Jim Rome's NT Protection Tips

I have learned these lessons the hard way. More than once. So I recommend that you protect your NT system by using these tips.

Keep an up-to-date emergency repair disk

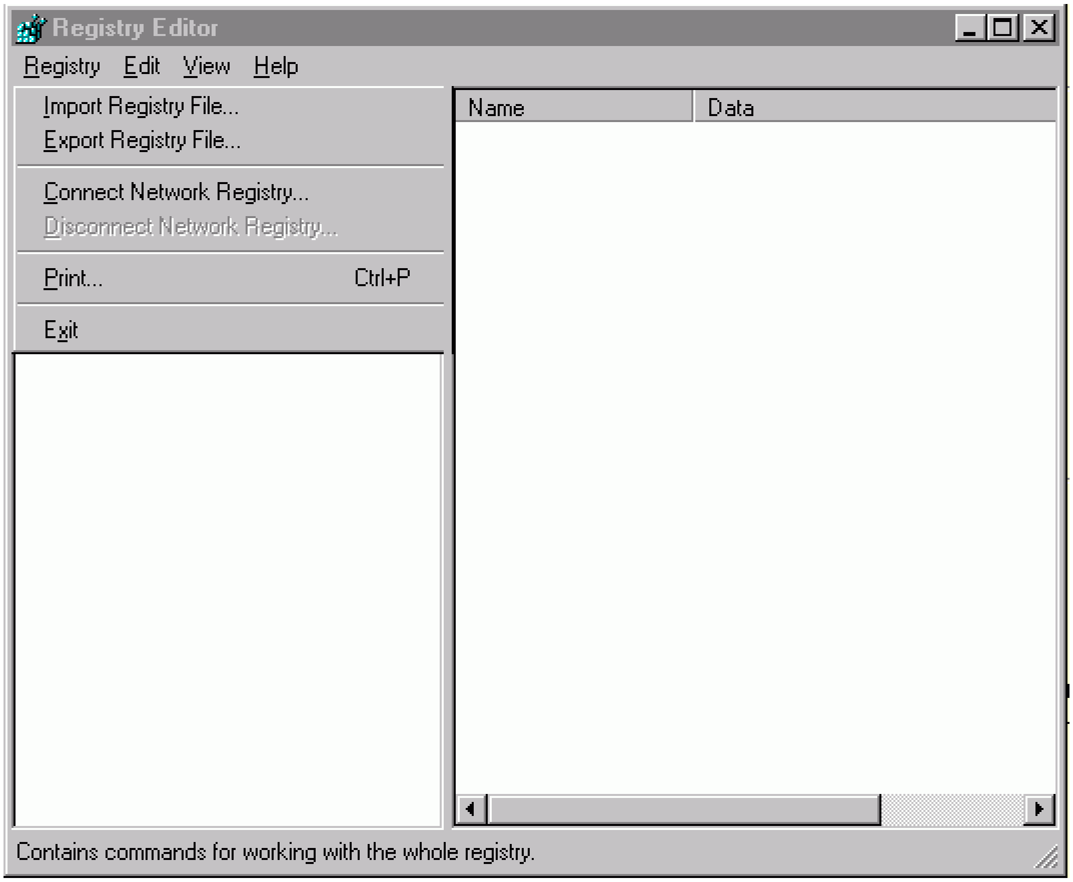
In a DOS box, use the command

```
rdisk /s
```

The /s is very important. Keep the disk in a safe place. Redo this disk every time you make a major change to your system (e.g., after a software install that changes the registry).

Backup your registry

The registry is large. Mine is almost 40 Mb. Therefore it will not fit on a floppy. Good places to put it are on a Zip drive, another disk on your computer, or on another computer you own. However, the registry contains all the "keys to the kingdom," so you must protect it from others. **Do not put it in a public server area!**

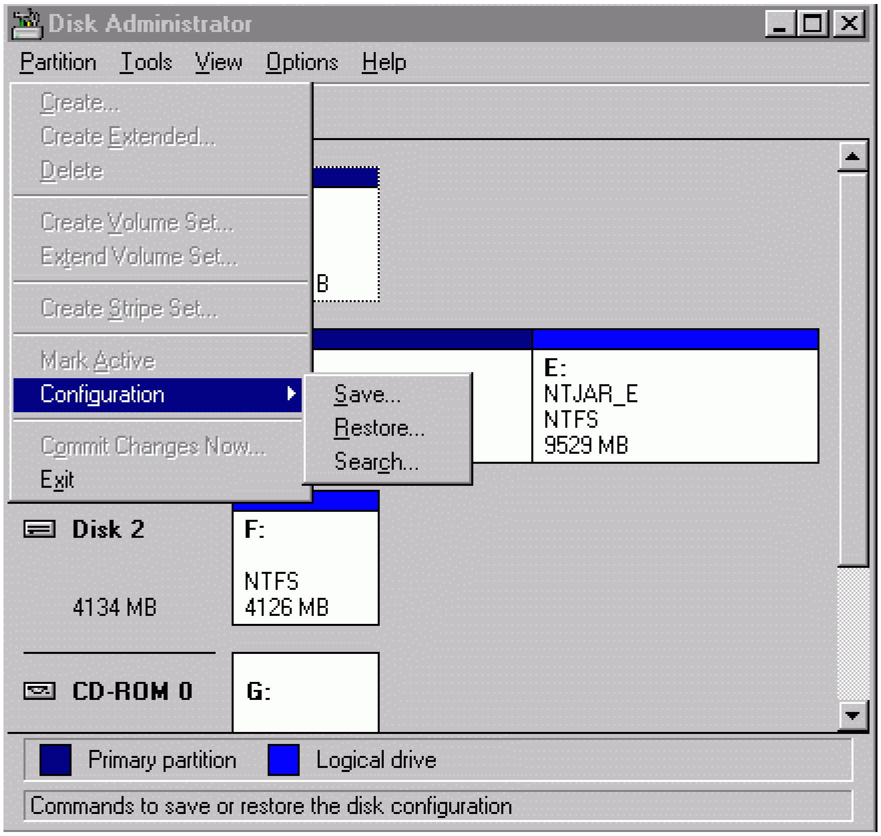


Contains commands for working with the whole registry.

The registry can be backed up using regedit (not regedt32) from the registry menu as shown above.

Backup your hard disk partition information

Unfortunately, disasters occur. The emergency repair disk does not store all the partition information. You can do this yourself. You can back up the partition information from the NT disk administrator (under the Administration Tools menu). This file is small, so you can save it on a floppy disk.



Commands to save or restore the disk configuration

Use NTFS

Unless you use the NT file system (NTFS) on your NT machine, you have **NO security** or file protection. It is easy to convert from FAT to NTFS (but not the other way).

NT provides the convert utility to perform this operation. In the run window, or a DOS box, use the command:

```
convert drive: /FS:NTFS /v
```

You cannot convert the boot partition while NT is running, so convert gives you the option of doing the conversion at the next reboot.

Backup...

Well, everyone always says this, and if you have a built-in tape drive, it is a good idea. But most of us do not have one.

Here are my thoughts on the matter:

- NT needs to be reinstalled every year or so to get it back in working order.
- Hard disks are cheap. I got a fast 20 GB disk for less than $200. A copy to a second physical disk is probably more reliable than a tape

backup.

- I try to keep only the system software in c: and put all applications elsewhere (on d:, e:,...). Then I can reinstall NT with a reformat of the partition. Unfortunately, the application DLLs are put in the \WINNT\System32 directory, so save this directory tree..
- If you do use a tape backup, make small save sets. I just got Seagate's Backup Exec, and the first thing it did was to ask me to make an emergency recovery backup set. I said "sure," and it backed up all 30 GB on 3 disks to one save set. There are two problems with this:
    - If there is any error reading the first tape (I needed 2 8-GB tapes) the second tape is unusable!
    - My disk crashed. The program ran out of memory (I have 390 Mb)!) reading the catalog of the files, halfway through the second tape. Luckily I recovered my disk without using the useless backup tape.
    - Thus, save every volume (or parts thereof) in separate save sets.
    - Oh, by the way it takes about 10% of your disk space to store the restore catalog if you have a lot of files.
- There is no reason to backup any commercial programs—you should have the original disks.
    - Most major programs need to be reinstalled every year or so
    - You do need to get the service packs for things like office. They are available on the PUBLICC node.
- You MUST backup anything you wrote or data that you need.
    - When I write important code, I zip up the whole workspace directory and put it in several places on several computers. If the information is sensitive, you can use a password for WinZip or PKZip to encrypt it, but this is not bulletproof, so beware where you put it.
    - The above code backups have saved me more than once from "oops I screwed up" mistakes..

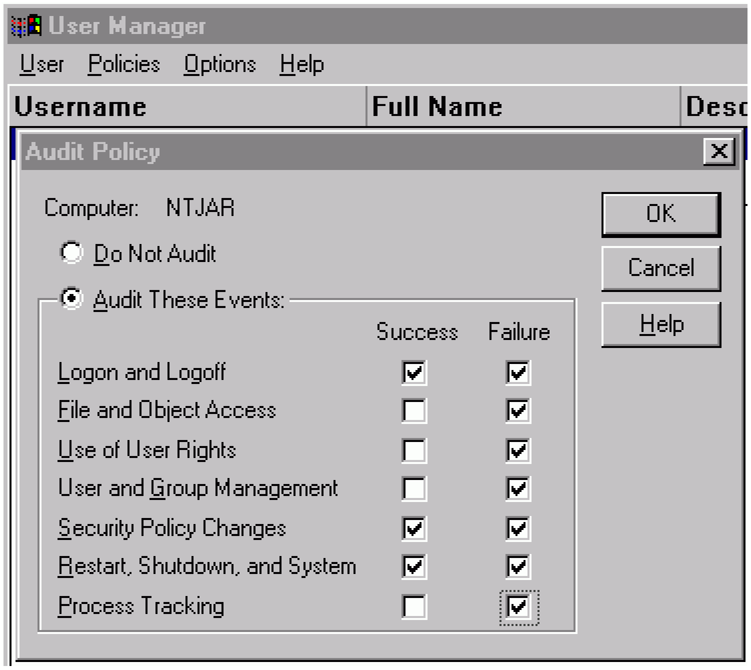
Keep your virus protection installed and up to date

At a computer security conference, a colleague (at another lab) asked to use my laptop for his presentation because his was acting up. He put his floppy into my PC to run the PowerPoint talk, and there in front of the whole audience, the McAffee screen popped up and said the disk was infected. No wonder his PC was acting up!

We had another incident in a Division where I was DCSO, where someone sent an infected Word document to DOE. Not a good way to make a favorable impression.

Turn on auditing

It is essential that you turn on auditing so that you can tell whether your NT system is being attacked. Under *Administrative Tools*, *User Manager*, select *Policies*, and then *Audit*:



Computer: NTJAR

○ Do Not Audit

● Audit These Events:

	Success	Failure
Logon and Logoff	☑	☑
File and Object Access	□	☑
Use of User Rights	□	☑
User and Group Management	□	☑
Security Policy Changes	☑	☑
Restart, Shutdown, and System	☑	☑
Process Tracking	□	☑

I audit failure for everything as shown above. You also want to see who is logging on and off of your system. Of course logs do no good unless you look at them. Use the Event Viewer to do so.

A really good article on how to analyze the event logs is at http://www.win2000mag.com/Articles/Index.cfm?ArticleID=9043 .

Check access permissions

By default, FTP and Web services are turned on if they are installed, and the only access is *anonymous*, so that anyone can use them. Go into the control Panel and under the services menu, select the *Peer Web Services* and *Startup* and select *Manual*. I use my *FTP* server, but change the access to require a uid/pwd. However, I have a separate account for just using the FTP with a password that is NOT my CTD one.

I also have set up my Web server to use SSL and to require a certificate for access. This is about as secure as you can get. See me if you need this level of protection. Get rid of the sample scripts in the InetPub directory, they can be compromised.

By default, all files are fully accessible to "everyone." This means everyone who can log in. But I right click on the disks in Explorer and change this to only give access to Administrators and me. Then if I need to give access to any colleagues, I explicitly add them to the permission list. Always deny everything by default to play it safe.

There are lots of issues with accessing the registry, and many permissions are set incorrectly there. The best thing is to install the latest Service Pack.

C2 Security

The truly paranoid among us can make their NT machine even more secure by changing its configuration to the NSA-approved C2 one by following the instructions in http://infosec.nosc.mil/TEXT/COMPUSEC/ntsecure.html. This turns on things like auditing for most actions and properly configures registry permissions and ownerships of files.

Install the latest Service Pack

Currently, the latest version is SP6a.

If you have a big hard disk (>4 GB), it is very important that you have access to the latest service pack from somewhere else. The version of NT on the install disk does not recognize large drives. I had to reinstall NT and would have been up the creek if I had not put SP6a on my c: drive. Once I installed SP6a, I had access to my large disk again.

When you install a service pack the **first time**, be sure to let it make a backup so you can uninstall it. You must reinstall the service pack every time that you install something from the original NT disk (such as a networking feature or a sound card). Do not make a backup when you reinstall a service pack because it will not allow you to regress anymore.

There are always pluses and minuses and lots of breath-holding when you install a new service pack. However, there are so many hot fixes on old service packs (each one requiring a reboot) that it is not practical to stay behind the curve. Wait a decent period (a few weeks from the service pack release) and install it.

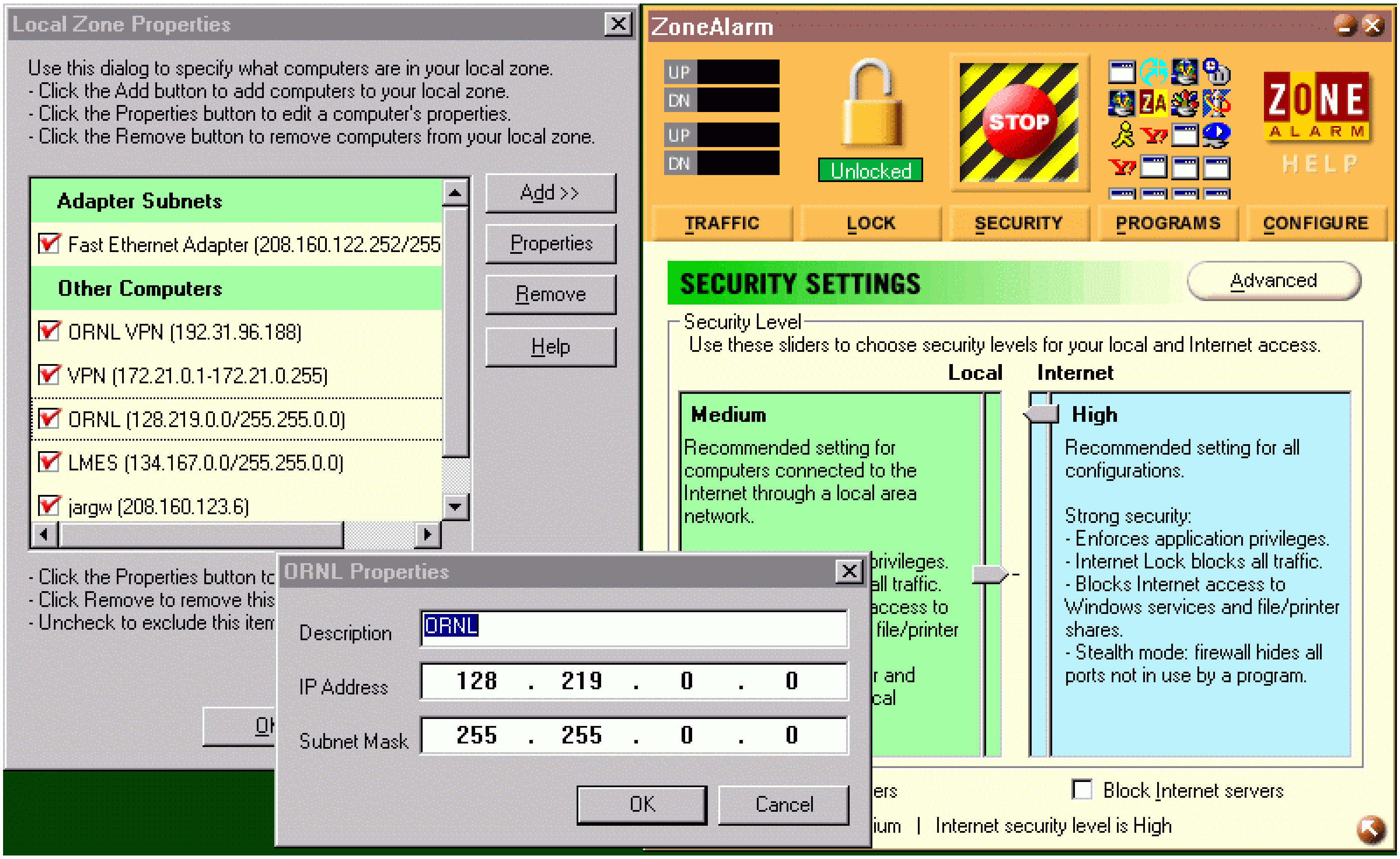
Once a service pack is installed and working, you can delete the old service pack backups (they are big).

Get a personal firewall

I highly recommend ZoneAlarm. You can obtain the latest version from http://www.zonelabs.com/. For personal use it is free!

I feel it is especially important to protect your home computers, especially if you are always on the Net via a Cable Modem or ISDN. ZoneAlarm is easy to use and very effective. Since installing it, I get about a half-dozen intercepted probes every day! All of my applications work.

To use ZoneAlarm properly, you need to identify what computers or subnets are in your "local" zone where restrictions may be less than for the Internet. This identification is done in the security menu.



Use this dialog to specify what computers are in your local zone.
- Click the Add button to add computers to your local zone.
- Click the Properties button to edit a computer's properties.
- Click the Remove button to remove computers from your local zone.

Adapter Subnets

☑ Fast Ethernet Adapter (208.160.122.252/255

Other Computers

☑ ORNL VPN (192.31.96.188)
☑ VPN (172.21.0.1-172.21.0.255)
☑ ORNL (128.219.0.0/255.255.0.0)
☑ LMES (134.167.0.0/255.255.0.0)
☑ jargw (208.160.123.6)

- Click the Properties button tc
- Click Remove to remove this
- Uncheck to exclude this item

Description: ORNL
IP Address: 128 . 219 . 0 . 0
Subnet Mask: 255 . 255 . 0 . 0

SECURITY SETTINGS

Security Level
Use these sliders to choose security levels for your local and Internet access.

Local: **Medium**
Recommended setting for computers connected to the Internet through a local area network.
privileges.
ll traffic.
access to
file/printer
r and
cal

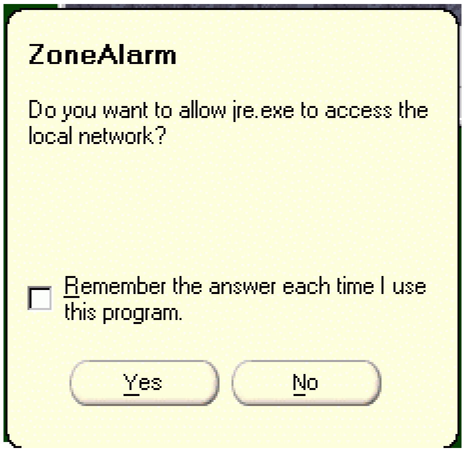
Internet: **High**
Recommended setting for all configurations.
Strong security:
- Enforces application privileges.
- Internet Lock blocks all traffic.
- Blocks Internet access to Windows services and file/printer shares.
- Stealth mode: firewall hides all ports not in use by a program.

ers ☐ Block Internet servers

ium | Internet security level is High

Here I have identified the ORNL subnet as a member of my local zone by using the Add>> menu. Note that I set the security for the local zone to Medium and for the Internet to High.

The other configuration process occurs whenever a program tries to contact the net. A box will pop up asking for permission to connect to the local zone and then the Internet zone. You can check the box to make this a permanent decision.



ZoneAlarm

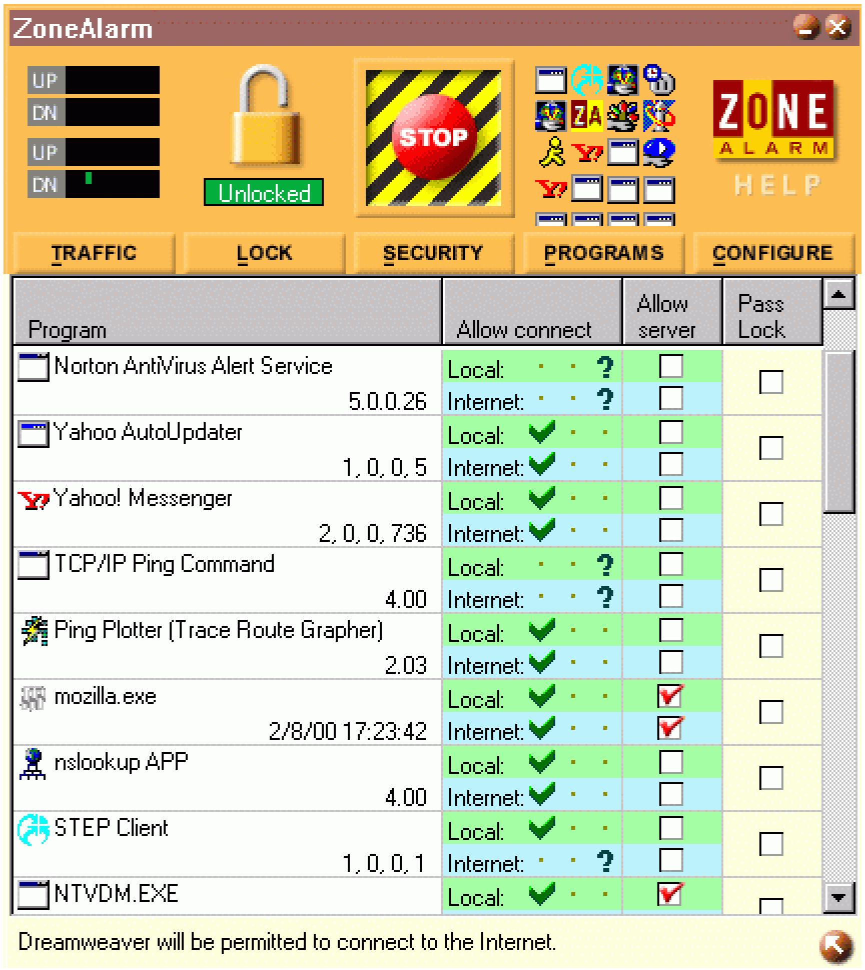
Do you want to allow jre.exe to access the local network?

☐ Remember the answer each time I use this program.

Programs like PALS that only access the Lab should only be allowed Local Zone access. Your Netscape needs Local and Internet access.

Some programs also must act as a server, and when this is needed, ZoneAlarm will pop up another box to get your permission.

The program permissions are visible on the Programs menu of ZoneAlarm.

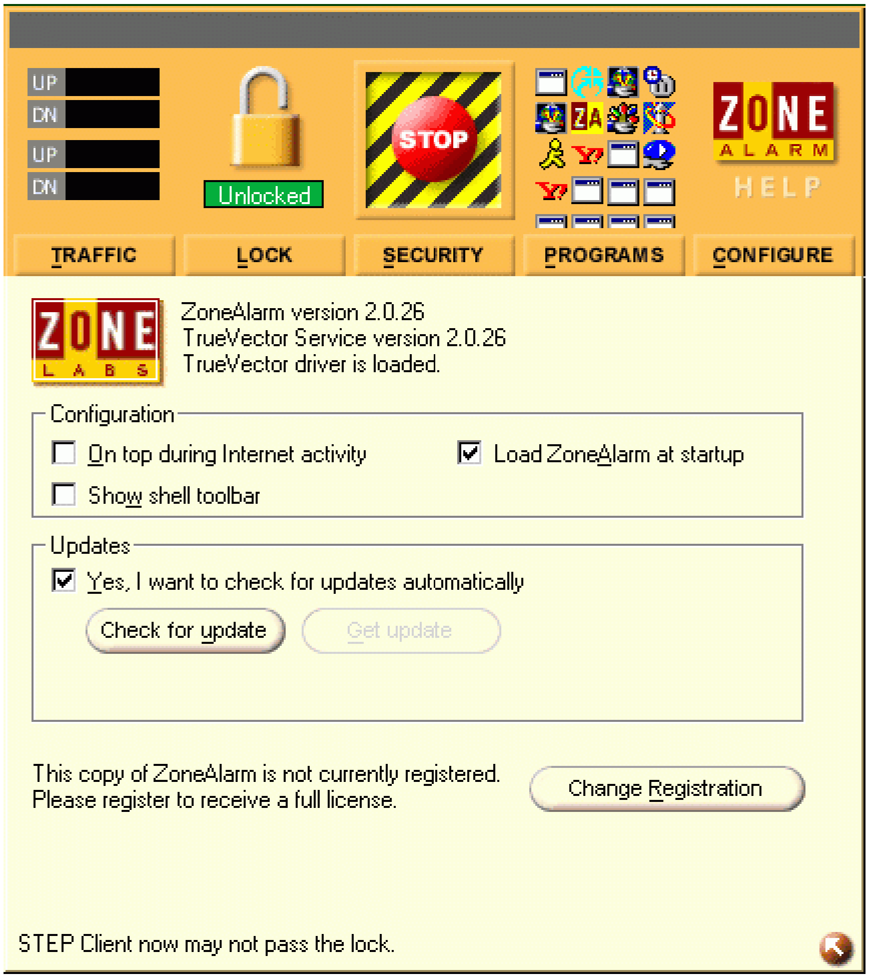


Program	Allow connect	Allow server	Pass Lock
Norton AntiVirus Alert Service	Local: ?	□	□
5.0.0.26	Internet: ?	□	
Yahoo AutoUpdater	Local: ✓	□	□
1, 0, 0, 5	Internet: ✓	□	
Yahoo! Messenger	Local: ✓	□	□
2, 0, 0, 736	Internet: ✓	□	
TCP/IP Ping Command	Local: ?	□	□
4.00	Internet: ?	□	
Ping Plotter (Trace Route Grapher)	Local: ✓	□	□
2.03	Internet: ✓	□	
mozilla.exe	Local: ✓	☑	□
2/8/00 17:23:42	Internet: ✓	☑	
nslookup APP	Local: ✓	□	□
4.00	Internet: ✓	□	
STEP Client	Local: ✓	□	□
1, 0, 0, 1	Internet: ?	□	
NTVDM.EXE	Local: ✓	☑	□

Dreamweaver will be permitted to connect to the Internet.

Note that I have only given the VPN client (STEP) permission to access the local net because I have designated the VPN server as a member of my Local zone.

ZoneAlarm can be configured to pop up when you access the Internet and to load when your system is booted via the configure menu.



ZoneAlarm version 2.0.26
TrueVector Service version 2.0.26
TrueVector driver is loaded.

Configuration

☐ On top during Internet activity ☑ Load ZoneAlarm at startup

☐ Show shell toolbar

Updates

☑ Yes, I want to check for updates automatically

This copy of ZoneAlarm is not currently registered.
Please register to receive a full license.

STEP Client now may not pass the lock.

These NT tips were taken from Lance Jensen, Director of Technical Support, Executive Software.

Keyboard Shortcuts

If you hold down the Shift key when you insert a CD-ROM, the AutoPlay feature will be disabled. This is advantageous when upgrading an application such as Diskeeper which requires that the original CD-ROM be inserted. If the original CD-ROM AutoPlays, you may accidentally reinstall the original instead of the upgrade.

If you hold down the Shift key when logging on, any program that is in the Startup folder will not automatically start. This is useful when you are troubleshooting, or any other time you do not want to wait for any automatic program startups.

If you press Tab while holding down the Alt key, a list of icons for your open applications will appear, with a frame around one. (Keep holding down the Alt key to continue to view this list; releasing the Alt key causes the framed application to become the current window). Pressing the Tab key again, while still holding down Alt, will move the frame to the next icon. Holding down Shift while you press Tab (still depressing the Alt key) moves the frame in the other direction. As noted above, when you release the Alt key, the application represented by the icon currently in the box will become the current (top) window. If the application is minimized, it will be expanded.

With several applications open in windows on your desktop, Alt-Esc brings up the next application, and Alt-Shift-Esc brings up the previous one. (Note that this won't work with minimized windows). If you only have a few applications active, this can be faster than using Alt-Tab.

Print Scrn will put a snapshot of the entire screen into the Clipboard; "Alt-Print Scrn" will save only the active window. After capturing the snapshot, open Paint (or your favorite graphics editing program) and Paste the snapshot into a new file. Use "File/Save as" to save the image. This tool can be invaluable when communicating a problem to Tech Support, as it shows us the exact error message displayed.

In Windows NT Explorer and in Microsoft Outlook, if you select a folder then press "*" on the numeric keypad (Num Lock can be on or off), the entire tree of sub-folders under the selected folder will be expanded. Pressing "-" on the keypad will collapse the tree again. However, if you now click on the "+" by the folder name, the entire tree will appear again. To go back to the default of displaying a folder's immediate sub-folders only, you must either click each "-" individually, or exit Windows NT Explorer or Microsoft Outlook and then re-open it.

You can open the Start menu by pressing Ctrl-Esc; Ctrl-Shift-Esc will open Task Manager.

If you print a lot of documents, try "drag-and-drop" printing. Select Control Panel / Printers, then click and hold the printer you usually use and drag it to the desktop. Now you can drag a file from Windows NT Explorer (or Microsoft Outlook or any similar file list) and drop it on the printer icon. If it's a printable file, it will print.

Your Interface

There are many ways to set up the interface between you and your computer. Each has advantages and disadvantages, so the only advice we can give is try different things and use what suits you. I make shortcuts to all of my commonly used programs and drag them to the desktop, then use the Microsoft Office suite Desktop toolbar. I keep it "Always on Top" and "Auto Fit into Title Bar area". The applications I want to keep open, such as Microsoft Outlook, are accessible from the Taskbar. The rest I access from the Microsoft Office Toolbar and close when I'm finished.

Here are some other interface tricks you can try. Did you know you can set a shortcut to open a program in the size window you prefer? Highlight and right click the shortcut. Click Properties, select the Shortcut tab and pull down the menu in the Run field. Here you will find MINIMIZED, NORMAL WINDOW and MAXIMIZED. The default is NORMAL WINDOW.

Within the same shortcut tab, you will see a field called SHORTCUT KEY. Select that and type in any key you like. This will cause the shortcut to be called when ever you select Ctrl + Alt + the key you selected - instant hot key! Be aware that if you use that same key again in another shortcut, it no longer will point to the previous one; one key per shortcut.

If you don't like having shortcuts on your desktop, you can put any shortcut you like into your Start menu:

a. Create a shortcut to any program you will use by selecting the .exe file in Windows NT Explorer, right clicking and selecting CREATE SHORTCUT.

b. Highlight the shortcut, right click and select CUT.

c. Right click the START button and select OPEN.

d. Right click anywhere in the window and select PASTE.

Viola, you have loaded your shortcut into the start menu!

You may want to set the TASK BAR PROPERTIES to SHOW SMALL ICONS ON START MENU if you have a lot of shortcuts in there:

a. Right click on an unused area of the task bar (usually at the bottom of the screen).

b. Select PROPERTIES.

c. Enable the SHOW SMALL ICONS ON START MENU option.

This article was mainly about ways to save time when doing routine work on your computer. An area often overlooked, however, these tips can save you a significant amount of time during the course of a day.