

## Re: LDAP bind allowing old password for 1 hour

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2008-08/msg00534](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2008-08/msg00534)

---

- *From:* AlanAlbany <[AlanAlbany@xxxxxxxxxxxxxx](mailto:AlanAlbany@xxxxxxxxxxxxxx)>
  - *Date:* Tue, 12 Aug 2008 00:21:03 -0700
- 

This is followup to report that defining registry value HKLM\SYSTEM\CurrentControlSet\Control\Lsa\OldPasswordAllowedPeriod as a DWORD with a value of 0 as recommended by Jian-Ping Zhu resolves this issue. Our earlier testing was at fault – we had made a typo in the registry value name – a trailing space that was difficult to spot.  
Alan Albany

"AlanAlbany" wrote:

Hi

The test code I supplied is not the code from the (third party) SSO application but just something we wrote to reproduce the problem. Unfortunately we do not have access to the code used in the SSO application. The domain controller is in a stand-alone domain/forest used primarily as a central password synchronisation domain and the client is external to this domain/forest. Its looking like we will need to ask them to use a different technique to authenticate other than using a simple LDAP bind to avoid this "feature" in Windows 2003 Active Directory. (For other purposes we have written web services that use .Net to authenticate a user and these do not exhibit the problem – we may need to get the SSO application to use such a web service.)

Regards,  
Alan