

# Emergency Repair Disk (ERD)

Lance Jensen

## INTRODUCTION

A current Emergency Repair Disk (ERD) is one of the vital tools needed to maintain a Windows NT system. Unfortunately, most Windows NT sites do not maintain their ERDs because many administrators have never been taught how to use them. We would like to help correct that situation.

In this article the designation **%systemroot%** will refer to the system folder. The default name is **WINNT**, but whoever actually installed Windows NT on your system may have given it a different name.

Many of the files in the **%systemroot%** tree are hidden files, and many are read-only. To see hidden files, start Windows Explorer, go to the Menu Bar and click "View", "Folder Options", and the "View" tab. In the Advanced Settings box, under "Hidden files", click the "Show all files" button, then OK. You will now be able to see all files. Before you can copy or edit a read-only file, you must right-click the file, then click "Properties". Under the General tab, in the Attributes section, uncheck the Read-only box.

## WHAT THE ERD IS

The ERD is a floppy disk containing the files in the **%systemroot%\repair** folder, which are the configuration files and Registry information. If your Registry or startup environment become damaged in any way, the ERD will usually be able to fix it. However, the ERD is not a substitute for a full backup. It's more like a "Backup Lite" which can frequently save you from having to do an entire restore from backup.

The files **sam.\_** and **security.\_** on the ERD are often not kept updated, because they can be too big to fit on a floppy. You probably won't see this except on a server with over a thousand users and groups. If these files are too big for a floppy, you can back them up them using your regular backup utility or the regback.exe utility in the Windows NT Resource Kit, and you can save copies in a special folder on the disk.

I strongly recommend keeping several ERDs for each machine. The first one should be made when you first install Windows NT. If you did not make one at that time, now is a good time to do it. Then make a second copy and store one off-site. As you expand and change your Windows NT system, keep these original ERDs as a safety factor. For convenience, you could also create a second repair folder (let's call it **\repair2**) and copy the original files from **\repair** into it.

If you do back up the **sam.\_** and **security.\_** files (which you should do if you can), you may some day find that you can no longer fit all of the files on a floppy disk. Remember that the entire contents of the **%systemroot%\repair** folder is copied to the ERD, so you must keep its size under 1.44MB. Should the folder grow too large, take the ERD from the original Windows NT installation (or from **\repair2**) and copy only the **sam.\_** and **security.\_** files into the **%systemroot%\repair** folder. The folder should now be small enough to make an ERD. If it's not, you need to reduce the size of **setup.log**. Edit **setup.log** and locate the line

## Emergency Repair Disk (ERD)

Lance Jensen

**[Files.WinNt]**, which is followed by a long list of file names. You can safely delete any of these file names that do not begin with **%systemroot%\SYSTEM32\**. At some point in this list you may find a line **[Files.InRepairDirectory]**; do not delete anything after this line!

There are two things you should keep in mind:

- The files **sam.\_** and **security.\_** contain your security database. If these files are included on the ERD, then your system could be invaded if a criminal should get his hands on it. Keep all copies of the ERD safe and secure, from theft as well as from damage.
- When you do a repair from an ERD, the **sam.\_** and **security.\_** files may be replaced with the ones from the ERD. If these files were too large to fit on the ERD, you have to recover them from someplace else. The easiest handling for this is a third folder, **\repair3**, in which you copy just the **sam.\_** and **security.\_** files.

### MAKING AN ERD

The ERD is created using the **RDISK** utility. You should make a new one whenever you make any significant change to the system, such as adding a new application or Service Pack, or changing the Registry. This is the procedure to use if you are including the security data on your ERD:

- If you have not already done so, create **\repair2** and copy the files from **\repair** into it. If you do not have an original **ERD**, make one now by using these steps, but leave off the **/S** switch in step 3.
- Click Start, go to Programs, and click Command Prompt. Type **RDISK/S <ENTER>**.
- When prompted "Do you want to create an Emergency Repair Disk?", click "Yes". Follow the prompts.
- Label and date the **ERD**.

The **/S** switch in step 2 is necessary because the files in the **%systemroot%\repair** folder are not updated when your system is modified; you have use **RDISK** to do it manually. The **/S** switch tells **RDISK** to update the repair files, including the **sam.\_** and **security.\_** files.

This is the procedure to use if you are not including the security data on your ERD:

1. If you have not already done so, create **\repair2** and copy the files from **\repair** into it. If you do not have an original ERD, do steps 6 to 9 now to make one.
2. Click Start, go to Programs, and click Command Prompt.
3. Type **RDISK/S- <ENTER>**. (The **/S-** switch updates the files, but does not proceed to create an ERD).

## Emergency Repair Disk (ERD)

Lance Jensen

4. Copy the **sam.\_** and **security.\_** files from **\repair** into **\repair3**.
5. Copy the **sam.\_** and **security.\_** files from **\repair2** into **\repair**.
6. Type **RDISK <ENTER>**.
7. Click the "Create Repair Disk" button.
8. Follow the prompts.
9. Label and date the ERD.

The ERD just created can be used to get your system running again if something goes wrong while modifying your system. Now go ahead and make the system changes. When you have finished and tested and you are satisfied that the change is done, repeat the steps to update your system with your new modifications, and make two new ERDs. The second ERD should be stored with your offsite backups. If you don't keep offsite backups, you may not want a second ERD; I like to have one in case the first copy gets damaged.

### IS THE ERD REALLY NEEDED

You may never have made an ERD, or you might lose it, or it might get damaged. If you ever have to do a repair without an ERD, you have several options.

Sometimes you can do a repair without any ERD at all. If the repair procedure can find your Windows NT install directory, it may be able to directly access the repair directory. Sometimes it works, sometimes it doesn't.

If that fails, you may be able to create a new ERD. First you need a floppy disk that was formatted on a Windows NT system. If the **%systemroot%\repair** folder is on a FAT partition, you can boot to a bootable DOS floppy and copy the repair files to the new floppy. Some are hidden, so be sure you get them all. The files are:

**autoexec.nt**  
**config.nt**  
**default.\_**  
**ntuser.da\_**  
**sam.\_**  
**security.\_**  
**setup.log**  
**software.\_**  
**system.\_**

It's harder to access the folder if it's on an NTFS partition, but here are some ways to do it.

- There are applications available that run under DOS and can read NTFS partitions. You can use one of these to create the floppy as described above.
- You could move the hard disk to another machine that is running Windows NT and create the floppy there.

## Emergency Repair Disk (ERD)

Lance Jensen

- You could make another Windows NT installation on the same machine, boot into it, and make your new floppy.
- Last, you may be able to copy the files from a backup tape. You might restore `%systemroot%\repair` folder, or copy it to another machine.

If all of this fails, you must reinstall Windows NT. As you can see, it's a lot simpler to make sure you always have a current ERD.

### RUNNING A REPAIR

Someday you may find your Windows NT system behaving oddly. Perhaps when you boot up, it will fail, complaining that some system file is missing or failed a check, or that it can't find the boot sector. Maybe you'll suffer a power surge or a virus or hack attack and find your applications won't start or you can't log in. Now what do you do?

This is what Microsoft designed the ERD to handle. You could reinstall everything, from Windows NT up through all of your applications and data (hope it was backed up!), but it is much easier to do a repair, if you have a current ERD. You will need the Windows NT Installation CD-ROM, the three bootable Windows NT Setup floppy disks, and the ERD.

Insert Setup Disk #1 and turn on the computer. When prompted to do so, insert Setup Disk #2. Now you will get the Welcome to Setup screen. This gives you the options to Install Windows NT, Update Windows NT, or Repair Windows NT. Press R to select Repair.

Next you get the Repair Options list. The options are:

- \* Inspect Registry Files
- \* Inspect Startup
- \* Verify Windows NT System
- \* Inspect Boot

By default, all of these options are selected. You must de-select any you do not want by highlighting it and pressing enter. How do you decide what to select? Well, here's what they do:

- **Inspect Registry Files** is used to repair the Registry hives. If you don't have a current ERD, do not select this option, because it will "roll you back" to the date of the ERD. Any system changes you have done since the ERD was made will disappear; any applications you have installed since that time will lose their Registry entries, and probably won't run any more. Remember, changes to the Registry can make your system completely unusable. If you do select this option, it will offer you a sub-menu which is a list of Registry hives:

## Emergency Repair Disk (ERD)

Lance Jensen

**SYSTEM (System Key)**  
**SOFTWARE (Software Key)**  
**DEFAULT (Default User Profiles)**  
**NTUSER.DAT (New User Profiles)**  
**SECURITY (Security Key)**  
**SAM (SAM Database)**

If you know enough about the Registry, you may know that the problem you are repairing is caused by a particular hive. If that's the case, select the file or files for that hive. But watch out for the Security and SAM files. Remember from the first article that these files might not be backed up on your ERD. If that is the case, do not select Security or SAM!

- **Inspect Startup Environment** replaces Windows NT startup files as needed from the Windows NT installation CD-ROM. Verify Windows NT System Files does a CRC (Cyclic Redundancy Check) on the Windows NT files. In essence, a CRC done on a file produces a number called a Checksum. If the file is changed in any way, the Checksum will be different. The correct Checksums for the files are stored in SETUP.LOG. If the CRC produces a different Checksum, you will be told the file name and asked if you want to replace it.
- **Inspect Boot Sector** checks and repairs the boot sector. I've never come across a situation where selecting this option would cause damage. In fact, aside from the Inspect Registry Files, these options should be safe to select, as long as you don't skip the last step below, reinstalling any Service Pack.

When you've finished selecting options, you highlight Continue and press enter. This brings you to the Mass Storage Detection menu. Just as it says, this tells the repair to detect your mass storage devices. Even though it does add a few minutes to the procedure, I recommend you always select it. In many cases, if you do not select it, the repair process won't be able to find your CD drive, and you'll have to start over.

Next you are prompted to insert Setup disk #3. After that you will be asked if you have an ERD. Press enter if you do, or Esc if you don't. Esc tells the repair to try to locate %systemroot%\Repair folder and use the files there in place of the ERD. This can be a lifesaver, but don't count on it working. Many problems that require repair also make it impossible to access these files.

If you have an ERD, you will now be prompted to insert it. The repair process will then display a list of suspect Registry files which will be replaced. You can override the selection of any file by removing the X next to it, but don't make any changes unless you know what you are doing.

If you selected Verify Windows NT, this is where it will be done. Just follow the prompts. If any file does need to be replaced, you will be prompted to insert the Windows NT Installation

## Emergency Repair Disk (ERD)

Lance Jensen

CD-ROM. Let it spin up to speed before continuing, or you'll get an error message. When this procedure finishes, you will be prompted to remove the floppy disk and CD-ROM and restart.

When the system comes back up, there is one more important step that is very commonly skipped. Reinstall your latest Service Pack. The repair replaces files from the Windows NT Installation CD-ROM. These are the original files, before any Service Packs. If you don't do the reinstall, you will probably have a mix of file versions, some from the original build, some from the Service Pack. System performance will be unpredictable.

I have mentioned the possibility that your SAM and Security files might be too large to fit on a floppy disk. It turns out the Software file may also be too large. Microsoft has a utility called RegClean which may shrink your Software file enough to make an ERD. RegClean is currently being upgraded, but you can find it here when it's re-posted:

<http://www.microsoft.com/ntserver/nts/exec/vendors/freeshare/Maintnce.asp#registry>

There are some other Registry tools at the same location; take a look, they might be just what you need.

For a while, the LS-120 looked like a good option for those whose files are too big to make an ERD. The LS-120 is a removable disk the same size as a floppy disk, but it holds 120MB. The LS-120 drive will read and write standard 1.44MB floppies as well as LS-120 disks. If your BIOS will support an LS-120 as drive A:, then one would think you should be able to use an LS-120 as an ERD. The problem is, it doesn't work. Although the BIOS recognizes the LS-120 as drive A:, and the setup starts normally, when the time comes to insert the ERD, Windows NT can't access the LS-120. Apparently the install procedure uses its own floppy driver which naturally will not recognize an LS-120. I see no reason why the install procedure could not be modified to use the driver which the BIOS supplies.

### ERD SECURITY

You all know you need to keep the ERD floppy disks secure, because anyone can read your security data from them. There is another security measure you should take to protect your repair data: Change the directory permissions on the **/repair** folder to allow only an administrator to access it. Here are the steps:

1. In Windows NT Explorer, right-click the %systemroot%\repair folder.
2. Click Properties, then the Security tab, then the Permissions button.
3. For any name except System and Administrator (domain or local), highlight the name and click Remove. You may also find CREATOR OWNER; I see no problem leaving that one, but it's not necessary.
4. If either remaining name does not have "Full Control (All) (All)", highlight that name and use the "Type of Access" pull-down menu to set "Full Control".
5. Check the "Replace Permissions on Existing Files" box. Click OK.

## Emergency Repair Disk (ERD)

Lance Jensen

6. If you have created \repair2 or any other folders to hold repair files, do this procedure on them.

### CD REPAIR

Normally you need to have the installation CD to complete a repair, but there is a way to get around it. On the Setup #2 floppy disk is a file Setupdd.sys. If you replace this file with the Setupdd.sys from the Service Pack you currently have installed, then you can run Repair without a CD. However, you will only be able to run the "Inspect Registry Files", "Inspect Startup" and "Inspect Boot" options; "Verify Windows NT System" still requires the installation CD-ROM. Rather than alter your original Setup floppy, you should make a copy and modify that. In fact, I strongly recommend you never use the original floppies, except to make copies to use during installations and repairs.

### SERVICE PACKS

Service Packs update Windows NT, which means some of your system files will be different versions from those you originally installed. The repair procedure may see these files as corrupt, and prompt you to replace them. This is why you must use an ERD made after installing the Service Pack.

If you have Service Pack 2 or later, you also need to make a copy of the Setup #2 floppy and copy Setupdd.sys from the Service pack. This is because Setupdd.sys compares the dates of your existing files to the dates of the files on the original CD-ROM. If any are different, you are prompted to replace them; and if you do so, you end up with the pre-Service-Pack files. The Setupdd.sys file in the Service Packs does not do this date check.

If you don't have an ERD made after the Service Pack was installed, use the Uninstall feature from the Service Pack before doing the repair or, if your Windows NT is on the C: partition, do a repair using the \repair folder on C:. (just answer "no" when Repair asks if you have an ERD.)

If you don't have a current ERD and you can't boot up, it is possible to use an ERD if it is from an identical installation of Windows NT on some other machine. Be warned that any difference however small between the two machines may cause problems. But if you don't have even this option, then you have to do an "update". This restores your no-Service-Pack version of Windows NT. After it finishes, reapply the Service Pack and make an ERD. There are Microsoft articles that explain this in detail for Service Pack 3:

<http://support.microsoft.com/support/kb/articles/q146/8/87.asp>

And for Service Pack 4:

<http://support.microsoft.com/support/kb/articles/q196/6/03.asp>

# Emergency Repair Disk (ERD)

Lance Jensen

## WHEN TO MAKE AN ERD

Obviously, whenever you make a change to the system. If you add a user or install an application, or if you add a new user or computer to a network, make a new ERD. But if the machine is a server on a network, you should make a new ERD at least once a week. Yes, every week. This is because of Windows NT security: It changes the System ID (SID) of each workstation every two weeks.

You could make the ERD manually. You should be doing regular backups; you can make an ERD at the same time. You can also set up an automatic update by scheduling RDIDK to run at some particular time, say every Friday night. You do this with the AT command at the command prompt. Click Start, go to Programs and click Command Prompt. Then enter "AT /?" To list the instructions for the AT command.

## MORE YET

In spite of everything you've tried, your Emergency Repair files still won't fit on a floppy disk. Your system is at risk, and possibly your job as well. Isn't there anything you can do?

Yes, there is. It takes a bit of work, and possibly some new hardware, but I have done this myself, and it works. However, it does involve rebuilding your Windows NT system, either reinstalling everything or reformatting and restoring from backup, but in the long run it will save you a lot of time, especially if the machine in question is a server with hundreds of users.

## OVERVIEW

I'm offering two routes here: The easier-to-accomplish, minimal change setup, and a full-blown "start from scratch". You will probably not want to use the full-blown route unless you are setting up a new system. In both routes we will be setting up your system so that it has a large boot/system partition with a primary Windows NT installation, and a second partition with a secondary Windows NT installation. The full route calls for a third partition for applications, and a fourth partition for data. This is a minimum; you may want to have several data partitions. For more information about partitions and why applications and data should be on separate partitions, see our articles from our Web site:

Configuring Your Partitions:

<http://www.diskeeper.com/tech-support/articles/art-0008.htm>

Multiple Boot Systems:

<http://www.diskeeper.com/tech-support/articles/art-0013.htm>

Efficient NTFS Partitions:

<http://www.diskeeper.com/tech-support/articles/art-0022.htm>

## FULL BLOWN ROUTE

First, back up everything. Everything! Now install a new disk drive on an existing computer. Create a 2GB bootable partition at the beginning of the disk and format it NTFS with a cluster

## Emergency Repair Disk (ERD)

Lance Jensen

size of 4096. I have heard that there is a tool that will create the boot sector, but haven't tracked it down. At worst, you can create the boot sector using the Windows NT setup disks.

Shut down the computer and reconnect the new drive as the Primary Master. This is usually done by setting jumpers on the disk; see the owners manual. Install this disk as Drive 0. Now install Windows NT without reformatting. This will give you an NTFS format partition C:, which will hold your primary Windows NT installation.

When the installation is complete, make 2 ERDs and label them "Initial Primary Installation". Then set the size of your paging file. It should be at least 10% larger than the total RAM. Go to Control Panel, double-click System, select the Performance tab and click Change. Set the initial and maximum sizes of the paging file to the same value (so the paging file will not grow or shrink) and click Set. Reboot.

Install the Diskkeeper defragmenter and defragment C:, set the boot-time consolidation of the paging file, and reboot. This will give you a contiguous paging file. You need to use Diskkeeper for this because only Diskkeeper can defragment the paging file.

Now create another 2GB partition, preferably on another disk, and format it NTFS with a cluster size of 4096. Install Windows NT to that partition, and create your application and data partitions. When you have finished, you should have all partitions created and in their permanent form. Make 2 ERDs and label them "Initial Secondary Installation". This is your secondary installation, which you can use to do most repairs and recoveries should you have problems with Windows NT. If you are using a Service Pack, you should install it now to your secondary installation. Run RDISK/S, then make another set of ERDs and label and date them. Your secondary installation is now complete.

If you are restoring your system from backups rather than reinstalling everything, you should now restore everything, including your primary Windows NT, then boot to your primary installation. Now you need to update your old disk configuration to include the new partition where you have the secondary installation. Go to Disk Administrator and click Partition, Configuration, Search, and "Yes" in the warning box that pops up. This will search the disks and list the existing disk configurations. When the "Get Previous Disk Configuration" box appears, select the configuration from the secondary installation and click OK.

If you are building your system from scratch, boot to the primary installation and install the applications. Whenever you are given an option of where to install them, select your application partition instead of C:. After you have installed all of the applications, install the Windows NT Service Pack (if any) which you use.

Make another set of ERDs, label them "Primary Installation" and date them.

Last step: Run RDISK/S- to update the primary installation's repair files. Create a folder \Primary Repair on the partition containing the secondary Windows NT installation. Copy the

## Emergency Repair Disk (ERD)

Lance Jensen

contents of C:\WINNT\repair to the new \Primary Repair folder. Make a new set of backup tapes.

### MIMIMAL ROUTE

Do the backup, new disk, and initial Windows NT installation as described above. Create the second partition and install your secondary Windows NT installation. Make ERDs for both installations. Now install your backup software to the secondary Windows NT installation and restore your original Windows NT from your backups to C:. Boot back to C:, create the partitions you need and restore your applications and data from backups.

Update your old disk configuration to include the new partition where you have the secondary installation. Go to Disk Administrator and click Partition, Configuration, Search, and "Yes" in the warning box that pops up. This will search the disks and list the existing disk configurations. When the "Get Previous Disk Configuration" box appears, select the configuration from the secondary installation and click OK.

Now do the "Last step" above, running RDISK and making the \Primary Repair folder. Don't forget to install the Service Pack (if needed) to the secondary installation, and make ERDs for the secondary installation.

### RECOVERING

Now, you will have to do your maintenance chores regularly. Update the primary installation's repair data weekly, and whenever you add or remove software, and don't forget to copy the \repair files to \Primary Repair. Run RegClean a couple of times a year. Keep your backups up-to-date, including a full backup of the primary Windows NT partition. If you update Windows NT with a new service pack or a new version, update your secondary installation as well. Do this and you will be ready.

OK, here's the fun part. Disaster strikes, so what do you do? You run a repair on your primary installation, but when asked if you have an ERD, you reply No. The repair then attempts to use the contents of the \repair folder, and usually succeeds.

What if the **\repair** folder is corrupt? Boot to the secondary installation, copy the files from \Primary Repair to \repair and try again. What if the problem is a corrupted system file? Boot to the secondary installation, copy the affected files from the secondary to the primary, and reboot.

What if it's major corruption involving many files, or the MFT itself is corrupt? Boot to the secondary installation and restore C: from your backup. What if the whole computer got burned up in a fire? Put together a new computer and follow the Minimal-Change Route, restoring from your off-site backups.

## **Emergency Repair Disk (ERD)**

**Lance Jensen**

Do you see the advantages here? No matter what happens, you can have your system fully restored in just minutes, once you have replaced any damaged hardware. That's worth spending a couple of hours to set up.