ManageEngine
ADSelfService Plus

Prevent Active **Directory password expiration with SMS** and **email alerts**

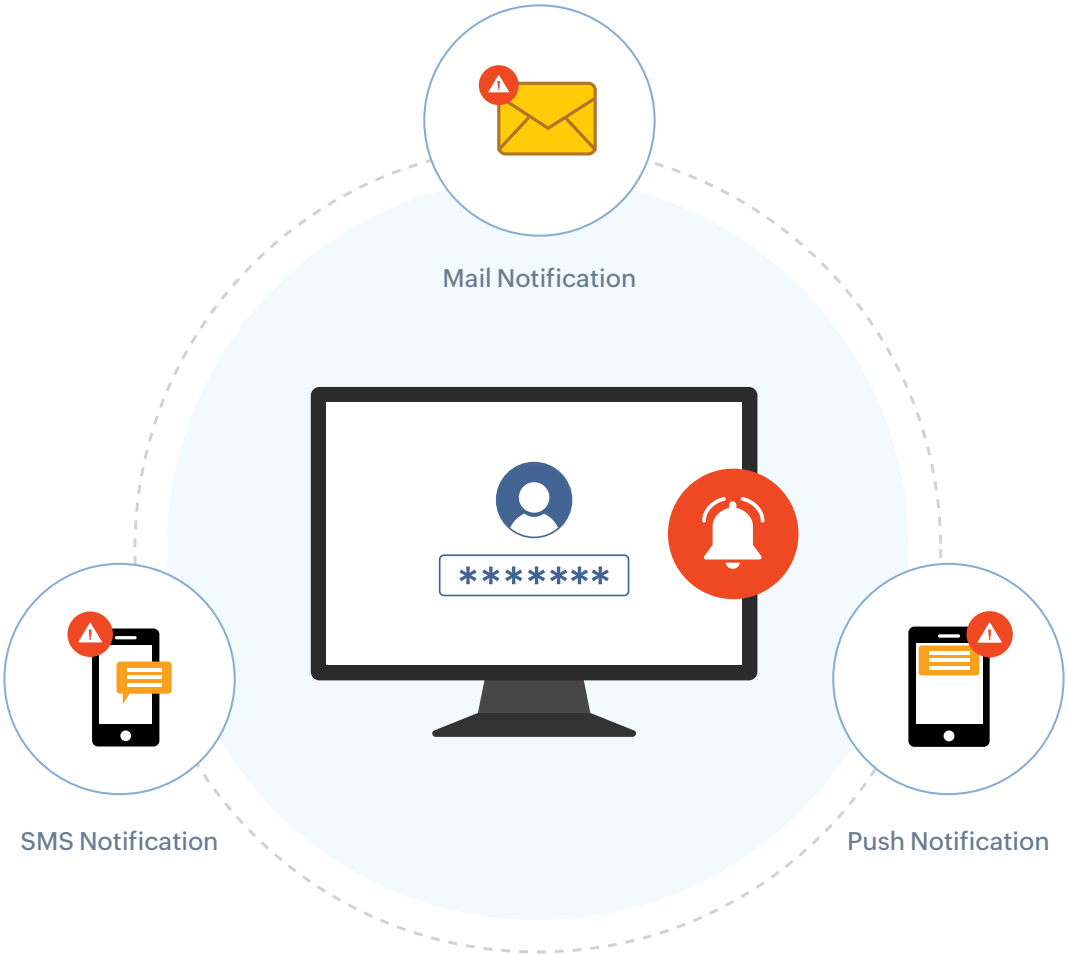


Table of Contents

Undeniable IT expenses due to expired passwords

According to 2018 research by Forrester, organizations spend around $1 million on resolving password-related help desk calls. Users often unintentionally let their Active Directory (AD) passwords expire because they:

- Have AD accounts only for VPN or Outlook Web Access (OWA), so they never log on interactively to see Windows notifications.
- Don't notice the password expiration warning in the taskbar.
- Use machines that aren't running Windows, so they don't receive AD password expiration notifications.

While enabling password expiration makes some extra work for IT teams, organizations can't just completely disable this option because passwords that never expire lead to security loopholes. Changing passwords periodically is essential as it prevents cybercriminals from gaining access to network resources, even if they have stolen user credentials.

How IT admins can deal with password expiration

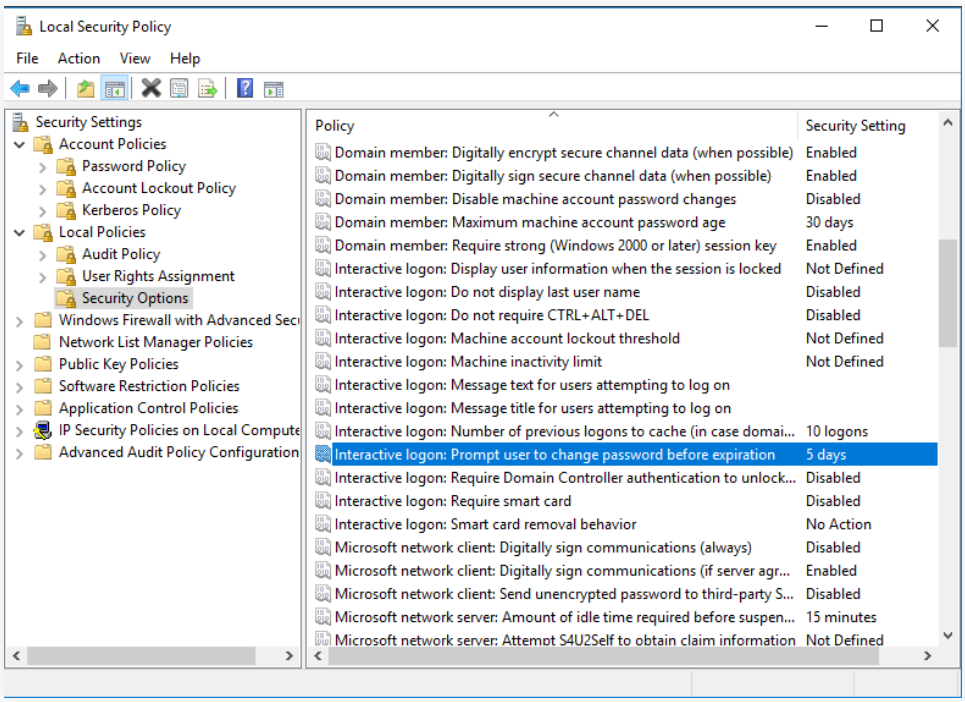
In a complete Active Directory environment, the most obivious choice for setting up password expiration reminders is via a Group Policy Object (GPO), although some IT admins use PowerShell codes to send out periodic password expiration reminders. Though both these techniques have their advantages, they also have their own set of challenges.

Sending password expiration reminders via GPO

Group policy password expiration notifications sent using the **Interactive logon: Prompt user to change password before expiration group policy setting** helps administrators notify users via a balloon tip before their password is due to expire. The major drawback of this setting is that Microsoft's password expiration balloon tip isn't very noticeable, so most users will miss the warning and let their account password expire. This setting also only applies to Windows machines, so it's not suitable in a workplace featuring macOS and Linux machines. Further, remote users won't receive a password expiration alert with this policy in place.

Steps to send password expiration reminders via GPO

1. Go to **Start > Run** and type **gpedit.msc** to open the GPO editor console.
2. Click OK.
3. Navigate to **Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options.**
4. Choose the **Interactive Logon: Prompt user to change password before expiration** policy.
   The default setting is enabled to send notifications 14 days prior to the password expiration date via GPO.
5. To modify the setting, right click on the policy and make the required updates.



Sending password expiration reminders via PowerShell

PowerShell scripts enable admins to send password expiration notifications to users via the email address configured in the AD. Although PowerShell scripts overcome a few limitations of the interactive logon policy setting by sending email alerts to all users, there is a catch. Coding is error-prone and time-consuming. A simple typo in the code could mean the script never runs, or worse, the notifications are sent to the wrong users. Hence, it is imperative to be extra cautious while sending password expiration reminders via PowerShell.

Steps to send password expiration reminders via PowerShell

1. Use the PowerShell script given below to send password expiration notification to the users a week before the expiration date:

```
Import-Module ActiveDirectory

$SevenDayWarnDate = (get-date).adddays(7).ToLongDateString()
$MailSender = " Password expiry <email address>"
$Subject = 'Your account password is expiring soon'
$EmailStub1 = 'Hello User! A gentle reminder that your account password'
$EmailStub2 = 'will expire in'
$EmailStub3 = 'days on'
$EmailStub4 = '. Please contact the administrator to change your password.'

$SMTPServer = 'smtp.gmail.com'
$SMTPPortNo = '587'
$SMTPCredUserName = 'MySmtpUser@zoho.com'
$SMTPCredPassword = 'Ho@g2sFGTrlzy7'
$SMTPCredSecurePassword = ConvertTo-SecureString $SMTPCredPassword -AsPlainText -Force
$SMTPCredentials = New-Object -TypeName System.Management.Automation.PSCredential -
ArgumentList $SMTPCredUserName, $SMTPCredSecurePassword

$users = Get-ADUser -filter {Enabled -eq $True -and PasswordNeverExpires -eq $False -and
PasswordLastSet -gt 0 } `
-Properties "Name", "EmailAddress", "msDS-UserPasswordExpiryTimeComputed" | Select-Object
-Property "Name", "EmailAddress", `
@{Name = "PasswordExpiry"; Expression = {[datetime]::FromFileTime($_."msDS-UserPasswordExpir
TimeComputed").tolongdatestring() }}

foreach ($user in $users) {
if ($user.PasswordExpiry -eq $SevenDayWarnDate) {
$days = 7
$EmailBody = $EmailStub1, $user.name, $EmailStub2, $days, $EmailStub3, $SevenDayWarnDate,
$EmailStub4 -join ' '
 Send-MailMessage -To $user.EmailAddress -From $MailSender -SmtpServer $SMTPServer
-Subject $Subject -Body $EmailBody -UseSsl -Port $SMTPPortNo -Credential $SMTPCredentials -Verbose
}
else {}
}
```

Even a basic code is complex to script and debug each time. Customizing this further to send password expiration notifications regularly with custom messages and for the required number of times or days is tough.

The ideal solution: Notify users about password expiration, for free

Businesses need a solution that can help:

- Eliminate help desk tickets due to password and account expiration.
- Generate reports on the delivery status of password expiration reminders.

ADSelfService Plus' Password Expiration Notifier

ADSelfService Plus' Password Expiration Notifier helps administrators by sending reminders about password expiration to users via email, SMS, and push notification. It is highly unlikely that a user will respond to a one-time password change alert, so ADSelfService Plus enables alerts to be sent at specific intervals.

For instance, admins can choose to send a password expiration alert when it is 15 days before the password expires; then send a second reminder 12 days before expiration; a third, when it's five days from expiration; a fourth, at three days; and a fifth and final reminder a day before the password expires. Admins can even make the content of the email message more imperative with each reminder.

Key features of Password Expiration Notifier

1. **Comprehensive audit reports:** Schedule and distribute reports to managers and administrators on the delivery status of all the password expiration notifications sent. Password Expiration Notifier also offers in-depth audit reports on the self-service activities performed by users; all reports can be exported in PDF, CSV, XLS, HTML, or CSVDE format as well.

2. **OU and group-based policies:** Control to whom and when the expiration notifications are sent by creating policies based on AD domain, organizational unit (OU), and group memberships. Admins can create multiple policies and set up a separate, less intrusive password expiration reminder policy for managers and C-levels similar to password expiration reminders via GPO .

3. **Customizable messages:** Customize email and SMS messages to make them more personal or imperative by adding specific instructions and images, those which are not easy to miss unlike the balloon tip password expiration notifications sent via gpo.

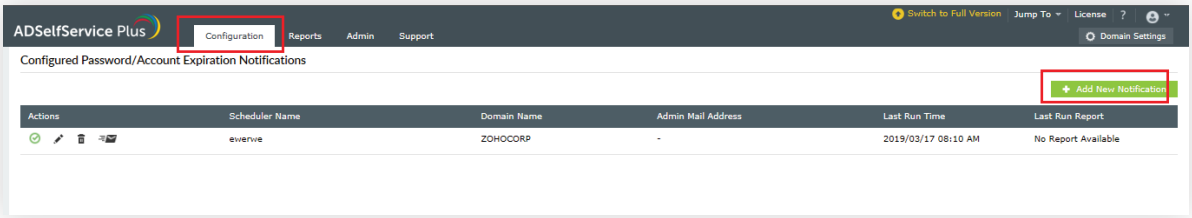
4. **Automated account expiration reminders:** Automate account expiration reminders, along with the usual password expiration alerts. Admins can also notify managers about other users' account expirations.

5. **Simple deployment:** Get the scheduler up and running in seconds. As this free tool uses the existing domain password policy, there are no changes made to AD or Group Policy infrastructure, and no extra steps required to get started.

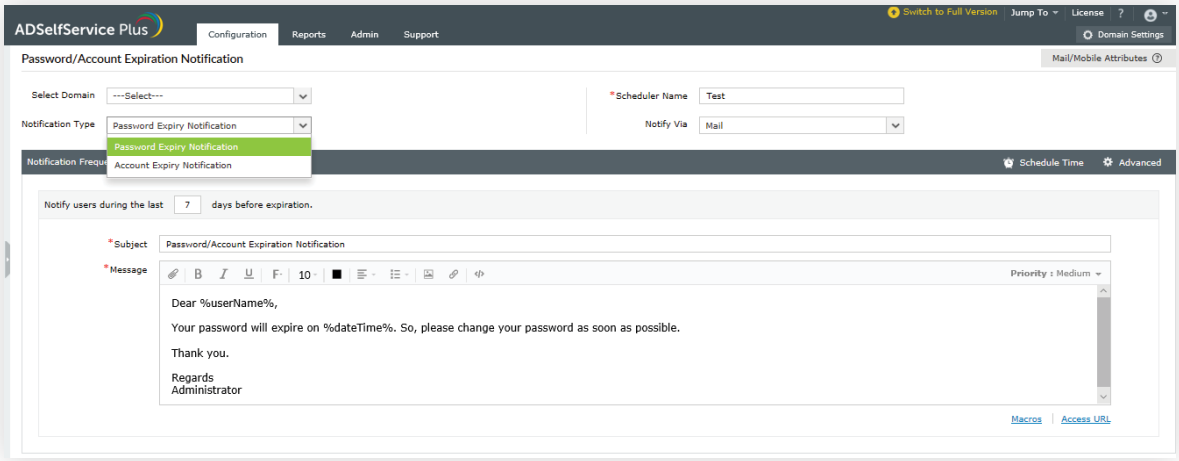
How to configure ADSelfService Plus' Password Expiration Notifier

It only takes a few steps to configure ADSelfService Plus' Password Expiration Notifier:

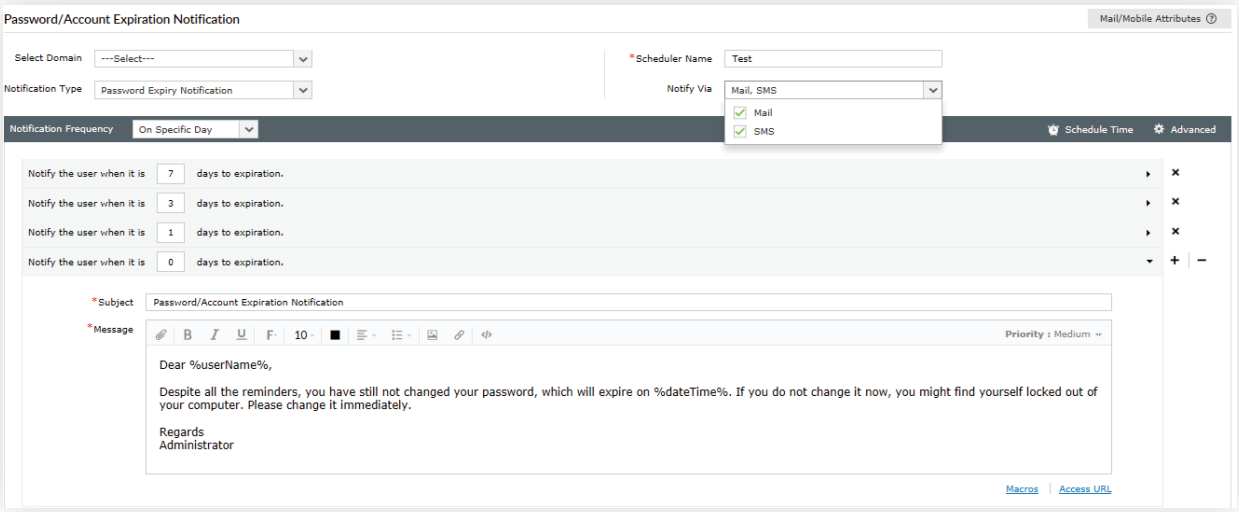
1. Download our free tool, Password Expiration Notifier.
2. Double-click the downloaded **EXE file**. The InstallShield Wizard for ADSelfService Plus will walk you through the entire installation process.
3. After the installation process is complete, access ADSelfService Plus' console using the configured access URL (<protocol>://<host_name>:<port_number>).
4. Go to **Configuration > Add New Notification.**



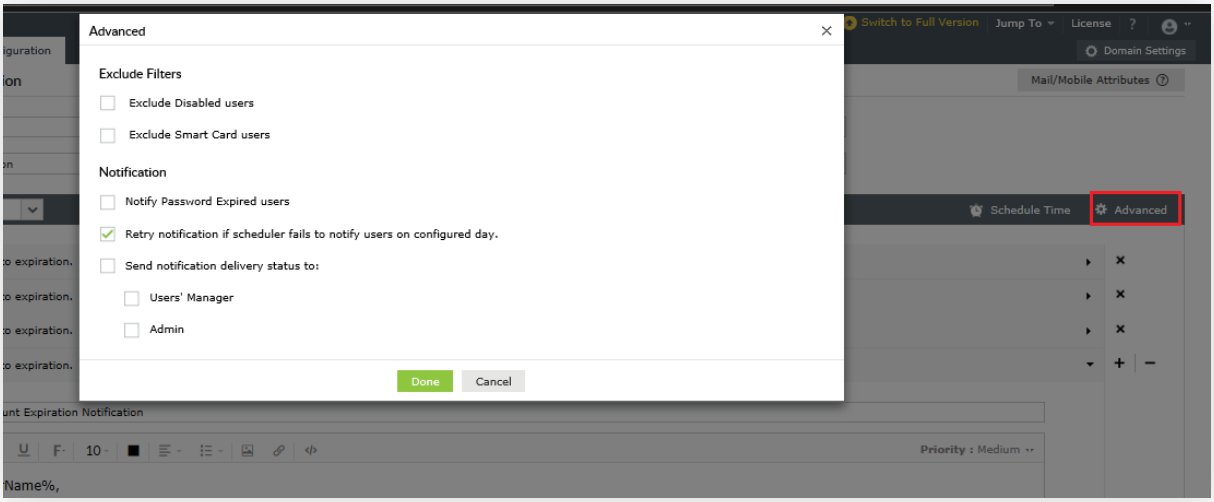
5. Enter the **Scheduler Name** and select the **Notification Type.**



6. Select the domains, OUs, or groups for which you want to send notifications.
7. From the Notify via drop-down, select the medium through which you want to send notifications (SMS and/or email).
8. Set the **Schedule Time** and configure the **Notification Frequency** as:
   - **Daily**
   - **Weekly**
   - **On specific days:** For instance, you can choose to email the first password expiration reminder when it's 15 days to password expiration; the second, when it's 10 days to password expiration; the third, when it's seven days; the fourth when it's three days; and so on.



9. Click the **Advanced** link. In the pop-up window that opens, you'll see options for excluding disabled users or smart card users from receiving expiration notifications.



10. You can also send a **notification delivery status** message to users' managers or anyone with an admin account.

11. Click **Save.**

Why get the full version of ADSelfService Plus?

Password Expiration Notifier is a free tool. However, if you want more features, try ManageEngine's ADSelfService Plus, our self-service password management and single sign-on solution. Here's a sneak peek at ADSelfService Plus' features:

a. **Self-service password reset and account unlock:** Empower users to securely reset passwords for Windows, Office 365, and other applications in a matter of seconds. Allow users to unlock their locked-out accounts for Windows, G Suite, and other applications without IT assistance.

b. **Multi-factor authentication:** Secure local and remote access to Windows, macOS and Linux operating systems with an additional layer of authentication. Enable MFA for VPN providers, endpoints supporting RADIUS authentication, Microsoft Remote Desktop Gateway (RDP) and Outlook Web access (OWA) logins.

c. **Real-time password sync and single sign-on:** Synchronize AD password resets and other changes in real-time. Enable secure, one-click access to enterprise applications through single sign-on.

d. **Granular password policy enforcer:** Enforce password policies across Windows and enterprise cloud apps with advanced filters to blacklist dictionary words, patterns, etc.

e. **Directory self-update and employee search:** Keep user profiles up-to-date by enabling employees to self-update their information as well as pull up their coworkers' profile information, such as their email address and phone number.