

# Re: Architectural question for product security deployment

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2005-08/msg01813](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2005-08/msg01813)

---

- *From:* "Al Mulnick" <[amulnick\\_No\\_SPAM@xxxxxxxxxxxxx](mailto:amulnick_No_SPAM@xxxxxxxxxxxxx)>
  - *Date:* Wed, 24 Aug 2005 13:58:40 -0400
- 

I haven't seen the code you're using or the perspective you're using, so it's hard to say why the change password is failing.

Here's some things to look for:

By default, ADAM uses the local and domain policies where it's installed.

Be sure you comply with that when setting up users. Your passwords must meet the policy requirements in order to be used.

Also, to change passwords via LDAP, you must connect via a secure method by default. I can't recall if you said you did that but I don't see it at the moment. You'll note in this example how they set the secure authentication bit (may not work in workgroup setting; you may need an alternate method, but you'll have to check the code to know what direction to go if any)

[http://msdn.microsoft.com/library/default.asp?url=/library/en-us/adam/adam/creating\\_users.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/adam/adam/creating_users.asp)

There's a registry key change that needs to be made to tell ADAM to use the workgroup accounts. That's why I was saying it would be a good idea to use a wrapper for your setup routine to check for domain vs. workgroup and then take appropriate action. ADAM is setup to work in a domain environment by default.

Why are you changing the login account at this point when you install ADAM.

Why not after you have everything working?

Keep things as simple as you can before trying to tighten security. After all, if it's too secure, it won't be usable right? :)

There are little tweaks and changes you can make to ADAM to change the default behavior. It sounds like some of those changes need to be made in your situation, but as you can imagine, we can only really point you to the resources vs. tell you exactly what to do. Nature of the beast I think.

You may want to have a look here:

[http://msdn.microsoft.com/library/default.asp?url=/library/en-us/adam/adam/quick-start\\_tutorial.asp?frame=true](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/adam/adam/quick-start_tutorial.asp?frame=true)  
to get some ideas to go with what you have so far.

HTH,

Re: Architectural question for product security deployment

AI

"evansight" <evansight@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message  
news:B95A6B3B-5ED0-4E20-92E5-EFFC056E4E55@xxxxxxxxxxxxxxxxxxxx

> Hi AI, thanks for your fast reply.

>

> Question on unattended deployment:

>

> In order to bind to ADAM as a separate ADMIN user:

>

> 1) I Installed ADAM by first logging in a system admin and creating the

> separate admin account on the ADAM serve ( A Win3K server box).

> 2) I then logged in again as that admin account

> 3) I then installed ADAM.

>

> At first I tried to install ADAM as the system admin and then bind to the

> ADAM server via the admin account. This did not work. I also tried

> running

> the Access scripts to set permissions which also did not work. In any

> event,

> I couldn't determine the right place to set the permission so that it

> would

> be inherited by all other objects within the ADAM store.

>

> Question on Binding to Windows Principal Object

>

> We're able to code LDAP queries that access the user's account and then

> instantiate a new Windows Principal Object. However, the desired process

> is

> to enable the workstation to already be aware of the identity of the user

> in

> a workgroup, as opposed to domain, connectivity scenario.

>

> Question on changing another user's password as the ADMIN. Attempts to

> bind

> as the ADMIN and use LDAP queries to change another user's password fail.

> However other attributes can be updated. Is this prohibited as a matter

> of

> policy or is there a different set of permissions needed to set passwords

> for

> other users programmatically. The questions are also the same for

> programmatically locking a users account.

>

> Thanks for your help!

>

>

>

>

>

>

>

>

>

Re: Architectural question for product security deployment

Re: Architectural question for product security deployment

> --  
> - evansight  
>  
>  
> "Al Mulnick" wrote:  
>  
>> I think you'll need to have some logic to figure out whether it's in  
>> domain  
>> or workgroup setting. That's something I envision as being like a  
>> wrapper  
>> around the setup process. You would make decisions based on that.  
>>  
>> Other thoughts inline.  
>>  
>> Al  
>>  
>>  
>>  
>> "evansight" <evansight@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message  
>> news:0E4284D9-FA09-47F4-BA8A-240737ED348C@xxxxxxxxxxxxxxxxxxxx  
>>> I'm fairly new to ADAM, though not to Active Directory. I've  
>>> downloaded  
>>> ADAM  
>>> and have successfully implemented some test users.  
>>>  
>>> I've been asked to deploy a VS .Net windows application software  
>>> product  
>>> that potentially would utilize ADAM to manage and authenticate users  
>>> via  
>>> role  
>>> based access. The product currently utilizes SQL Server 2000 for  
>>> business  
>>> entitlements and for a transactional as well as analytic data store.  
>>> I've  
>>> successfully set up sample users and a complete set of roles to which  
>>> the  
>>> users are mapped as members.  
>>>  
>>> The existing application is a VS 2003 .Net remoting application that  
>>> includes a well defined set of layers for client and server processing.  
>>>  
>>> Here's our need:  
>>>  
>>> The goal is to find a way to deploy an identity management and policy  
>>> store  
>>> for a windows application that works in a network workgroup as well as  
>>> a  
>>> domain environment, that can be automatically deployed through an  
>>> installation script, without manual configuration of a windows server.  
>>>  
>>> Before I started the project ADAM had been deployed successfully in a

## Re: Architectural question for product security deployment

>>> workgroup environment. However, after my own redeployment,  
>>> reconfiguration  
>>> there are the following issues:  
>>>  
>>> 1) It does not appear that the store can be fully deployed without  
>>> manual  
>>> configuration of the server environment. This is an issue since the  
>>> majority  
>>> of our target install base is not technically savvy and we don't have  
>>> the  
>>> resources to send engineers to every site for an install.  
>>>  
>>>  
>> When you say it requires manual setup, what exactly are you doing that  
>> you  
>> need manual interference?  
>>  
>>  
>>>  
>>> 2) It does not appear the Workgroup implementation allows a direct bind  
>>> to  
>>> the Windows Principal object in the way that Active Directory does in a  
>>> domain solution. This seems to be verified by documentation for ADaM,  
>>> specifically the "Administering users and groups" table that shows that  
>>> integrated security is not supported in the Workgroup, as opposed to  
>>> Domain,  
>>> deployment.  
>>>  
>>> 3) Deployment of an ADMIN user who can, via .Net code, reset other user  
>>> passwords seems to be an issue. Perhaps this is just a permissions  
>>> issue,  
>>> but I was pretty careful to set up the correctly delegated permissions  
>>> of  
>>> the  
>>> ADAM ADMIN user account, including importing the fully defined schema  
>>> for  
>>> users, e.g. inetorg, etc.  
>>>  
>> Again, what steps are you taking here. I would expect that the  
>> credentials  
>> used to setup ADAM were sufficient for you to be able to do this. But I'm  
>> interested in the steps you took to see why it wasn't working for you.  
>>  
>>  
>>>  
>>> The identity management workflow we are trying to provide is a way for  
>>> a  
>>> person in the ADMIN role to create new users through a custom  
>>> interface,  
>>> and  
>>> assign or reassign temporary passwords. Upon subsequent logon, the

Re: Architectural question for product security deployment

>>> user  
>>> set  
>>> up by the admin would then be prompted to set up a permanent password,  
>>> as  
>>> well as create a security reminder (question and answer). While this  
>>> would  
>>> seem to be fairly standard workflow, I've not seen any complete  
>>> scripting  
>>> examples.  
>>>  
>>> In summary, I'm looking for confirmation as to whether the above  
>>> problems  
>>> are in fact known issues or ADAM product limitations or if we're just  
>>> not  
>>> following the right process. And if we're not following the right  
>>> process,  
>>> what would that be?  
>>>  
>>> Thank in advance for your help.  
>>>  
>>> —  
>>> – evansight  
>>  
>>  
>>

---

• **References:**

- ◆ **[Architectural question for product security deployment](#)**  
    ◇ From: evansight
- ◆ **[Re: Architectural question for product security deployment](#)**  
    ◇ From: Al Mulnick
- ◆ **[Re: Architectural question for product security deployment](#)**  
    ◇ From: evansight

- Prev by Date: **[Listing and editing active directory information in IIS](#)**
- Next by Date: **[Re: ADPREP Fails with Win32 error " Cannot find file specified "](#)**
- Previous by thread: **[Re: Architectural question for product security deployment](#)**
- Next by thread: **[Problem to setup dns caused by Active Directory](#)**
- Index(es):
  - ◆ **[Date](#)**
  - ◆ **[Thread](#)**