Lepide Software Private Limited

Helping Administrators to avoid unnecessary User Account Lockups

Lepide User Password Expiration Reminder

The purpose of this White Paper is to illustrate the issues with default password expiration alerts, discussing the ideal solution, and highlighting how LUPER can help the administrators to avoid password reset complaints or account lockups.

2013

1. Abstract

Even though periodic password expiration enhances the security inside an organization's network still it burdens the IT help desk with a lot of password reset complaints. Such tickets are mostly unnecessary as user either has ignored or not received any password expiration alert. In larger organizations, such issues cannot be considered small as they can eat up the precious time and resource of the entire IT support team.

In this White Paper, we'll discuss the password aging, importance of periodic password expiration, issues with the default alert system, and a feasible solution to help the organizations with such unwanted complaints.

2. Password Aging

Password Aging is a standardized concept to decide the age of an account after which its password expires. Usually in Windows environment, the IT help desk configure the server to deliver logon alerts to the users before seven or more days of the password expiry. Users have to change their passwords on time to save their account; else, their account will be locked up because of expired passwords.

Forcing the Active Directory users to change the password regularly over a specific period is one of the essential security policies being employed in the organization. It completely removes the chances of unauthorized password leakage to the outsiders. If not applied intelligently, it often results in unwanted headaches for both the users and IT help desk. The major drawbacks of periodic password expiration are related to the default reminders as users either neglect or don't receive them.

3. Realty of Password Expiration Alerts

Active Directory sends out the Windows logon alerts to notify the active users but this system has significant drawbacks listed herein below.

- Users who don't interactively login to the domain don't receive these alerts because their account is limited to File Share, Citrix, VPN, OWA, or another Web service.
- There is no option to notify the out-of-premises users.
- Always logged in users don't receive the alerts.
- Users of Linux, Ubuntu, Mac or other non-Windows OS doesn't receive logon alerts.
- Requiring administrators to create scripts manually in PowerShell or another scripting engine again need manual tedious working.
- Windows Vista, 7, and 8 doesn't show the logon alerts. Rather they show small balloon pop-ups in the system tray, which can be easily missed by the users. Such notifications are sometimes disabled because of the Windows inactive icon management and thus, users don't receive any password expiration alert.

4. Account Lockup

Users cannot change their passwords on time due to above drawbacks of the default alert system and thus, their passwords will be expired resulting into account lockup. It increases the downtime, hits the productivity, and raise the number of calls for IT help desk. The situation can be worsening for the remote users whose online availability is important for the organization but they're not able to connect with IT staff directly to raise account lockup complaints. IT help desk has to reset the user's password in order to activate the account.

5. Issues of IT Administrators

The organizations don't want the downtime just because of password expiration and they require IT help desk to take feasible steps to avoid the same. Let us have a look at some issues faced by administrators while managing password expiration.

- They don't know what all users have received the password expiration notifications.
- They've to take different steps manually such as keeping a track of the password expiration, passwords to be expired soon, and expired passwords.
- They've to drill down through the intensive log files of Active Directory for creating reports in this regard.
- They've to code complex scripts manually in PowerShell or other programs for emailing password expiration notifications to the users. Such scripts are complex in nature, not customizable, or send the message only once.
- They've to create the scripts for displaying password expiration notification on each non-Windows machine. These scripts have to be tested, maintained and upgraded regularly.

Administrators and their team have to invest many resources in performing above listed manual tasks. This can sometime even create a bottleneck where no other computer issues can be handled in the organization. In order to focus on other important issues and grievances, it's a mandate to have a sophisticated and centralized mechanism to address the significant drawbacks of both the default alert system and administrators' issues.

6. The Ideal Solution

When Active Directory doesn't have any solution and manually created scripts doesn't serve the purpose, the need of a third party innovative solution arises. Such a system should

- send proactive alerts to the users who
  - don't login at the domain interactively as their account is only limited to OWA, File Share, VPN, Citrix, or another Web-based service
  - are logged in always
  - use the non-Windows operating systems
  - doesn't give attention to password alerts during logon or received by an email

    - don’t notice or receive the password expiration alert due to default properties of Windows Vista, 7, and 8
- automatically send the password expiration notifications periodically to the users
- automatically generate the reports of
    - those users whose passwords are going to expire soon
    - users with expired passwords
    - logon failures
    - those users who’ve to change password on next logon
- send above reports automatically the administrators and other intended recipients
- be a centralized place to automatically track the user accounts in all organizational units and domains
- be user friendly for saving the precious time
- send alerts for the critical items to the administrators

7. Lepide User Password Expiration Reminder

Lepide User Password Expiration Reminder (LUPER) tool is a true one-stop solution to address the issues of administrators, override the drawbacks of the default alert system, and has all above discussed features. This software can be installed on any networked machine including normal workstations but needs administrator rights to establish the connection with the servers.

6.1 Proactive Password Expiration Alerts

Lepide User Password Expiration Reminder emails the proactive password expiration alerts to all the active users regardless of their domains, organizational units, account status, login, availability in the premises, and operating systems.

LUPER notifies those users who don’t log in interactively, are logged in always, use non-Windows operating systems, out-of-premises users, and remote users. Administrators can send more than one email between defined intervals and they can even replace the default content with attractive advisory information.

Moreover, one can set the alerts for IT help desk and other recipients notifying any critical situation like details of a user who’ve to change the password on next logon or who’ve to change the password within the specified number of days.

6.2 Reports

LUPER acts as a centralized repository to detect the user accounts of all domains and organizational units at one place. After data collection, it generates following six types of important reports for the administrators that can be exported CSV, PDF and HTML formats.

1. **Soon to expire users**

   This report notifies the administrators about the users whose password is going to expire soon. IT help desk will have a quick track of such users who’ve to change their password.

2. **Users whose password never expire**
   This report lets the administrators to segregate the users whose password will never expire and they'll not give much attention to them as they are added as an exception to password aging.
3. **Users with expired password**
   Some users ignore the password expiration alerts during Windows logon and notification emails. As a result, their passwords can be expired resulting into their account lockups. This report alerts the administrators to be ready and take necessary steps in order to avoid the unnecessary complaints related to these two points.
4. **Recent logon failures**
   This report alerts the administrators about the recent logon failures, which can be a valuable hint for the account lockup. Instead of letting the user with multiple logon failures to call the help desk, the support team itself calls the person to resolve its problem instantly.
5. **Password Change Reports**
   This report informs the administrators about the users who've changed their passwords on time.
6. **Change Password at Next Logon Users**
   This report alerts the administrators about the users whose password has to be changed on next logon. If these users have not changed their passwords then their accounts will be locked up. Administrators will get enough time to track how many accounts they've to reactivate.

6.3 Scheduling of Reports

Administrators can schedule the automated delivery of all reports to themselves and other intended recipients at the defined interval. These reports are easy to understand and well formatted, thus IT help desk will have a quick overview about all situations related to the password expiration.

About company

Lepide Software Pvt. Ltd. is a leading provider of Network management, Server management and IT management solutions. The company has offered a number of cutting edge technological tools to serve these areas. Lepide User Password Expiration Reminder is yet another valuable addition to the list of software products from the company that has won accolades from the industry. The strength of the company lies in deep industry experience and expertise of technical workforce that helps in producing cost-effective solutions. To know more about the company visit:

http://www.lepide.com/

Sales, Support Contact information

Contact:

+ 1-800-814-0578

For Sales: sales [@] lepide.com

For Support: support [@] lepide.com

For Resellers: resellers [@] lepide.com