# SysOp Tools Learning Guide:

## How do I implement a password change policy in my already-existing domain? What will happen to my user accounts if I enable the change-password policy?

Updated November 6, 2007

These are questions we've dealt with on many occasions- Unfortunately Microsoft does not offer much guidance on this particular issue. The below information will help you to plan and implement a successful change-password policy deployment in your domain environment.

### Foreword: Be cautious, know your AD user objects, take your time on planning

Implementing your domain password change policy for the first time must be approached very carefully. If planned right it will not be too much of a headache. If planned incorrectly...Well, let's just say it is not going to be fun and will leave a very poor first impression on your users.

**PwdLastSet attribute – What is it and Why is it Important?**

One of the most important attributes you will want to review for your domain user objects is the PwdLastSet attribute, or "Password Last Set". This attribute tells Active Directory when the user password has last been changed. *It is important to note this, as any passwords that are older than the new policy you plan to implement will be immediately expired, causing your users problems.*

For example, you implement a password change policy requiring users to change their password every 60 days. Most of your users have a password that is older than 60 days since they have never had to change it.

The result? As soon as each of these users is placed under the new 60 day policy, their old password will immediately be expired because Active Directory sees that the PwdLastSet date is much older than 60 days.

Your goal? Get your users to update their password prior to placing them under the change policy, so they have a PwdLastSet date that is newer than the 60 day policy.

Why is this? Each time a user's password is changed in Active directory, the PwdLastSet attribute for that user object is updated with the date/time that it was changed.

*Remember, if you turn on the password expiration policy in your domain without either first ensuring your users have updated their old passwords or you have explicitly set their accounts to 'Password Never Expires', you will have a lot of frustrated users with an expired password calling the help desk.*

### 1. Ok- Let's get things Rolling and Activate that Domain Password Policy!

Ok so where should I start?

To get a feel for what is being discussed in regards to the PwdLastSet attribute and old passwords, begin your planning by searching in Active Directory for your users with the oldest PwdLastSet timestamp. To make things easy, we will use the tool **Password Reminder PRO** from **SysOp Tools** to view your oldest password accounts in the domain.

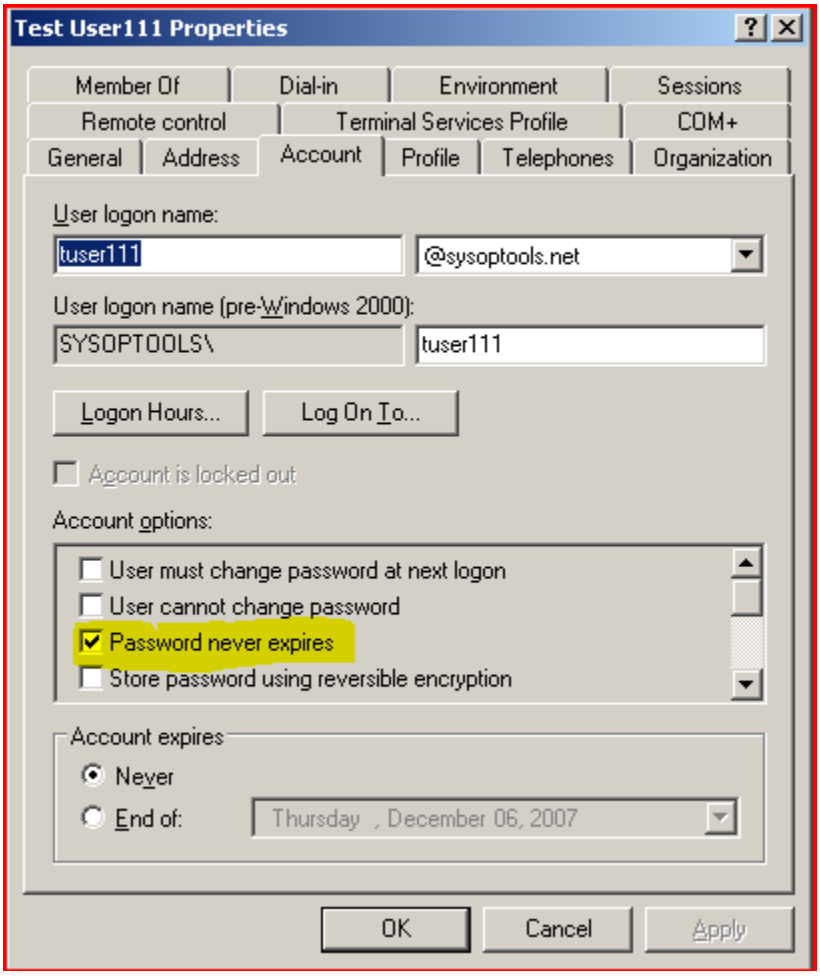
You can also use a VB script and some math conversion, but this tool makes it very easy and is totally free to use for two months. Download from http://www.sysoptools.com

**(continued on next page.. )**

**Before you enable the domain password expiration policy in your domain, it is a good idea to go through your domain user objects and explicitly check the box for *Password Never Expires*.**

This will allow you to enable the password expiration policy in the domain without accidentally expiring the passwords of your existing users. You should also make certain that this setting is checked for all service and resource user accounts. This change to the accounts will be transparent to users.

**TIP:** You can shift-select multiple user objects in an OU and right-click to set the 'password never expires' attribute. A real time-saver ☺.



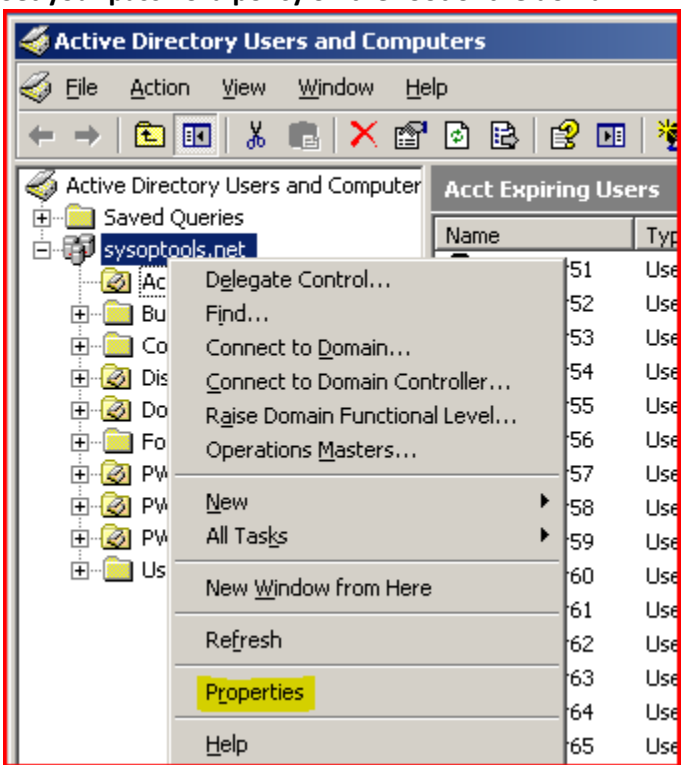

Once you have checked all of your user accounts, you may now safely define your domain password expiration policy in the default policy at the root of the domain.

This is the ONLY place that you can define this policy, it will not work if you define a password expiration policy on an OU policy or on the Domain Controller's default policy.

To do this, open the Active Directory Users and Computers MMC and right-click the domain name that hosts your user objects.

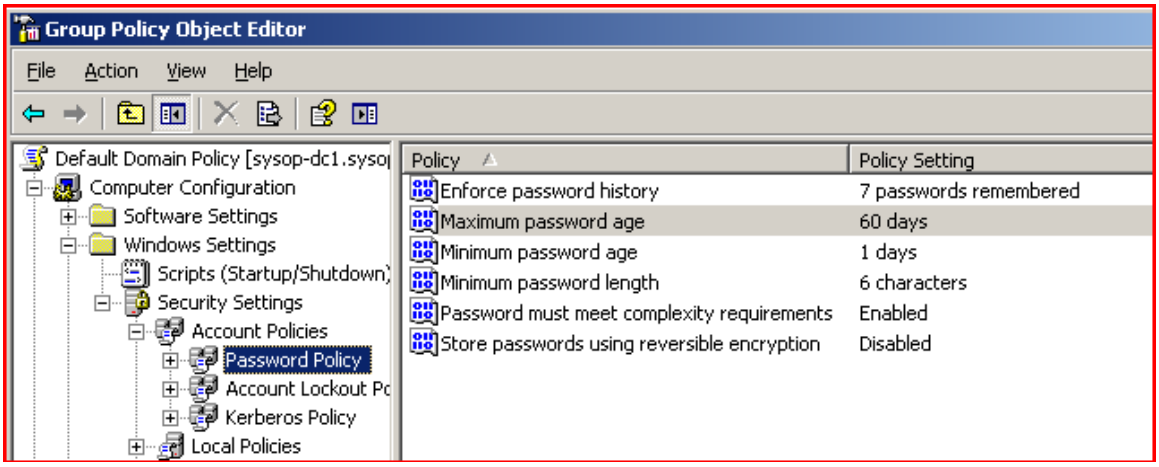
**(continued on next page..)**

**Set your password policy on the root of the domain:**




Choose Properties, go to the Group Policy tab, highlight the default domain policy and choose Edit. The editor window opens up.

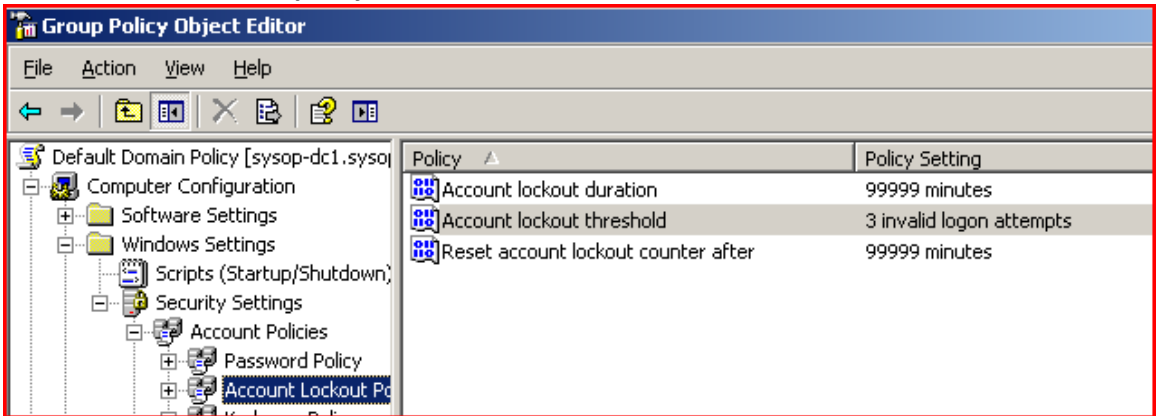
Go to "Computer Configuration -> Windows Settings -> Security Settings -> Account Policies -> Password Policy". The below settings are suggested for a good start.




You should also define how incorrect logon attempts are handled to help ensure proper security in the Account Lockout policy. Again, these are suggested settings for a good start.

**(continued on next page…)**

**Set the account lockout policy**




***Note:*** *"99999 minutes" pretty much means forever, until an Admin unlocks the account. Give your domain 15-20 minutes to replicate the changes to all computers.*

**Congratulations, your domain's password change policy is now in effect and will apply to all user account objects that DO NOT have the box checked for 'Password Never Expires'!**

## 2. Planning A Password Change Policy Deployment to Users in a Small Company

Now on to the fun stuff, placing your user accounts under the new password change policy.

**Viewing Your Oldest Password User Objects**

***Note:*** *Before proceeding, make sure you have already gone through your domain and checked all of your staff member's users accounts to 'never expire' the password!*

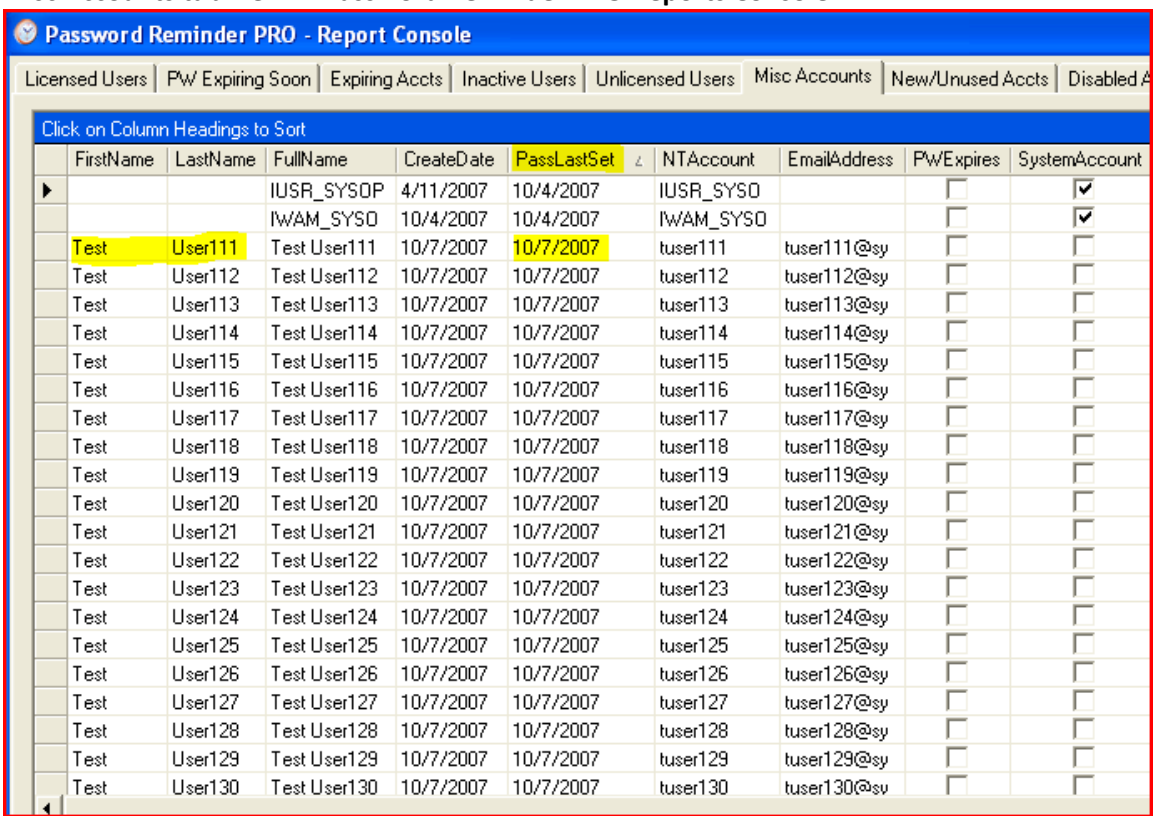
Install Password Reminder PRO on a domain workstation that can talk to your main DC's. Configure the software settings per the Quick Start Setup guide on the SysOp Tools Support webpage, then open the User Reports console. Navigate to the "Misc Accounts" tab to view all of your user objects set with a non-expiring password.

Sort users by the column "PassLastSet" by clicking the column heading. Look at the oldest password user accounts, ignoring any obvious Service, Resource or "$" accounts (these user accounts do not belong to 'real' users, and you may in fact want them to not expire the password).

See screenshot on next page, the "oldest password" user in our test domain is highlighted.

**(continued on next page…)**

**Misc Accounts tab view in Password Reminder PRO Reports Console**




| FirstName | LastName | FullName | CreateDate | PassLastSet | NTAccount | EmailAddress | PWExpires | SystemAccount |
|---|---|---|---|---|---|---|---|---|
| | | IUSR_SYSOP | 4/11/2007 | 10/4/2007 | IUSR_SYSO | | ☐ | ☑ |
| | | IWAM_SYSO | 10/4/2007 | 10/4/2007 | IWAM_SYSO | | ☐ | ☑ |
| Test | User111 | Test User111 | 10/7/2007 | 10/7/2007 | tuser111 | tuser111@sy | ☐ | ☐ |
| Test | User112 | Test User112 | 10/7/2007 | 10/7/2007 | tuser112 | tuser112@sy | ☐ | ☐ |
| Test | User113 | Test User113 | 10/7/2007 | 10/7/2007 | tuser113 | tuser113@sy | ☐ | ☐ |
| Test | User114 | Test User114 | 10/7/2007 | 10/7/2007 | tuser114 | tuser114@sy | ☐ | ☐ |
| Test | User115 | Test User115 | 10/7/2007 | 10/7/2007 | tuser115 | tuser115@sy | ☐ | ☐ |
| Test | User116 | Test User116 | 10/7/2007 | 10/7/2007 | tuser116 | tuser116@sy | ☐ | ☐ |
| Test | User117 | Test User117 | 10/7/2007 | 10/7/2007 | tuser117 | tuser117@sy | ☐ | ☐ |
| Test | User118 | Test User118 | 10/7/2007 | 10/7/2007 | tuser118 | tuser118@sy | ☐ | ☐ |
| Test | User119 | Test User119 | 10/7/2007 | 10/7/2007 | tuser119 | tuser119@sy | ☐ | ☐ |
| Test | User120 | Test User120 | 10/7/2007 | 10/7/2007 | tuser120 | tuser120@sy | ☐ | ☐ |
| Test | User121 | Test User121 | 10/7/2007 | 10/7/2007 | tuser121 | tuser121@sy | ☐ | ☐ |
| Test | User122 | Test User122 | 10/7/2007 | 10/7/2007 | tuser122 | tuser122@sy | ☐ | ☐ |
| Test | User123 | Test User123 | 10/7/2007 | 10/7/2007 | tuser123 | tuser123@sy | ☐ | ☐ |
| Test | User124 | Test User124 | 10/7/2007 | 10/7/2007 | tuser124 | tuser124@sy | ☐ | ☐ |
| Test | User125 | Test User125 | 10/7/2007 | 10/7/2007 | tuser125 | tuser125@sy | ☐ | ☐ |
| Test | User126 | Test User126 | 10/7/2007 | 10/7/2007 | tuser126 | tuser126@sy | ☐ | ☐ |
| Test | User127 | Test User127 | 10/7/2007 | 10/7/2007 | tuser127 | tuser127@sy | ☐ | ☐ |
| Test | User128 | Test User128 | 10/7/2007 | 10/7/2007 | tuser128 | tuser128@sy | ☐ | ☐ |
| Test | User129 | Test User129 | 10/7/2007 | 10/7/2007 | tuser129 | tuser129@sy | ☐ | ☐ |
| Test | User130 | Test User130 | 10/7/2007 | 10/7/2007 | tuser130 | tuser130@sy | ☐ | ☐ |

The initial review process of your domain user accounts can be time consuming, but will help you to get a good understanding of what is going on 'under the hood' before you enable password expirations for all of your users, and help you ensure a smooth deployment.

As you review the PassLastSet age of some of the current user passwords in the Password Reminder PRO User Reports, you may notice the date the password was last set for some of your users is as old as several years ago! Had you deployed a 60 day password change policy and not proactively set these old-password user accounts to 'Password Never Expires', you would have had some unhappy folks on your hands with immediately-expired passwords.

However, since you did in fact change the setting on their account to 'Password Never Expires', you can contact the users at your leisure to have them update their password, then uncheck the box for 'Password Never Expires', that's it. Once the user has set a new password, and you uncheck the property on their account for 'password never expires', their password is now managed via your domain password policy. If you plan to use Password Reminder PRO, your managed users will receive proactive email reminder notices in advance of their password expiration date.

Now, let's say you have a lot of users… hundreds, thousands… yikes! On the next page we'll take a look at another rollout approach with may be of some help.

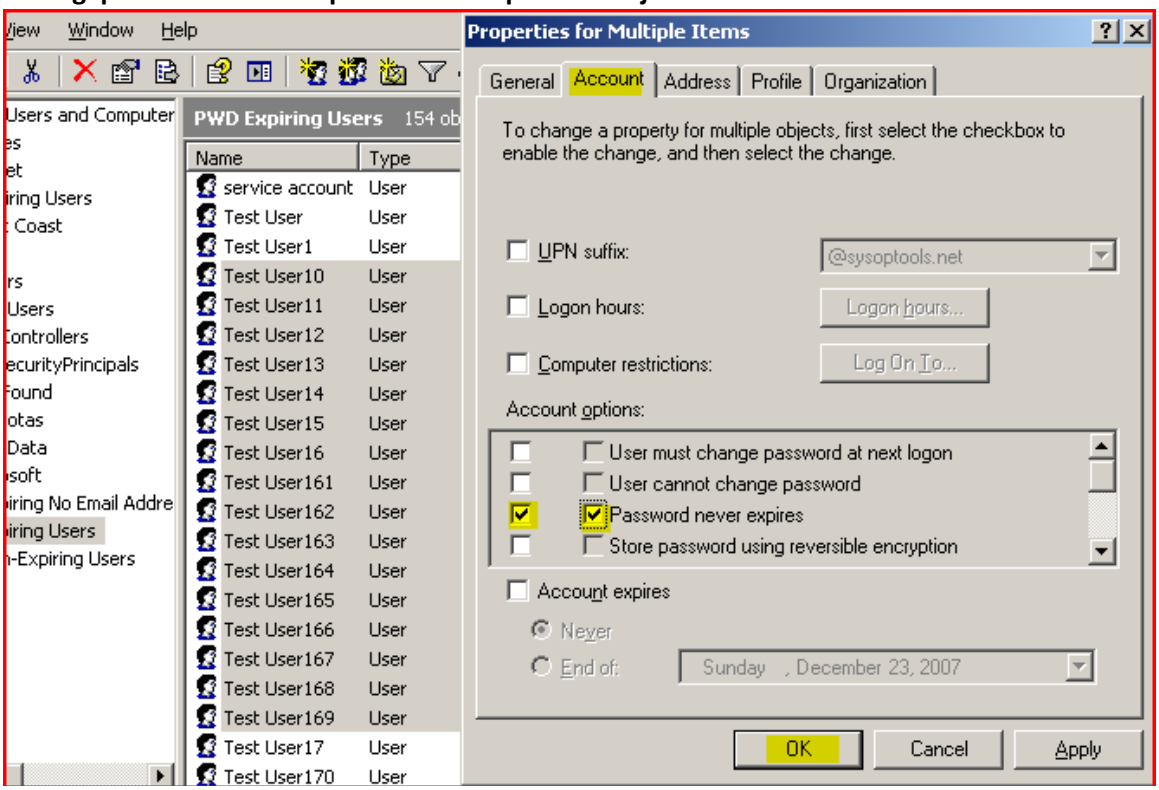
**(continued on next page…)**

## 3. Rolling out Password Policy Changes in a Large Organization

Ok, so you have several hundred (or thousand) users in your domain that need to be placed under the password expiration policy. Oh my!

Depending on your preferences and situation I recommend looking at the below methods of attack designed to greatly reduce impact to your large user community. Scripts may come in handy for bulk changes to setting / unsetting the 'Password Never Expires' attribute, however for sake of keeping this paper short I will not get into scripting. You can also shift-select users in the AD Users and Computers console, right-click the selected users, and change this setting for multiple accounts at once.

**Setting 'password never expires' on multiple user objects**




### 3a. The 1st Approach: Conquer-Over-Time based on the Oldest Password in the Domain

Let's say you have some users who have a PwdLastSet timestamp 200 days old. Let's say you don't want to hassle with setting all of your user accounts to 'Password Never Expires', and you want to phase in all of your users under a 60-day password expiration policy.
You also want to make this project low-impact and there is no rush to get it completed.
How can you do this?

**Find the oldest password user**

First you'll want to find the OLDEST password in the domain that belongs to a real staff user. Use the Password Reminder PRO User Reports > Misc Accounts and sort by PassLastSet date. Look at the date and count back the number of days from today to determine how old this password is.
Let's say for purpose of this example that your oldest user password is **210** days old.

**(continued on next page…)**

**Enable the password policy at a number of days older than the oldest user password**
What you can then do is enable the password expiration policy Max Password Age to **225** days (or longer, depending on how much advance warning you want to give that user- In this case we've given the user 15 days to change their password) and gradually decrease the number as the oldest password folks change their password.
Once the person with the 210 day old password changes his/her password, you have noted that the next oldest password belonging to a user is **190** days. You would bump your policy Max Password Age down to **205**. And so on, until you eventually hit your target password change policy of 60 days.

Doing this will prevent the situation when everyone is required to change his / her password right after the password change policy is introduced (or end up with an expired password), and will let you gradually hit your target of managing user passwords under a 60 day change policy. This method is pretty low-impact to users but could conceivable take a long time to complete, depending on how old your user passwords are and how aggressive you want to be.
As you phase in users under the new password change policy, you can use Password Reminder PRO to easily notify these users in advance as to when their password expiration date is approaching.

Now, if you have users with a PwdLastSet timestamp that is 1,500 days old or something ridiculously high, you may want to go on to the next approach.

**3b. The 2nd Approach: Divide and Conquer**
If time to completion is a factor, you may wish to consider a more controlled way to reach your target password change policy goal. Below are a couple of methods you can use to create a strategic approach that targets groups of users.

***Note:*** *This method requires that you go through your user accounts and explicitly set the accounts to 'Password Never Expires' before enabling the domain password expiration policy.*
After you have completed this step, go ahead and configure your domain password expiration policy to your target requirements. You can do this safely since your user accounts will not be managed by the domain policy until you uncheck 'Password Never Expires' in their account properties.

**Method 1: Force users to change password at next logon**
Your goal is to make sure that all of your users have a password last set date that is newer than your password expiration policy. You can do this fairly easily with internal LAN users by going into their user account properties and check the box for 'Require password change on next logon'. This method should NOT be used for external-only VPN or OWA users, as checking their setting on their account will not allow them to log in to OWA or most VPN systems.

This setting will "semi-expire" the user's password in AD and will force them to create a new password that meets the new requirements at next logon (if you have enabled password complexity and minimum length in your policy, their new password must meet the configured requirements).
This approach can work well but will require a bit stronger communication and pre-warning to users, as well as your IT support staff. Plan on starting out with email campaigns a couple weeks in advance to your users and inform them of the upcoming change, what to expect, and instructions on what to do. The more you communicate to your users, the smoother this project will be.
If you have a large and geographically-dispersed organization, you could select OU groups of users at a time or department groups, and coordinate / schedule with users as appropriate.

**(continued on next page…)**

**Method 2: Schedule groups of users to change their password voluntarily**
This is an approach that you will probably need to use with external-only OWA and VPN users, since they do not log on to the domain directly. If you have OWA's change password functionality enabled or have a change password provision in your VPN portal, all you will need to do is schedule with your groups of users and have them go change their password, then report back to confirm it has been updated. As your groups of users update their passwords, you will go through their accounts and uncheck the box for 'Password Never Expires'. Now they are fully managed under the new password expiration policy.

If you do not have an external provision for users to change their own password, this task will be much more difficult and will require you to change the password for them and then call to tell them their new password. You should implement some method of external password change ability for external users prior to placing them under a password change policy, or you are going to really have your hands full come next password change interval.

## 4. Final Thoughts

- Be sure to create a good game plan that includes user awareness and pre-planning, and provide a high level of support availability during the first and second password change periods to answer questions, explaining password requirements, etc. The first and second password change periods after implementing a domain password change policy always carry the highest administrative overhead. After the first couple of password change intervals, users are pretty much adjusted and familiar with the process. If you provide a high level of support initially, you will help cement a good relationship with your users regarding the new password change policy.

- It is always a good idea to set your user's expectations appropriately *before* implementing the password change policy- Good PR is king! Again, *the first two password change intervals following implementation are always the toughest on users and require the most support from IT.* Using a good pre-notification tool like Password Reminder PRO will ensure that your users are always kept informed of upcoming password changes and will keep support incidents low.

- BE SURE to make note of your specific Service and Resource accounts, and set them to not-expire BEFORE implementing your domain password change policy.

- A domain password change policy should be applied uniformly to all users, without exception. If you 'make allowances' for some users, you will eventually have a line of users asking "well, how come so-and-so doesn't have to change their password, but I do?". This is not a road you want to go down, and you should BE SURE to have 100% Executive support and buy-in on the password change policy enforcement before deployment. As a matter of fact, if your Executives do not want to be forced to change their password, neither will your users. If the top of the chain does not help enforce and lead by example it is suggested that you do not bother with implementing the password change policy until you obtain the necessary support. Now, if your company must adhere to Payment Card Industry, Sarbanes-Oxley, HIPAA or other regulatory compliance requirements then it's a no-brainer. Every active user account will need to be managed by the domain password expiration policy and regular password changes will be required.

Our dedicated support team is always available to assist you with setup, installation and deployment of our software during your trial period. Your success is our success!

Provided by:
Enterprise Support Team
**SysOp Tools, Inc**
www.sysoptools.com
Copyright 2007 SysOp Tools, Inc