

Windows Server Password Recovery Techniques

Courtesy of Daniel Petri

<http://www.petri.co.il>

The LOGON.SCR Trick

To successfully reset the local administrator's password on Windows NT and some versions of Windows 2000 follow these steps:

1. Install an alternate copy of Windows NT or Windows 2000.

You must install this instance of NT/2000 on a **different folder** than WINNT, otherwise you'll end up with the same bad situation. Use ALTWINNT for example.

It is best that you install the alternate instance of the OS into a **different partition** than the one you have your original installation. You'll delete this folder anyway, and it's best that you just format that partition after you're done. Formatting the partition will be much easier than deleting individual files and folders.

Also, if you lost your password on NT - install a new instance of NT, not Windows 2000, as doing so will ruin your old NT installation (because of the difference between the NTFS versions). Same goes for W2K, XP and Windows Server 2003. Always install the same OS.

Note: On Windows NT 4.0 machines that were installed out-of-the-box you **do not** have to install a fresh copy if you still have access as a regular user to the system. E.g. if you can log-on as a regular, non-administrator user, you can still manipulate the file's permissions. This is simply because NT's default permissions are set for Everyone - Full Control. This is **not** true on W2K/XP/2003 machines.

Another note: Reader **Mike** wrote:

In the article you mention installing the OS on top of the existing OS to do the logon screensaver manipulation.

I wanted to mention that this can also be accomplished by removing the hard drive, placing it as a slave on another computer (XP and W2K play nicely) and then accessing the file system. Of course you need a second computer, but for some folks it may be an easier solution.

Thanks,

Mike

That's correct, and it will work for you unless you converted the disk to a dynamic disk, on the original OS. In that case you will no longer be able to boot the old OS, even if you do manage to access the files from the other computer.

2. Boot the **alternate** install.

Windows Server Password Recovery Techniques

Courtesy of Daniel Petri

<http://www.petri.co.il>

3. Use Control Panel/System/Startup (for NT) or Control Panel/System/Advanced/Startup and Recovery for W2K to change the default boot instance back to your original install.

Lamer note: If you don't do that you'll end up booting into the alternate installation next time you turn on your computer. You don't want that, do you?

4. Open Explorer. Browse to your original Windows NT/2000 folder, navigate to the %systemroot%\System32 sub-folder.

Lamer note: %systemroot% is a system variable used to point to the folder where NT/2000 is installed, usually \WINNT in NT/2000, or \WINDOWS in XP/2003.

5. Save a copy of LOGON.SCR, the default logon screen saver, anywhere you like. Just remember where you've placed it. You can also just rename the file to something you'll remember later, I user LOGON.SC1.

Lamer note: To rename a file use the REN command in the Command Prompt window, or just select the file in Windows Explorer and press F2.

6. Delete the original LOGON.SCR from the %systemroot%\System32 sub-folder. It is not necessary to delete the file if you renamed it, you can leave it there.

Note: You might not be able to delete the LOGON.SCR file because of permission settings. Regular users can only read and execute the file, not delete it. If that is the case (and it is in W2K, XP and Windows Server 2003) then you need to take ownership of the file and give the EVERYONE group FULL CONTROL permissions.

Lamer note: In order to take ownership of a file right-click it, select Properties, select the Security tab, click Advanced, and then click on the Owner tab. Select one of the users found in the list, click ok all the way out.

In order to change the LOGON.SCR permissions follow the previous instructions, in the Security tab click Add and browse to the Everyone group. Add it and make sure you give it Full Control. Click Ok all the way out.

7. Make a copy CMD.EXE in the %systemroot%\System32 sub-folder. CMD.EXE is located in %systemroot%\system32.

Lamer note: In order to copy a file via GUI, select the file, right-click and chose Copy, then go to the destination folder, right click the folder name and select Paste. You can also use the keyboard by typing CTRL-C to Copy, CTRL-V to Paste.

8. Rename the copy of CMD.EXE to LOGON.SCR.

Lamer note: See step #5.

9. Shutdown and restart your computer. Boot into the **original** install.

Windows Server Password Recovery Techniques

Courtesy of Daniel Petri

<http://www.petri.co.il>

10. Wait for the logon screen saver to initiate - around 15 minutes. Oh, and no, do NOT move your mouse while you wait, duh...

After the screensaver is initiated, instead of running the normal LOGON.SRC actual screensaver, it will run the renamed CMD.EXE file (which is now called LOGON.SCR), and will actually open a CMD prompt in the context of the local system account.

In step #7 you could have used EXPLORER.EXE instead of CMD.EXE, and in that case a My Computer window will pop up.

Note: As noted earlier on this page, there is a way to make the wait time shorter, but you'll need to dig into the Registry for that.

11. Open the CMD.EXE prompt (it should already be opened if you've used CMD.EXE in step #7) and type:

```
net user administrator 123456
```

This will reset the local administrator (or domain admin if you are doing this trick on a DC) password to *123456*.

Lamer note: You can, of course, use ANY password you want...

12. Delete the LOGON.SCR from %systemroot%\System32
13. Rename the saved default screen saver from step 5 back to LOGON.SCR.
14. If you wish to remove the alternate install:

- Delete its' folder.
- ATTRIB -R -S -H c:\BOOT.INI
- Edit c:\BOOT.INI and remove the alternate install's entries.

If you've used a different partition to install the alternate install then now you can simply delete or format that partition if you don't need it anymore, plus edit c:\BOOT.INI and remove the alternate installation entries.

This trick has been tested a zillion times. Don't bother to tell me it doesn't work, it does (for Windows NT and some versions of Windows 2000), and that's a fact.

Windows Server Password Recovery Techniques

Courtesy of Daniel Petri
<http://www.petri.co.il>

Reset Domain Admin Password in Windows 2000 AD

Note: In order to successfully use this trick you must first use one of the password resetting tools available on the [Forgot the Administrator's Password?](#) page.

The reason for that is that you need to have the local administrator's password in order to perform the following tip, and if you don't have it, then the only method of resetting it is by using the above tool.

Read more about that on the [Forgot the Administrator's Password?](#) page.

Update: You can also discuss these topics on the dedicated [Forgot Admin Password - Related Discussions](#) forum.

Lamer note: This procedure is NOT designed for Windows XP, nor will it work on Windows Server 2003. For that you should read the [Forgot the Administrator's Password? - Change Domain Admin Password in Windows Server 2003 AD](#) page.

Reader John Simpson added his own personal note regarding the changing of Domain Admin passwords on Windows NT domains and Windows 2000 Active Directory domains ([HERE](#) 🌐). I will quote parts of it (thanks John!):

As stated above, the very useful "[Offline NT Password & Registry Editor boot disk](#)" will only let you reset the password for the MACHINE Administrator account, not the DOMAIN Administrator account. As you probably know, on a Windows 2000 server which is an Active Directory controller, you CANNOT log into any machine-level account. Which means that resetting the MACHINE Administrator password is pretty much useless.

Or so it would seem. It turns out that "Directory Service Recovery Mode" uses the MACHINE-level accounts, since the whole point of this mode is that the AD control databases may be corrupted and you need a way to manually edit them (presumably using some high-priced third-party software package...)

I (John Simpson - DP) was able to reset the password on the DOMAIN Administrator account using the following procedure:

1. Use the Offline NT Password & Registry Editor disk to reset the MACHINE Administrator password to "no password".
2. Reboot, hit F8, and enter "Directory Service Recovery Mode". The machine will boot up as a standalone server without any Active Directory support.

Windows Server Password Recovery Techniques

Courtesy of Daniel Petri

<http://www.petri.co.il>

3. 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.

4. Run "REGEDIT.EXE" (without the quotes). Navigate to

HKEY_USERS\Default\Control Panel\Desktop

Lamer note: Make sure you write down the default values BEFORE changing them. You could also just PRINT SCREEN your registry editor display. The best option is to just backup the values to a .REG file by selecting the DESKTOP key and then selecting EXPORT from the FILE menu.

After you made sure you know what the default values are, change the following values:

SCRNSAVE.EXE - change from *logon.scr* to *cmd.exe*

ScreenSaveTimeout - change from *900* to *15*

ScreenSaveActive - change to *1* (if it wasn't *1* already)

5. 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).

6. In the command prompt, type the following command:

MMC DSA.MSC

Lamer 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.

More lamer notes: 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.

Windows Server Password Recovery Techniques

Courtesy of Daniel Petri

<http://www.petri.co.il>

5. After resetting the Administrator password, exit the management console and type the command EXIT in the command prompt window.
6. 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.

Reset Domain Admin Password in Windows Server 2003 AD


Note: In order to successfully use this trick you must first use one of the password resetting tools available on the [Forgot the Administrator's Password?](#) page.

The reason for that is that you need to have the local administrator's password in order to perform the following tip, and if you don't have it, then the only method of resetting it is by using the above tool.

Read more about that on the [Forgot the Administrator's Password?](#) page.

Update: You can also discuss these topics on the dedicated [Forgot Admin Password - Related Discussions](#) forum.

Lamer note: This procedure is NOT designed for Windows XP since Windows XP is NOT a domain controller. Also, for a Windows 2000 version of this article you should read the [Forgot the Administrator's Password? - Change Domain Admin Password in Windows 2000 AD](#) page.

Reader Sebastien Francois added his own personal note regarding the changing of Domain Admin passwords on Windows Server 2003 Active Directory domains ([HERE](#) ). I will quote parts of it (thanks Seb!):

Requirements

1. Local access to the Domain Controller (DC).
2. The Local Administrator password.
3. Two tools provided by Microsoft in their Resource Kit: SRVANY and INSTSRV. Download them from [HERE](#) (24kb).

Step 1

Restart Windows 2003 in Directory Service Restore Mode.

Windows Server Password Recovery Techniques

Courtesy of Daniel Petri

<http://www.petri.co.il>

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.

Step 2

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:

A screenshot of a Windows command prompt window. The text inside the window reads: `instsrv PassRecovery "d:\temp\srwany.exe"`. The window has a standard Windows XP-style title bar and navigation buttons.

(change the path to suit your own).

It is now time to configure SRVANY.

Start Regedit, and navigate to

A screenshot of the Windows Registry Editor. The address bar shows the path: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\`. The window has a standard Windows XP-style title bar and navigation buttons.

Create a new subkey called Parameters and add two new values:

A screenshot of the Windows Registry Editor showing two registry values. The first value is: `name: Application`, `type: REG_SZ (string)`, `value: d:\temp\cmd.exe`. The second value is: `name: AppParameters`, `type: REG_SZ (string)`, `value: /k net user administrator 123456 /domain`. The window has a standard Windows XP-style title bar and navigation buttons.

Replace 123456 with the password you want. Keep in my mind that the default domain policy

Windows Server Password Recovery Techniques

Courtesy of Daniel Petri
<http://www.petri.co.il>

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.

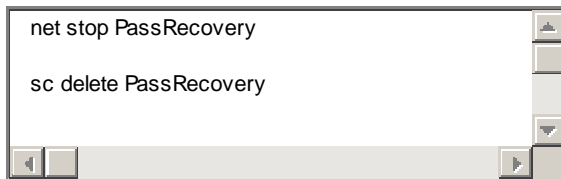
Go to the Log On tab and enable the option Allow service to interact with the desktop.

Restart Windows normally, SRVANY will run the NET USER command and reset the domain admin password.

Step 3

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 PassRecovery
sc delete PassRecovery
```

Now delete d:\temp and change the admin password if you fancy.

Done!

Supplement

Robert Strom has written a cool script that will completely automate this process. He wrote:

"My script is really just an automation of his process which performs all the post cleanup of itself. Launch one script and it's all done. No manual registry entries, the service is created, the service settings are all imported into the registry, etc."

Download it from [HERE](#) (186kb).

Note that you still need physical access to the DC and the ability to log on locally as the local administrator. If you do not have the local administrator's password use the following tip: [Forgot the Administrator's Password?](#)

Thanks Robert!

Acknowledgments

This tip was compiled and written with the help of Antid0t, Robert Strom and Sebastien Francois. Thank you all!

Windows Server Password Recovery Techniques

Courtesy of Daniel Petri

<http://www.petri.co.il>

How To Reset the Domain Admin Password Under Windows 2003 Server

Written by Sebastien Francois, February 2004.

Abstract

I have recently installed a Windows 2003 Server at home and I set up a local domain using Active Directory features. Everything worked fine until I changed the Domain Admin password. It seems that I mistyped the new password twice (which I would attribute to the previous heavy night out), and, well, I could not log on the Domain Controller anymore (I did not have a backup admin account, I do now!).

A few tricks about resetting the Domain Admin Password on Windows 2000 Server have been published, but after Microsoft strengthened some security aspects on Windows 2003 Server, those hacks do not work anymore.

After struggling a few days, I finally managed to reset the domain account and I am going to present the trick to you in this paper.

This trick has a few important requirements, be sure you meet them before yelling at me.

This paper does NOT intend to serve any malicious sort of hackers, but just lousy administrators (like **me**).

Requirements

These are compulsory!

You need:

1/ Local access to the Domain Controller (DC).

2/ The Local Administrator password.

3/ Two tools provided by Microsoft in their Resource Kit: SRVANY and INSTSRV. Download them from [here](#).

The Local Administrator account is also called Directory Restore Administrator or Machine Account. The password is set at Windows installation. It is possible to reset this password using some (free) recovery tools.

The trick has been tested on a domain with a single DC. If your domain has multiple DCs, it should not matter which one you decide to use.

Let's get started

Windows Server Password Recovery Techniques

Courtesy of Daniel Petri
<http://www.petri.co.il>

Step 1

Restart Windows 2003 in Directory Restore Service Mode.

Note: At startup, press F8 and choose Directory Restore Service 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.

Step 2

You are now going to install SRVANY. This utility can virtually run any programs as an NT Service. The interesting point is that the program will have SYSTEM privileges (as it inherits 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\srwany.exe"

(Replace d:\temp with your folder name)

It is now time to configure SRVANY.

Start regedit, and open the key
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 new_password

Windows Server Password Recovery Techniques

Courtesy of Daniel Petri

<http://www.petri.co.il>

'net user username password' is the command line utility to set a new password. Replace new_password with the password you want. Keep in my mind that some domain policies require complex passwords (including digits, respecting a minimal length etc.)

Now open the Services applet (Control Panel\Administrative Tools\Services) and open the PassRecovery property tab. Check the starting mode is set to Automatic.

Show the Log On tab and enable the option Allow service to interact with desktop.

From now on, anytime you restart Windows, SRVANY will run the netuser command and reset the domain admin password.

Step 3

Restart Windows in normal mode and wait for the login screen. You will not see the command prompt running the net user command as it is displayed on another desktop. But no worries, the command is still executed in the background.

Log on as Administrator on your domain by using the password you set above. The system should grant you access. If not, go back to Step 2 and check you did not mistype any commands or values.

When the desktop is displayed, you should see a command prompt. This is the one started by SRVANY.

Use this command prompt to uninstall SRVANY (do not forget to do it!) by typing:

```
net stop PassRecovery (, then:)
```

```
sc delete PassRecovery
```

Now delete d:\temp and change the admin password if you fancy.

Voila!