

Re: Changing ADAM user password

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-06/msg01719

- *From:* "Joe Kaplan \ (MVP – ADSI)" <joseph.e.kaplan@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Sat, 24 Jun 2006 09:52:18 –0500
-

That's even more interesting. I didn't have an easy way to test that and would not have thought that going "off box" would make a difference, so I would definitely have missed that. I wonder if there is a bug in there though, as I'm pretty sure when doing negotiate auth it works fine on box or off.

Thanks for the extra investigation.

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>
—

"Lee Flight" <lef@xxxxxxxxxxxxxxxx> wrote in message
<news:%23Zq05V2IGHA.4808@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Hi

I just rechecked this on W2K3SP1 and it DOES work. However only in a client server setup: In my first test I connected to the ADAM instance (localhost) and made the digest bind with LDAP_OPT_ENCRYPT=1, the attempted change of password fails with the error I posted.

Running the bind from another W2K3SP1 machine and attempting the same works!

Apologies for the confusion, I have not yet work out why working locally on the instance (as localhost or FQDNS) fails.

Lee Flight

"Dmitri Gavrilov [MSFT]" <dmitrig@xxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
[news:Otnp\\$LwlGHA.1972@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](news:Otnp$LwlGHA.1972@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

Re: Changing ADAM user password

I'll show this to digest folks. Something is missing indeed. Maybe by design, maybe not.

--

Dmitri Gavrilo
SDE, DS Admin eXperience

This posting is provided "AS IS" with no warranties, and confers no rights.

Use of included script samples are subject to the terms specified at <http://www.microsoft.com/info/copyright.htm>

"Joe Kaplan (MVP - ADSI)"

<joseph.e.kaplan@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

wrote in message <news:uammLpglGHA.1276@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

That's too bad. I assume you tried that using a 2003 client as well. I know this works ok when using negotiate auth, as I've used that trick often with ldp. There is probably something missing with the encryption support in digest or something like that.

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>

--

"Lee Flight" <lef@xxxxxxxxxxxxxxxxxxxx> wrote in message <news:u8tbqEelGHA.3924@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

I just tried this using ldp and an Delete/Add on unicodePwd:

--

```
0 = ldap_set_option(ld,
LDAP_OPT_ENCRYPT, 1)
res = ldap_bind_s(ld, NULL,
&NtAuthIdentity,
DIGEST (16518)); // v.3
{NtAuthIdentity:
User='cn=test1,ou=testou1,o=myorg,dc=myroot';
Pwd=<unavailable>; domain = "}
Authenticated as:
'CN=test1,OU=testOU1,O=myorg,DC=myroot'.
```

Re: Changing ADAM user password

```
***Call Modify...
ldap_modify_s(ld,
'CN=test1,OU=testOU1,O=myorg,DC=myroot'
,[2] attrs);
```

Error: Modify: Operations Error. <1>
Server error: 00002077: SvcErr:
DSID-0338070C, problem 5012
(DIR_ERROR), data 8237

Error 0x2077 Illegal modify operation.
Some aspect of the modification is not
permitted.

--

Not sure if there is anything in code that
could improve on this but at
first glance it appears that the security of the
channel is not being
recognized in this case. Simple bind + SSL
worked fine.

Lee Flight

"Joe Kaplan (MVP - ADSI)"
<joseph.e.kaplan@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
wrote in message
news:%23KRfPgalGHA.4540@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

I'll give the
digest/encryption thing a try
as soon as I get a chance
to flip my ADAM back to
requiring encrypted
password mods. :)

Re: Changing ADAM user password