

# Re: IISADMPWD solution for AD expired password ?

---

*Source:*

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2007-12/msg00098.html>

---

- *From:* Pascal <pascal\_t@xxxxxxxxxxxxxxxxxxxx>
  - *Date:* Tue, 18 Dec 2007 10:05:32 +0100
- 

I will make further test and let you know what I find, thank you.

I was thinking that the password will be modified by IIS credentials not the user one.

Thank you

My understanding regarding this is that the anonymous access to the page doesn't help you at all. In order for the user to be able to change their password, they must authenticate to the directory as themselves first and that this key problem, as they cannot authenticate when their password has expired.

However, I could be wrong about that. I have very little knowledge of this particular page and how it works. I'm mostly familiar with how these things work from an LDAP perspective.

Try it and find out.

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>

--

"Pascal" <pascal\_t@xxxxxxxxxxxxxxxxxxxx> wrote in message  
<news:mn.8bf07d7c724cd64d.70874@xxxxxxxxxxxxxxxxxxxx>

Hi Joe,

thank you for your nice explanation.

Like you, I have heard about the policy to log on with expired passwords but I didn't find anything about that on Microsoft.com.

You said that IIS will not let the users to change their password if it expired and that I have to allow them to log on with expired passwords.

Re: IISADMPWD solution for AD expired password ?

I am not agree as it would be possible to allow external users to connect to IISADMPWD website with anonymous access (configured only for this virtual directory).

So, users will be able to enter their login/password and to reset them even if it expired. Am I wrong ?

Thank you for your nice advices about challenge/response !

You will need an alternate auth method for your self-service pwd reset if you need self-service pwd reset. You would likely need this because you want to allow users to reset their pwd after it expires or if they forget it. Self-service here prevents a help desk call and saves money.

If you can change your policy to allow users to log on with expired passwords, then you don't need this solution for the first reason. You might still want it for the second reason though. Also, I'm not sure how to actually allow users to log in with expired passwords. I'm guessing that this is possible since one of the other MVPs mentioned it, but I'm not familiar with that setting. It is also a question as to whether you want to allow that to happen, even if it is a valid option.

You don't necessarily need 2 factor auth for self service pwd reset. You just need an alternate way to authenticate your users. 2 factor is usually better since it is considered stronger than password alone. The normal approach is to use challenge/response questions. However, most security professionals consider those to be weaker than passwords, so there is a question as to whether you want to make allow your self-service pwd reset app use a weaker auth mechanism.

My experience is that most orgs don't have 2 factor auth and would rather save the money on help desk calls for password resets, so they make the sacrifice on security. It is a little sad, but not surprising. The risk associated with the weaker security is hard to quantify whereas help desk calls are generally quite easy.

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>

---

Re: IISADMPWD solution for AD expired password ?

"Pascal" <pascal\_t@xxxxxxxxxxxxxxxxxxxx> wrote in  
message  
[news:mn.731a7d7c46078493.70874@xxxxxxxxxxxxxxxxxxxx](mailto:news:mn.731a7d7c46078493.70874@xxxxxxxxxxxxxxxxxxxx)

-- Pascal

--  
Pascal

.