

Reset Expired Password

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.scripting/2004-08/0043.html>

From: Mike Garner (*anonymous_at_discussions.microsoft.com*)

Date: 08/03/04

Date: Tue, 3 Aug 2004 12:56:29 -0700

I'd like to have a script (which will eventually run via CGI/WWW) were a user can reset his or her own password in Active Directory. I've got one that works great except when the user's password has already expired. I'm binding to LDAP/AD with the user's credentials, username and old password so that they'll only have the rights to their user object (and only be able to change that 1 user's password). However, if their password has expired because the max password age as been reached or the help desk checks the box in AD User and Computers to Have the user reset password at next login, the script won't bind to AD. Of course, I can get around this by using an administrator account to connect to LDAP but I really want to connect in a way that

- 1) verifies the old password
- and
- 2) only allows the user to change his or her password

Any ideas? I'm sure this can't be a unique situation. Or maybe something is wrong...I was quite surprised that the expired password caused the bind to fail...the expired password IS the user's password...

Here's what my bind string looks like (in PERL but WSH folks can probably read between the lines:

```
my $adsinamespaces = CreateObject
Win32::OLE 'ADsNameSpaces' || &errors('1');
my $ldapnamespace= $adsinamespaces->GetObject("", "LDAP:")
|| &errors('2');
my $userdsobject=$ldapnamespace->OpenDSObject
("LDAP://dc.domain.com/OU=Users,dc=domain,dc=com", "cn=$user,ou=$ou,OU=Users,dc=domain,dc=com", $old_password, 1) ||
&errors('3');
```

Thanks,
~Mike