

## Real-World Scenario 11-2: User Password Security and Account Expiration

**Scenario:** A consultant (Douglas) will be working at your company for three months. Your company has a policy stating that user passwords must be changed every 42 days. What are the two most important issues that you see in the figure?

**Douglas Adams Properties** [?] [X]

Member Of	Dial-in	Environment	Sessions
Remote control	Remote Desktop Services Profile		COM+
General	Address	Account	Profile
Telephones	Organization		

User logon name:  
d.adams @11-8.com

User logon name (pre-Windows 2000):  
11-8\ d.adams

Logon Hours... Log On To...

☐ Unlock account

Account options:

- ☐ User must change password at next logon
- ☐ User cannot change password
- ☒ Password never expires
- ☐ Store password using reversible encryption

Account expires

☒ Never

☐ End of: Friday, January 20, 2017

OK Cancel Apply Help

## Real-World Scenario 11-2 Solution

First of all, the most glaring issue is that the "Password never expires" checkbox is selected. The company has a 42-day change policy, and should also have a policy stating that a user cannot reuse the same password (usually for at least a year, if not forever). So that needs to be deselected and, possibly, we should review our policies and make sure that this account (and its group) have the policies applied to it.

More importantly, the consultant (Douglas) will only be working at the company for three months. We need to set an account expiration date for that user account. This way, the user will not be able to log on to the domain after the consulting period has ended. In the video solution I show how to reconfigure this within Active Directory Users and Computer in Windows Server 2012.

**Video Solution:** Watch the video solution "11-2: User Password Security and Account Expiration."