

Re: LDIFDE Error when trying to change passwords.

## Re: LDIFDE Error when trying to change passwords.

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2006-10/msg00363](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-10/msg00363)

---

- *From:* "Joe Kaplan" <[joseph.e.kaplan@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:joseph.e.kaplan@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Mon, 2 Oct 2006 10:41:36 -0500
- 

Add the -h switch to that.

```
C:\CSV:ldifde -i -f -h chPwd.ldif -j c:\csv
```

The SASL bind (with -b and specific credentials) is only needed if you don't want to use the credentials of the logged on user. Since you probably logged on as DA, that will be fine. LDIF defaults to do a SASL bind with the current user's credentials if none are specified.

The -h adds the encryption. That should allow password mod operations on 2K3 DCs.

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>

--

"JBaxter" <[JBaxter@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:JBaxter@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)> wrote in message  
[news:EF4EF876-D0EA-4219-9101-F0B9ADEFBDC1@xxxxxxxxxxxxxxxxxxxx](mailto:news:EF4EF876-D0EA-4219-9101-F0B9ADEFBDC1@xxxxxxxxxxxxxxxxxxxx)

Which command would you like to see, I do not have an example of the SSAL command or the bind command as I am not sure how to use them. The command that I am using for the ldifde is standard and works as long as I do not try to change the password.

```
C:\CSV:ldifde -i -f chPwd.ldif -j c:\csv
```

Importing users works fine, otherwise I get the error "a device attached to the system is not functioning"

"Joe Kaplan" wrote:

Can you show the command line you are trying to use? If you are running this from the DC (presumably logged in as the DA), you don't actually

Re: LDIFDE Error when trying to change passwords.

Re: LDIFDE Error when trying to change passwords.

need  
to provide credentials. By default, LDIFDE will bind with the current  
credentials using SSPI. The -h argument is the key one, as that enables  
encryption.

As long as the clients and servers are 2003, the domain/forest mode  
should  
not matter here. The higher encryption strength of SSPI in Win2K3 (and  
XP)  
is a function of the improvements made to SSPI at the OS layer and not a  
DC-specific thing. SSPI is a general mechanism for remotely  
authenticating  
clients using different protocols and establishing a secured network  
connection between them which is used by tons of other services in  
Windows,  
not just AD/LDAP.

One thing I'm not certain about is whether the encryption actually kicks  
in  
when the traffic doesn't leave the machine. I think it does in this  
case,  
but you want to be sure. You might consider running LDIF from a member  
server instead to be sure (logged in as DA or preferably called by using  
Runas; logging in as DA is generally not a good idea).

HTH,

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>

--

"JBaxter" <JBaxter@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message  
<news:48074FCA-F772-43E4-A87C-3FA1859742FD@xxxxxxxxxxxxxxxxxxxx>

I have looked over the SSAL bind options but I cannot seem  
to figure it  
out,  
any chance you can give me an example of what the  
command is, I am  
doing  
the  
import directly from the server via a command prompt, the  
only reason I  
am  
trying the LDIFDE is that I cannot import the passwords  
with my CSVDE  
file.

Re: LDIFDE Error when trying to change passwords.

the Server all of my servers in this domain are 2k3. Another question is do they have to be running in 2k3 mode or is 2000 native ok for mixed environs, or does it matter at all.

"Joe Kaplan" wrote:

Ok, there are a few things. I'm not sure exactly why you are getting the error you are getting, but your value is definitely wrong.

The value you have specified is this:  
"cGFzc3dvcnQ="

That is a base64 encoded value of the ASCII (or possibly UTF8 or 1252) encoding of the string "password". You have then enclosed that in quotes.

That is not correct. You need to take the password string, enclose it in quotes, convert the entire value to binary using UNICODE encoding, and base64 that value. Using the same password value:

password

Enclose in quotes

"password"

Convert to binary using Unicode encoding (shown as hex pairs; notice the double bytes and the quote characters 22-00?)

22-00-70-00-61-00-73-00-73-00-77-00-6F-00-72-00-64-00-22-00

Convert binary to Base64:

IgBwAGEAcwBzAHcAbwByAGQAIgA=

Re: LDIFDE Error when trying to change passwords.

To get the encrypted channel, you can either use SSL like the article suggests, or if you have 2K3 DCs and your client is also XP or higher, you can use SSPI bind and the `-h` option with LDIF to encrypt the connection after bind. If you are supplying credentials on the commandline, you need to use the `-b` option.

If you are having trouble with the unicode or base64 conversion, you may need to get a better utility. I have a little thing I wrote in .NET that helps with this that I could share offline if you need it.

Note also that your test password won't work if password complexity is enabled, so make sure you improve that if needed (Password1 is the crappy choice for testing that gets used a lot :)).

Given the error you are getting, you might be having different problems with actually connecting to the directory. Typically, you'll get an "unwilling to process" error message from LDAP if it doesn't like the value you use or you don't have a secure connection.

HTH,

Joe K.

--

Joe Kaplan—MS MVP Directory Services  
Programming  
Co—author of "The .NET Developer's Guide  
to Directory Services

Re: LDIFDE Error when trying to change passwords.

Programming"

<http://www.directoryprogramming.net>

--

"JBaxter"

<JBaxter@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

wrote in message

<news:879F0511-1793-4C4C-AC7A-B98B41919C33@xxxxxxxxxxxxxxxxxxxx>

Thank you for the reply Joe,  
the question is why am I  
receiving the  
error  
that I am

A device attached to the  
system is not functioning,

is it because I am not using  
SSL, here is the code that I  
am using

dn:

CN=testuser,OU=example,DC=example,DC=local

changetype: modify

replace: unicodePwd

unicodePwd:"cGFzc3dvcmQ="

-