

Re: Setting Passwords via DSML with non-admin type Domain User Cre

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.platformsdk.security/2005-05/0245.html>

From: Joe Kaplan \ (MVP - ADSI) (joseph.e.kaplan_at_removethis.accenture.com)

Date: 05/26/05

Date: Wed, 25 May 2005 20:56:58 -0500

I think we are confusing terms now. :)

There are three different types of LDAP attribute modifications: add, delete and replace. You need to do a delete operation on the old password value and an add on the new password value. This is not to be confused with deleting the whole object from the tree. :)

My guess is that it would look like this:

```
<modification name="unicodePwd" operation="delete">
<valuexsi:type="xsd:base64Binary">IgbVAGwAZABQAGEAcwBzAHcAbwByAGQAIgA=</value>
</modification>
<modification name="unicodePwd" operation="add">
<valuexsi:type="xsd:base64Binary">IgbuAGUAdwBQAGEAcwBzAHcAbwByAGQAIgA=</value>
</modification>
```

The DSML docs on MSDN are pretty sketchy, so I'm not sure if that's right or how to find out since I have no DSML directory to play with. Hopefully this will help you though.

Joe K.

"Marvin Bobo" <marvinb@community.nospam> wrote in message
news:BF246E03-290B-4D24-A44C-88734EF4E838@microsoft.com...

```
> Yes, I have the old password so I believe I can do this. You can do a
> batch
> of operations in a single request and it basically uses the LDAP syntax
> wrapped in the XML tags of the DSML schema. Deleting the old password is
> where I am running into the LDAP syntax. For instance, the DSML for
> delete
> is as follows:
>
> <se:Envelope xmlns:se="http://schemas.xmlsoap.org/soap/envelope/">
> <se:Body xmlns="urn:oasis:names:tc:DSML:2:0:core">
> <batchRequest xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
> xmlns:xsd="http://www.w3.org/2001/XMLSchema">
```

```
> <!--Clean up any existing entries-->
> <delRequest dn="cn=testuser,ou=testou,DC=TFODev,DC=local"/>
> <delRequest dn="cn=testuser1,ou=testou,DC=TFODev,DC=local"/>
> <delRequest dn="cn=testuser2,ou=testou,DC=TFODev,DC=local"/>
> </batchRequest>
> </se:Body>
> </se:Envelope>
>
> This would remove the user object testuser, testuser1, and testuser2 from
> the OU testou. If this is for an object in a OU, how do you remove the
> attribute unicodePwd from testuser? Not even sure if I am asking the
> correct
> question or if I am offbase. Once I have some clarity here I can try some
> items. Any thoughts?
>
> "Joe Kaplan (MVP - ADSI)" wrote:
>
>> Ok, so in this case you are just doing an LDAP replace operation. That
>> is
>> essentially the AD equivalent of Reset Password when modifying
>> unicodePwd.
>> This is done by administrators when creating an account with an initial
>> password or doing an administrative reset when the user forgets.
>>
>> To do a change password, you do two mod ops, a "delete" and an "add",
>> although I'm not sure what the DSML for this is. You delete the old
>> password value and add the new one. You need the old password to do
>> this.
>> I assume DSML lets you do a batch of modifications in a single operation.
>>
>> Generally, normal users have rights to change their own password but
>> cannot
>> set the password for anyone. Admins can set the password for anyone and
>> can
>> change their own, but can't change a normal user's password.
>>
>> So, I think it might depend on what you are trying to do here. If the
>> goal
>> is for end user password change, then you can do that, but you need the
>> old
>> password.
>> "Marvin Bobo" <marvinb@community.nospam> wrote in message
>> news:556AE95B-B6F6-49FD-A058-10D2087853D4@microsoft.com...
>> > My apologies, code would help but I am not sure how to do the remove op
>> > in
>> > DSML. What is happening is we have an external system that will
>> > "create"
>> > the
>> > password and this is transferred to Active Directory in support of a
>> > proprietary application. Therefore the unicodePwd field is being
>> > modified.
```

>>> *What I am not sure of is how to "remove" the unicodePwd attribute and
>>> then
>>> set it. Here is the batch request (in DSML) which works under
>>> administrator
>>> level but not doing the suggestion in your original post.*
>>>
>>> `<se:Envelope xmlns:se="http://schemas.xmlsoap.org/soap/envelope/">
>>> <se:Body xmlns="urn:oasis:names:tc:DSML:2:0:core">
>>> <batchRequest xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
>>> xmlns:xsd="http://www.w3.org/2001/XMLSchema">
>>> <modifyRequest dn="cn=test,ou=testou,DC=TFODev,DC=local">
>>> <modification name="unicodePwd" operation="replace">
>>> <value
>>> xsi:type="xsd:base64Binary">IgbuAGUAdwBQAGEAcwBzAHcAbwByAGQAIgA=</value>
>>> </modification>
>>> </modifyRequest>
>>> </batchRequest>
>>> </se:Body>
>>> </se:Envelope>
>>>`
>>> *"Joe Kaplan (MVP – ADSI)" wrote:
>>>
>>>> It isn't easy finding any help for DSML as it is not very well used.
>>>> I
>>>> actually know almost nothing about it.
>>>>
>>>> Based on the previous post that you referred to (which I guess I wrote
>>>> :)),
>>>> I want to ask if you are doing the remove and add mod op instead of
>>>> the
>>>> replace. If you show your code, that might help (although I know
>>>> neither
>>>> DSML or PERL very well, I should be able to figure it out, especially
>>>> if
>>>> you
>>>> post both versions).
>>>>
>>>> If you try to do a set password (just an LDAP replace), you'll
>>>> probably
>>>> have
>>>> a permissions problem because normal users don't have rights to reset
>>>> passwords, only to change their own.
>>>>
>>>> HTH,
>>>>
>>>> Joe K.
>>>> "Marvin Bobo" <marvinb@community.nospam> wrote in message
>>>> news:FC83C34F-44F5-4108-A60A-DF55EFB0F7BF@microsoft.com...
>>>>> When I execute the DSML request to change the password as Admin,
>>>>> works
>>>>> ok.*

microsoft.public.platformsdk.security: Re: Setting Passwords via DSML with non-admin type Domain User Cre

>> >> > *When I execute as the domain user, fails with "HTTP Error 401.3 – Unauthorized: Access is denied due to an ACL set on the requested resource".*

>> >> > *I have set the specific user to full control on the ou and container for*

>> >> > *the*

>> >> > *user. The domain user logging on is changing its own account.*

>> >> >

>> >> > *Here is a post that is related to what I need to do but this is with*

>> >> > *LDAPs*

>> >> > *using Perl scripts:*

>> >> >

>> >> >

<http://msdn.microsoft.com/newsgroups/managed/Default.aspx?dg=microsoft.public.active.directory.interfaces&mid=8>

>> >>

>> >>

>> >>

>>

>>

>>

>>