Preventing Password Expiration Proactively
Table of Contents

1. Password Expiration: Why Should You Care? ............................................. 3
2. How to Tackle the Problem ................................................................. 3
   2.3 Going the Easy Way ......................................................................... 3
   2.4 Coding Your Way Out of It ............................................................. 4
   2.5 Passing the Buck ........................................................................... 4
   2.6 What Matters in a Solution ............................................................. 5
4. About Netwrix Corporation .................................................................... 6
Password Expiration: Why Should You Care?

Password expiration is a well-known pain for IT help desk personnel. Requests to reset expired passwords can constitute a sizable portion of the total help desk workload. Because password expiration is periodic, the help desk tends to be flooded with calls about expired passwords every once in a while.

This issue wastes time and limits productivity, but setting passwords never to expire is not an option. Periodically renewing passwords is not only common sense practice, but often also an important requirement for security compliance.

Barring irresponsibility, users typically let the passwords of their accounts expire because:

- they don’t login interactively (e.g. VPN and OWA users)
- they stay logged on for long periods of time and don’t receive reminders
- they use operating systems other than Windows (e.g. Linux or Mac)

How to Tackle the Problem

Going the Easy Way

Arthur administers an Active Directory domain where most computers run Windows Server 2003 and Windows XP. A few Linux boxes are also joined to the domain, and authentication is transparent on these boxes due to a single sign-on system. To prevent password expiration, Arthur uses built-in Active Directory notification. Of course, that does not cover the Linux users, but they have been instructed to use calendar reminders to warn them when their passwords are about to expire. The Linux users don’t seem to mind, and the reminders help most of the time.

Group Policy is the obvious choice for reminder configuration in an Active Directory environment. In particular, the Interactive logon: Prompt user to change password before expiration option is helpful. It makes sure that during Windows interactive logons, users are prompted to change their password a few days before expiration.

To provide similar prompts for Outlook Web Access users, you need to take additional Exchange configuration steps, which decentralizes the setup of essentially the same feature.

This solution is valid in a Windows-only environment but becomes a lot less attractive as soon as Active Directory-integrated Unix, Linux and Mac hosts come into the picture. Users of these systems will not receive Group Policy-triggered warnings, and the password age of these accounts needs to be tracked specifically.

Another consideration is that the default prompts are not always effective. They are suitable for an informed audience who realize the importance of password policies. Without this knowledge, people tend to ignore the prompts and carry on with their work, letting the passwords expire. In these cases, there should be a notification method informing the user that changing the password is not “just something you do,” but a way to make the workplace more secure.
Coding Your Way Out of It

Bill is in charge of a heterogeneous Active Directory environment comprising Windows, Linux and Mac OS. The share of Linux and Mac boxes is considerable, although thankfully there is little variety in operating system versions. Being a competent coder, Bill has designed and remotely deployed a set of logon scripts for the non-Windows computers that duplicates the functionality of built-in Windows password expiration reminders. The scripts are production-tested and work fairly well, but recently due to an upgrade of the Linux systems it took Bill a whole day to update and debug the scripts.

One way to deal with expiring passwords on non-Windows computers is to deploy scripts or programs that use LDAP to check the state of the account password at logon. This is easier said than done. An administrator tasked with rolling out such a configuration would face the following complications:

- The same logic has to be ported to multiple systems, considering initialization methods, installed software, etc.
- The scripts and programs require testing and support.
- If no centralized software rollout system is in place, this software has to be installed on each computer individually.

As a result, the solution might not prove cost-effective, and the administrator might have to cut the costs by deploying freely available software instead of developing it in-house. In the process, the administrator will sacrifice support, and often reliability.

Passing The Buck

Carol is the administrator of an environment that integrates Windows, Mac, Solaris and Linux computers, some of them operated by remote users. Setting up password expiration warnings on all the computers is impractical and infeasible, so it has been decided that help desk should monitor password age and notify the users in advance when their passwords are about to expire. Carol has equipped help desk with reporting software for the purpose. This proactive measure alleviates the problem but does not remove it — help desk workload is such that notification messages do not arrive as frequently as they should. Carol is researching to find a better, more automated solution.

The administrator might decide that client-side password expiration warnings are just not worth the effort. Then help desk personnel might be charged with using reports on account password state and manually sending email notifications to users whose passwords are about to expire.

On the one hand, this quick and dirty solution has a few benefits:

- It provides control of the state of all account passwords, including the accounts whose owners do receive the expiration warnings.
- It rightly shifts attention from computers to people who use the accounts.
It is easy to find and deploy reporting software that displays the necessary information.

On the other hand, this method has several disadvantages:

- Users who do not receive the warnings are out of the loop, although they could easily tend to reset their passwords themselves.
- Help desk personnel have to spend time tracking password age instead of handling more serious issues.

**What Matters in a Solution**

As these examples show, a good solution to the problem of warning the owners of soon-to-expire passwords should:

- Reliably and flexibly inform users about impending password expiration — the administrator should be able to configure how soon the notification starts and to make the notification messages informative.
- Be platform-independent — the system should work identically on all platforms that the account may be used on.
- Be account-centric, not computer-centric — no client software installation should be necessary; the warnings are directed to the account owner, not to the user of a particular machine.
- Reinforce the notification functionality with reporting tools for help desk personnel — although this is a secondary goal, it can reduce the number of calls.

One way to satisfy these requirements is to design software that:

- Sits in a single place in an Active Directory domain
- Automatically monitors the age of account passwords
- Sends configurable notification messages to the mailboxes of accounts whose passwords are about to expire
- Generates password expiration-related reports for help desk personnel
Fully Automated Approach:
Netwrix Auditor for Active Directory

Netwrix Auditor for Active Directory fits this description perfectly. Its Password Expiration Alerting feature completely automates password expiration monitoring and notification, and generates related reports. Importantly, there is also an alternative freeware tool called Netwrix Password Expiration Notifier which is fully functional and can be used in a production environment with no strings attached, but it lacks several customization-related options of the paid solution’s functionality.

Netwrix Auditor uses email, which has a number of benefits:

- The messages reach the addressees whether they are using a Windows workstation, a Unix box, VPN or Outlook Web Access from home.
- No additional infrastructure configuration is necessary — your environment already has all you need.
- Reports on password expiration can automatically be sent to administrators and help desk personnel.
- The notification messages can be made as informative as necessary.

By providing editable notification templates, Netwrix makes it easy to achieve integration with a self-service password management system (such as Netwrix Password Manager or any other product) that might be deployed in the environment. For that, the notification template should simply include a link to the self-service Web page and possibly a brief set of instructions for the user.

To learn more about the Netwrix Auditor’s Password Expiration Alerting feature, please read the overview of this feature or download a free 20-day trial of Netwrix Auditor for Active Directory.

About Netwrix Corporation

Netwrix Corporation is the leading provider of change auditing software, offering the most simple, efficient and affordable IT infrastructure auditing solutions with the broadest coverage of audited systems and applications available today. Founded in 2006, Netwrix has grown to have thousands of customers worldwide. The company is headquartered in Irvine, California, with regional offices in New Jersey, Ohio, Georgia and the UK.