID=...> syntax only works with base64 encoding the #member line in Dmitri's post indicates a comment. More here:

Re: Add Windows User to ADAM Role using LDIFDE.exe

<http://groups.google.com/group/microsoft.public.windows.server.active...>

Note that if you having been testing this by against your ADAM instance and already imported the Windows user the foreignSecurityPrincipal will have already been created in your ADAM instance and that will cause a violation when you try the ldf import even using the correct encoding. For a clean test delete any matching FSP, the ldf import will create it for you as you say.

Lee Flight

"Jeremy Wiebe" <jeremy.wi...@xxxxxxxxxx> wrote in
messagenews:1169228507.640926.157200@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

I'm trying to add a Windows user to an ADAM role by creating an LDIF file and importing it into ADAM using ldifde.exe. I found this post which seems to be exactly what I need, but I can't get it to work ([http://groups.google.ca/group/microsoft.public.windows.server.active ...](http://groups.google.ca/group/microsoft.public.windows.server.active...)).

Here's my LDIF file:
dn:
CN=Readers,CN=Roles,CN=MyApp,DC=MyCompany,DC=COM
changetype: modify
add: member
member:
<SID=S-1-5-21-1644491937-113007714-1957994488-1007>
-

I got the SID by manually adding a windows user to a role using ADAM-AdsiEdit and then exporting that role using ldifde.exe

The error I'm getting is:

===

There is a syntax error in the input file
Failed on line 5. The last token starts with 'm'.
An error has occurred in the program

===

In the post I mentioned above Dmitri's (last poster) LDIF specifies the SID using both the <SID=XYZ> and base64 encoded method. Is that required? (If it is, I couldn't get that working either). So, am I missing something obvious here or does LDIFDE.exe actually not support this?
Also, I'm under the impression that LDIFDE.exe (or

Re: Add Windows User to ADAM Role using LDIFDE.exe

probably ADAM) will
automatically create a ForeignSecurityPrincipal for me, if
needed, when
I add the user to the role.