

The following is some helpful information for resetting the password on Windows 2000, 2003 and 2008 Server running Active Directory.

Please note: Password Reset will allow you to log in locally via Directory Service Restore Mode. This is what Password Reset is designed to do. We do not support the following information nor do we guarantee it. If you are not proficient with Windows Server, we recommend contacting a local computer technician.

For Windows Server 2003 and 2008, scroll further down the page.

Windows Server 2000

- Reset your password using our Windows Password Reset disk from www.Password-Reset.com.
- Reboot, hit F8, and enter "Directory Service Restore Mode". The machine will boot up as a standalone server without any Active Directory support.
- When the login screen appears, hit CTRL-ALT-DEL and log in as "Administrator" with no password. This is the MACHINE Administrator account, and does not have the ability to modify anything specific involving the Active Directory information, although it can backup and restore the physical files which contain the AD databases.
- Run "regedit". Navigate to **HKEY_USERS\.Default\Control Panel\Desktop** and change the following values:

Value	Original	Change to
SCRNSAVE.EXE	logon.scr	cmd.exe
ScreenSaveTimeou t	900	15
ScreenSaveActive	<i>Maybe 0 or 1</i>	1

- Reboot normally. When the box appears asking you to hit CTRL-ALT-DEL to log in, just wait. After 15-30 seconds you will see a command prompt appear (since that is the screensaver.)
- In the command prompt, type the following command:

MMC DSA.MSC

Note: There is a space character between the "mmc" and the "dsa.msc". Also, note that the DSA.MSC file is usually

located in the SYSTEM32 subfolder of your WINDOWS or WINNT folder.

DSA.MSC is actually the executable name for Active Directory Users and Computers, which in turn is the main tool for managing users, groups and computers in Windows 2000 Active Directory.

This should bring up the management console where you can edit users' passwords, including the password for the Administrator account.

- After resetting the Administrator password, exit the management console and type the command EXIT in the command prompt window.
- Hit CTRL-ALT-DEL and log into the DOMAIN Administrator account using the new password!

Don't forget to undo the changes you made to the registry (see step #4, lamer note), or you will always have a command prompt with Domain Administrator rights appear whenever somebody logs out.

Windows Server 2003 & 2008

You might also want to check out the script available that is supposed to automate this process. You can find the link at the bottom of this page.

- Reset your password using our Windows Password Reset disk from www.Password-Reset.com.
- Get two tools provided by Microsoft in their Resource Kit: SRVANY and INSTSRV. Download them from here: <http://www.password-reset.com/downloads/srvany.zip>
- Restart Windows in Directory Service Restore Mode. Note: At startup, press F8 and choose Directory Service Restore Mode. It disables Active Directory. When the login screen appears, log on as Local Administrator. You now have full access to the computer resources, but you cannot make any changes to Active Directory.

You are now going to install SRVANY. This utility can virtually run any programs as a service. The interesting point is that the program will have SYSTEM privileges (LSA) (as it inherits the SRVANY security descriptor), i.e. it will have full access on the system. That is more than enough to reset a Domain Admin password. You will configure SRVANY to start the command prompt (which will run the 'net user' command).

- Copy SRVANY and INSTSRV to a temporary folder, mine is called D:\temp. Copy cmd.exe to this folder too (cmd.exe is the command prompt, usually located at %WINDIR%\System32).
- Start a command prompt, point to d:\temp (or whatever you call it), and type:
instsrv PassRecovery "d:\temp\srvany.exe" (change the path to suit your own).

It is now time to configure SRVANY.

- Start Regedit, and navigate to:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\PassRecovery
- Create a new subkey called Parameters and add two new values:
name: Application
type: REG_SZ (string)
value: d:\temp\cmd.exe

name: AppParameters
type: REG_SZ (string)
value: /k net user administrator 123456 /domain

(replace 123456 with the password you want). Keep in my mind that the default domain policy require complex passwords (including digits, respecting a minimal length etc) so unless you've changed the default domain policy use a complex password such as P@ssw0rd

- Now open the Services applet (Control Panel\Administrative Tools\Services) and open the PassRecovery property tab. Check the starting mode is set to Automatic.
- Go to the Log On tab and enable the option Allow service to interact with the desktop.
- Restart Windows normally, SRVANY will run the NET USER command and reset the domain admin password.
- Log on with the Administrator's account and the password you've set in step #2.
- Use this command prompt to uninstall SRVANY (do not forget to do it!) by typing:

net stop PassRecoverysc delete PassRecovery
- Now delete d:\temp and change the admin password if you fancy.

There is also a script that has been created for this process as well. We have not tested this in any way and do not guaranteed or endorse it. We provide it strictly as a convenience. You can download the script here: http://www.password-reset.com/downloads/dc_pass_reset.zip