

Re: AD password policy in Forms auth against AD

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.dotnet.framework.aspnet.security/2004-12/0219.html>

From: Nils Magnus Englund (*nils.magnus.englund_at_orkfin.no*)

Date: 12/18/04

Date: Sat, 18 Dec 2004 14:07:18 +0100

Oh, that wasn't good news :(

Do you think it's a good idea to do it like this, or perhaps I should find another method? I'm trying to avoid using any other storage medium than AD.

Regards,
Nils Magnus Englund

"Joe Kaplan (MVP – ADSI)" <joseph.e.kaplan@removethis.accenture.com> wrote in message news:ecCz\$WF5EHA.2676@TK2MSFTNGP12.phx.gbl...

> *This is going to be a lot of work if you plan to do this via LDAP. You'll need a service account that can access the user account to read all of their attributes and you'll need to learn how to determine all of the various things that indicate these states. AD doesn't tell you why a bind failed (due to lockout, disabled, expired, user must change password, etc. vs. simple bad password), so you have to figure this out for yourself.*

>
> *Joe K.*

>
> "Nils Magnus Englund" <nils.magnus.englund@orkfin.no> wrote in message news:eDXKeXC5EHA.1188@tk2msftngp13.phx.gbl...

>> *Hey!*

>>
>> *I've successfully followed Microsofts example on how to use Forms authentication with Active Directory (from the "Building Secure ASP.NET Applications" How To-section). However, I would very much like to use AD's password policy features, specifically:*

>>
>> *1. I want the user to get a warning e.g. two weeks before his/hers password expires*

>>
>> *2. I want the user to be able to change password (assuming the new password meets the requirements set by the password policy)*

>>
>> *3. If the password has expired, I want the user to still be able to log in, but forced to change password in order to continue. (If this isn't possible with AD, I could set the expiration time to a year, and force*

microsoft.public.dotnet.framework.aspnet.security: Re: AD password policy in Forms auth against AD

>> *the user to change password if there's less than 300 days left, in effect*
>> *giving the user two months password expiration with another 300 days*
>> *before the user is disabled/blocked).*
>>
>> *Any ideas and/or suggestions? This will be used on a portal with several*
>> *hundred customers, where all customers will be stored in a AD (in their*
>> *own "External users" OU).*
>>
>> *Thanks!*
>>
>>
>> *Regards,*
>> *Nils Magnus Englund*
>>
>
>