CloudSavvy IT

How to Disable & Fix Password Expiration in Windows Server

ANTHONY HEDDINGS
JUN 8, 2021, 2:00 PM EDT | 2 min read

Windows Server passwords expire. After a while, your password will be invalid, and you will need to "contact your IT administrator" to reset it manually. But what happens when *you* are the IT administrator?

The Problem

By default, Windows Organizations have password expiration turned on. The idea is that you must change your password every so often (The default is only 42 days.) to minimize the impact of security breaches. This is a good idea for large organizations, but if you're just trying to run a machine with Windows Server, it can be quite annoying.

Even worse, if you're new to Windows hosting, you might have missed the prompt about it expiring if you didn't log in recently. By default, nothing is set up to warn you if you don't sign in regularly. This can actually completely lock you out of your account, requiring a server restart into rescue mode.

Luckily, it's pretty easy to turn off the feature before it's a problem, and if you did get locked out by password expiration, booting into rescue mode will fix the issue by allowing you to reset the password from outside of
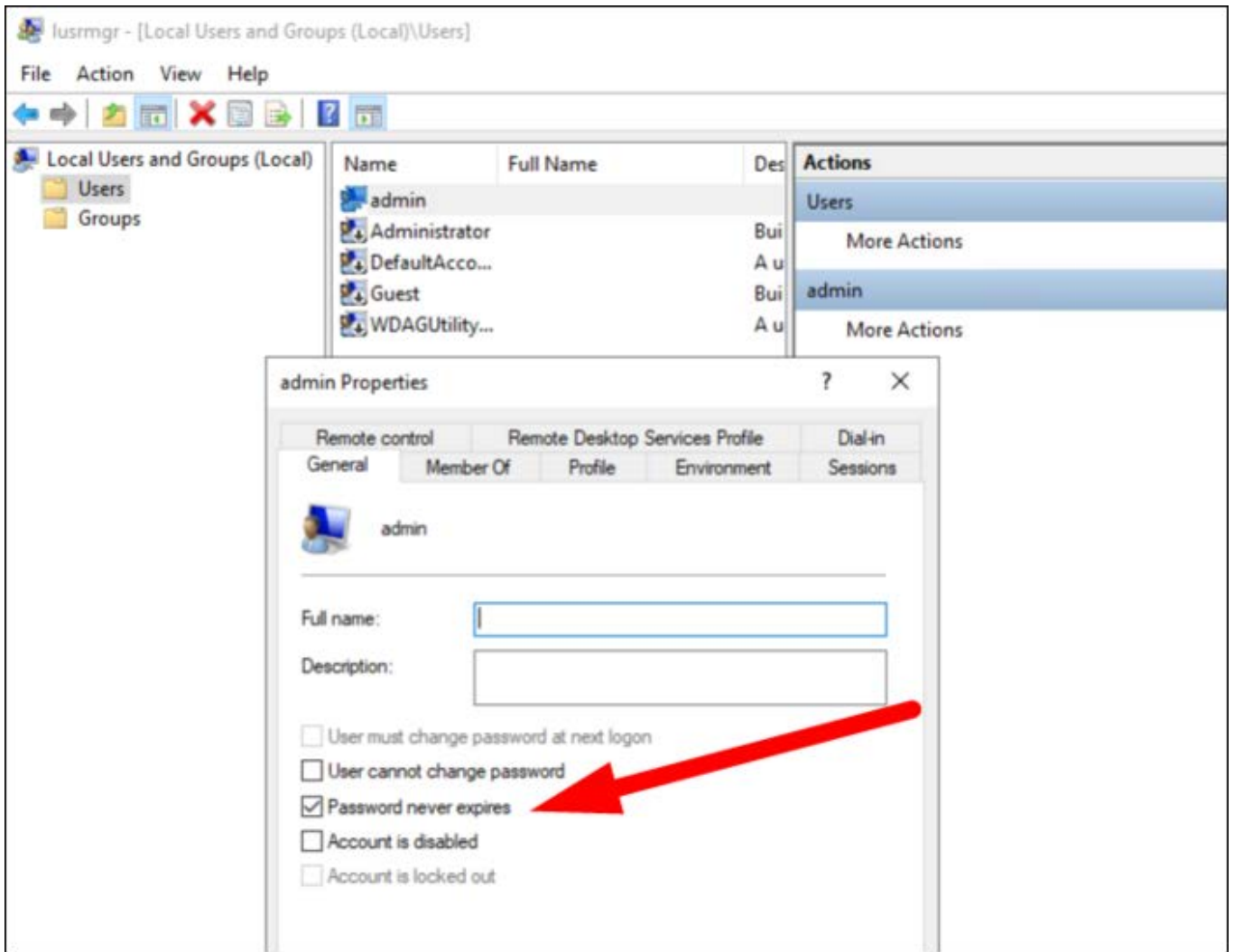
the operating system.

Fixing It Early

The way to prevent passwords from expiring is to just disable them using the Local Users and Groups control panel. Open it up by searching for **lusrmgr.msc** in the start or run menus.
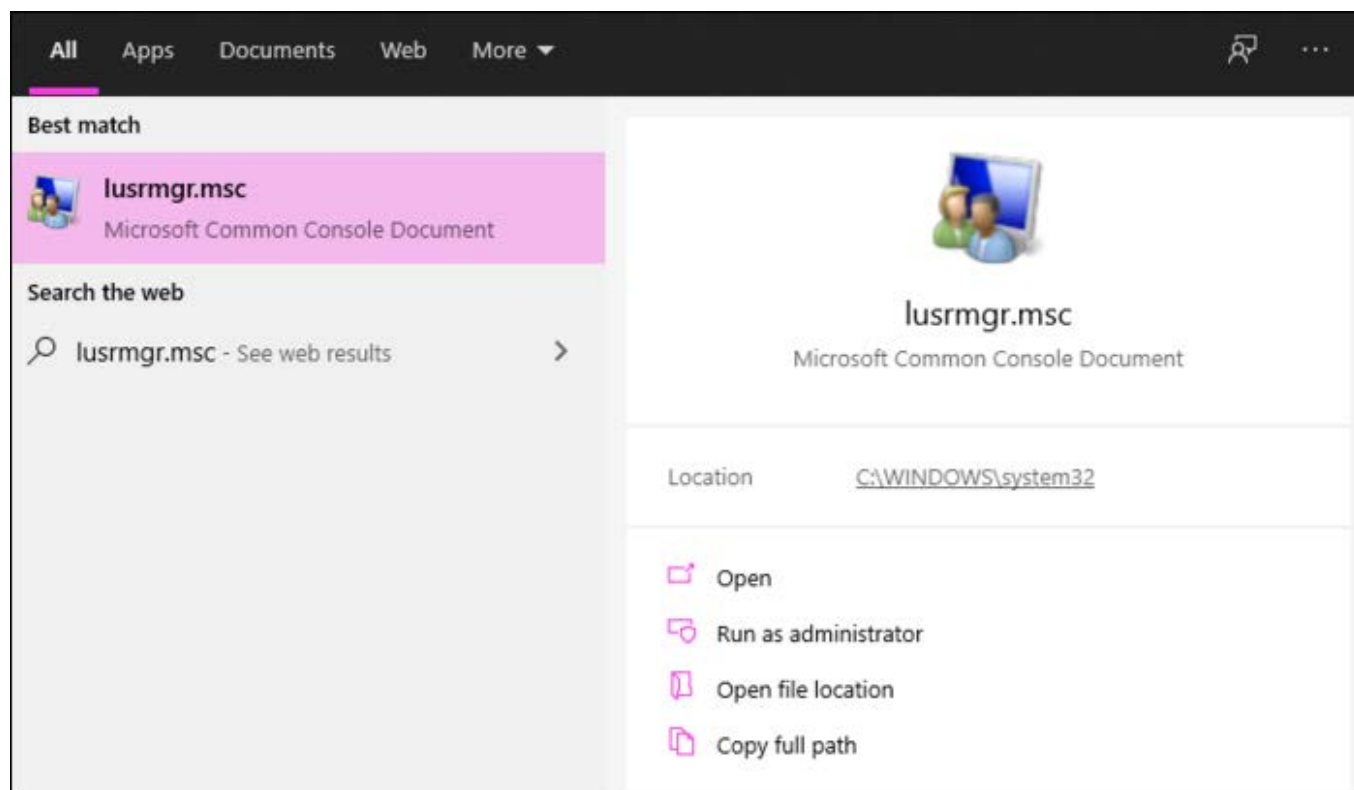
ADVERTISEMENT

Click on "Users" and find your user account. Right-click and view properties, and then check "Password Never Expires" under the settings.

Alternatively, you can do this manually from the command line:

```
wmic UserAccount where Name='username' set PasswordExpires=False
```

What to Do If You've Already Been Locked Out

If you've already been locked out, you might be getting an error that says *"You must change your password before logging on for the first time. Please update your password or contact your system administrator."*

Unfortunately, this means that you've probably been locked out unless you're able to reset the password from elsewhere in your organization. If you don't have outside access, this might have just cut off your only credentials for access to the server.

You might not need RDP credentials, though. Some server providers offer direct KVM access, which could allow you to bypass your remote login and change the password from there. You should try this first, as it will result in no downtime.

Resetting with Win PE

You will need to boot the server into a rescue operating system. Many providers should have this option—for example, OVH allows you to change the netboot mode to a Windows Preinstallation Environment, or Win PE. This allows you to use tools like NTPWEdit to modify SAM files directly.

To use it, you'll need to open the SAM file, unlock the user that you want to modify, and click "Change Password." Enter it twice and click "Save Changes."
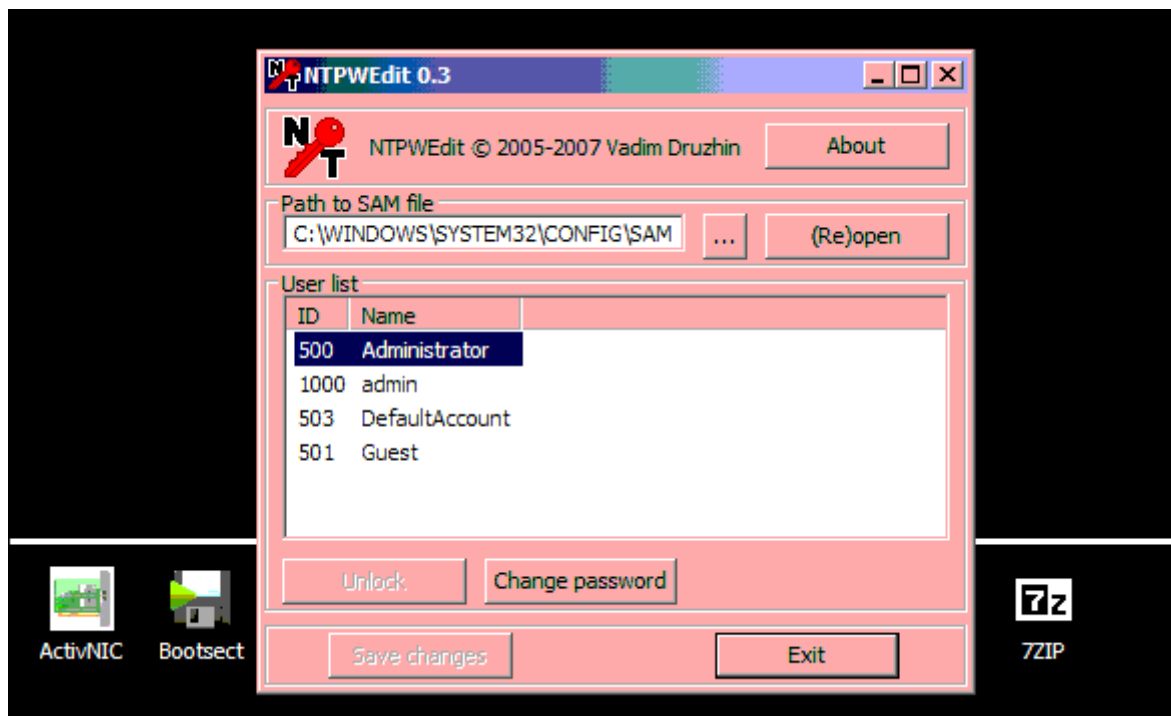
Resetting with Linux and chntpw

Alternatively, you could be given a Linux-based rescue system like `rescue64-pro`. In this case, you'll need to mount the Windows drive and change it manually with `chntpw`.

List the disks and mount the main partition:

```
fdisk -l
mount /dev/sda4 /mnt
```

Navigate to the location of the SAM file and run `chntpw`

```
cd /mnt/Windows/System32/config
chntpw -l SAM
```

Then, follow the prompts to clear the password for your account.

```
# chntpw -u admin SAM
chntpw version 1.00 140201, (c) Petter N Hagen
Hive <SAM> name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 686c <lh>
File size 65536 [10000] bytes, containing 8 pages (+ 1 headerpage)
Used for data: 361/39344 blocks/bytes, unused: 35/13648 blocks/bytes.


================== USER EDIT ====================


RID     : 1000 [03e8]a
Username: admin
fullname:
comment :
homedir :

00000221 = Users (which has 3 members)
00000220 = Administrators (which has 2 members)

Account bits: 0x0010 =
[ ] Disabled        | [ ] Homedir req.    | [ ] Passwd not req. |
[ ] Temp. duplicate | [X] Normal account  | [ ] NMS account     |
[ ] Domain trust ac | [ ] Wks trust act.  | [ ] Srv trust act   |
[ ] Pwd don't expir | [ ] Auto lockout    | [ ] (unknown 0x08)  |
[ ] (unknown 0x10)  | [ ] (unknown 0x20)  | [ ] (unknown 0x40)  |

Failed login count: 0, while max tries is: 0
Total   login count: 5

- - - - User Edit Menu:
 1 - Clear (blank) user password
(2 - Unlock and enable user account) [seems unlocked already]
 3 - Promote user (make user an administrator)
 4 - Add user to a group
 5 - Remove user from a group
 q - Quit editing user, back to user select
Select: [q] >
```

You'll need to log back in with the blank password and change it to something secure.

ANTHONY HEDDINGS

Anthony Heddings is the resident cloud engineer for LifeSavvy Media, a technical writer, programmer, and an expert at Amazon's AWS platform. He's written hundreds of articles for How-To Geek and CloudSavvy IT that have been read millions of times. **READ FULL BIO »**