Novell Client Firewall

www.novell.com

September 03, 2003

NOVELL CLIENT FIREWALL
INSTALLATION GUIDE

Novell®

Legal Notices

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.

www.novell.com

Novell Client Firewall Installation Guide
September 03, 2003

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

Novell Trademarks

Novell is a registered trademark of Novell, Inc. in the United States and other countries.

Third-Party Trademarks

All third-party trademarks are the property of their respective owners.

About the Guide

This guide provides you the information that you need to configure and use Novell® Client Firewall (NCF).

The guide is divided into the following sections:

Documentation Updates

For the most recent version of the Novell Client Firewall Installation Guide, see the Novell online documentation

Documentation Conventions

In Novell documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

In this documentation, a trademark symbol (®, TM, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as UNIX*, should use forward slashes as required by your software.

1 Understanding

This chapter provides a brief overview of the Internet and firewall concepts that you need to understand before using Novell® Client Firewall (NCF).

The following are discussed here:

Internet Basics

The Internet is interactive, which simply means that when a computer is connected to the Internet, data can be sent and received by that computer to other computers on the Internet. This inter-activity is built into the Internet and is a fundamental part of it.

To see a web site on the Internet, your computer basically asks that site for its files. The site's computer (server) then sends (serves) those files to your computer. For the files to get from the server all the way through the Internet over to your computer, your computer must give the site's server your computer's address. This address is unique and called IP address. No other computer on the Internet has this same address.

The Internet uses what's called a server-client way of doing things. Web sites use servers to supply their web pages and people use their computers as clients that are served those pages. The vast majority of information on the Internet goes from the servers to the clients, from the web sites to the desktop computer. Very little information goes from your computer back to the server.

Why NCF is Needed

The major reason Outpost is needed is because a small percentage of Internet users are destructive. These people are called hackers or crackers. Traditionally a hacker is an accomplished computer programmer who is an expert in networks. A cracker is the term for someone who gains unauthorized access to a computer or system. The news media has blurred these definitions and refers to anyone who breaks into other people's computers as a hacker.

It used to take some skill to crack into a system but nowadays there are programs that can do it automatically. Children without much training or expertise can use them. These programs can be gotten effortlessly from the Internet. Many of these programs are sent around the Internet haphazardly as attachments to e-mails. Once the program is running on a user's machine, it "calls home" to a central site and reports where it is. The hacker can then control that user's machine remotely without the user even being aware of it. The hacker can record all the keyboard actions

and mouse movements of the user's computer so can capture credit card data and passwords with ease. Sounds like science fiction but it is very much a cold, hard fact.

Another undesirable element of the Internet is the ever-present threat of computer viruses that are disseminated through email. These are so numerous that if something goes wrong with a computer the first thing suspected (and often discovered) is a virus.

Advertiser tracking of your surfing habits and interests has recently become a concern of privacy advocates. Advertisers use the data they gather on you to push specific ads calculated to increase your purchasing.

The Main Threat

- Someone on the Internet thousands of miles away can access your computer and personal files more easily than your neighbor down the street.
- Once your computer is accessed, all of its files can be viewed, copied and erased.
- Your computer can be used to attack other innocent user's computers without your knowledge.
- A hacker can very easily make your Internet connection totally unusable just for kicks.
- Your passwords, credit card info, house address can all be obtained remotely very easily.
- Unscrupulous advertisers can track your surfing habits, your interests and your locale, thereafter target specific ads at you.
- Personal info about you can be collected for various reasons, all without your knowledge or consent.

How NCF Works

Outpost is a firewall, the technical name for a barrier between your computer and the rest of the Internet. It's like the locks on the doors of your home. Most of your neighbors can probably be trusted not to walk into your home and vandalize it or steal from you. Usually only a small number of your neighbours are untrustworthy. But, if you live in heavily populated area, there are a greater number of dishonest people around.

The Internet is similar except that your immediate neighborhood consists of hundreds of millions of people. Even the small percentage of those people who have a destructive bent is a large number of people.

Outpost Firewall not only locks your computer's "doors", it makes your computer invisible on the Internet. Your computer normally your computer normally lets other Internet users know its address. It's like the address sign of your home or the license plate of your car. Your computer's address is plainly visible. Outpost prevents your computer from broadcasting its address unless specifically authorized by you. Hackers are not just kept out; they cannot find out that your computer is connected to the Internet.

NCF Features

- Starts protecting immediately after being installed.
- Has default configuration settings for new users.
- During the installation auto-configures for optimum protection.

- Can be customized in detail by advanced users.
- Makes your computer invisible on the Internet.
- Locks your computer's "doors" ports against intrusion.
- Let's you decide how much an application should be trusted.
- Uses plug-ins to increase its power while keeping the same familiar interface.
- Stops Internet ads from distracting you or slowing your browsing.
- Prevents ad tracking of your surfing habits and interests.
- Prevents your computer from being controlled remotely.
- Notifies you of any hidden software attempting to "phone home" to a hacker.
- Runs on all recent versions of Windows so can still be used if you upgrade.
- Uses very little system resources so does not noticeably affect your computer's performance.
- Advanced Log System lets you view any event on your system.
- Successful on all known "leak-tests".§Multi-language: Outpost Firewall supports up to 14 languages.

2 Getting Started

This chapter discusses the basic information that you need to know about Novell® Client Firewall (NCF).

The following are discussed here:

System Requirements

The minimum system requirements needed for NCF to operate are given below:

Processor	166 MHz Intel* Pentium* or compatible CPU
RAM	16 MB
Operating System	·Windows 98, Windows NT 4.0, Windows 2000 or Windows XP
Hard disk space	4 MB

NOTE: There is no special network card or modem needed and there are no special configuration settings of these boards needed for the normal operation of the software.

NCF Capabilities

NCF provides an easy-to-use interface. To effectively use NCF, you do not need to know the inner workings of Windows. The default settings are configured for you. However, you can change any of these many settings at any time. (cross refer) These are covered later in this manual.

A tremendous strength of NCF is its modular organization. NCF's capabilities are implemented as special modules called plug-ins, files with the .ofp extension. Each module is independent and can easily be added to an installed system.

The major benefits of NCF are:

- Protects you against the full spectrum of security threats from privacy issues to data leaks and exploits.
- Can be used immediately after installation without any customization.
- Can be auto-configured for best protection or will let you easily create your custom secure configuration very quickly using system prompts and default settings without interrupting your work.

- Performs very complicated adjustments to the security of your system with just a few keystrokes.
- Supports up to 14 languages.
- Can be used to restrict network access both to your computer and from your applications. Advanced users can also adjust service protocols and create special security facilities as required.
- Stealth mode makes your computer invisible to hackers while letting you browse the Internet as usual.
- The modular structure of the system lets you add new protective modules in the form of plug-ins.
- The system is compatible with all versions of Windows 98/2000/ME/NT and XP.
- Has minimal system requirements.
- Restrict a list of applications having access to the network and specify acceptable protocols, ports and directions of access (incoming or outgoing) for each of these applications.
- Block or restrict non-requested information being sent to your computer, in particular:
  - Banner advertisements
  - Pop-up windows on web pages
  - Inappropriate content data from specific web pages.
- Restrict or prohibit the action of program components built into web pages, such as Java applets, ActiveX scripts and JavaScript.
- Restrict or prohibit the use of cookies.
- Specify a zone of "friendly" IP addresses, your own LAN for example. In this zone, Outpost Firewall does not control or restrict network exchange.
- Can quarantine e-mail attachments to protect your system from Internet worms.
- Warn of any indication of someone attempting an attack of your computer from any other computer and instantly prevents access.
- Its Advanced Database driven Log System supports custom queries for data mining tasks.
- Successful with all known "leak-tests".

3 Installing Novell Client Firewall

This chapter provides you information on how to install Novell® Client Firewall (NCF).

The following are discussed here:

Installing NCF

NCF's installation procedure is similar to that of most Windows programs.

NOTE: Be sure to uninstall any other firewall software and reboot before installing NCF to prevent a system conflict of different firewalls fighting to control network access.

Shutdown any other firewall software before installing NCF on your computer. Trying to install a firewall over other running firewall software will crash your computer. Like a car with two drivers, each firewall tries to steer and the computer runs into a pole!

Once you are certain no other firewall is operating on your computer, install NCF by running NCFInstall.exe. It is recommended that you use the default settings when the installation utility asks you to confirm its choices if you are not an advanced user.

To start the NCF installation program:

1. Before installing NCF, uninstall any other firewall software on your computer and reboot.
2. Close all open applications.
3. Click the Start button on the Windows Task Bar.
4. Select Run… on the Start menu.
5. In the Open field of the Run dialog window, enter the full path to the setup program file (NCFInstall.exe). For example, if the setup program is on disk D: in the folder and subfolder \downloads\ncf\ type into this field:

   D:\downloads\ncf\NCFInstall.exe
6. Click the ?? button.

   The setup procedure is arranged in several steps. The installation begins with a Welcome screen that reminds you to exit all Windows programs and guides you through the entire process. The installation screens have the following buttons.

   - **Next**—takes you to the next step of the procedure

- **Back**—returns you to the previous step
- **Cancel**—aborts the entire setup procedure

7 After clicking Next, you will be asked you to accept the License Agreement to use the NCF.

8 Please read this carefully. In this screen, Next is enabled only if you select the option button "Yes" indicating that the License Agreement is acceptable to you

9 After you have accepted the License Agreement, the Next button brings you to the following Read Me File window:

10 After pressing the Next the Choose Destination Location is shown:

11 Specify the folder in which the NCF components are to be installed. Keep the default folder shown as the Destination Folder if you have no other particular preferences in mind.

If you want to change the default location, click the Browse... button and Windows' familiar Folder Selection dialog is displayed. Select the preferred folder or type the name of a new folder to be created and click the button.

12 The Next button takes you to the Select Language dialog:

13 Choose the language for NCF interface and press Next button.

Then comes the Start Installation dialog window:

This is the last step before the actual installation of the software takes place. If you decide to change any of the choices you made, you can click on the Back button. When you are ready to go ahead with the installation, click the Next button.

The program displays the Installation progress window:

After the installation is finished you are prompted to auto-configure the rules for applications and network settings:

If you want to skip the auto-configuration step press the Skip button, otherwise if you want to use this procedure then press Next. We strongly recommend that you let NCF auto-configure the rules and network settings for your system.

After pressing the Next button in the previous dialog window NCF scans your hard disk for any installed applications that might use the Internet. NCF offers specific rules for each application it detects. The rules are created for optimum performance and security of these applications. After the search is completed the following dialog window asks you to apply the auto-configured rules for the applications:

It is strongly recommended that you apply the auto-configured rules until you are an advanced user and would like to create some rules manually. To do this make sure "Apply the auto-configured rules" is checkmarked as in the screenshot above. You can change these settings at any time while using NCF. For more info please refer to 7.4 Creating Rules for Applications

If you want to see the list of applications the rules were auto-configured for, press the Details button, which displays this window:

To remove auto-configured rules for an application just uncheck the box next to the application component name

To close this window press the OK button. You will see the previous Application window, press Next to continue the installation.

NCF then auto-detects your network settings and displays the Network settings window that looks very like the previous applications window:

It is strongly recommended to accept the auto-configured rules for your Network. To do this, make sure that "Apply the auto-configured rules" is checkmarked as in the screenshot above. You can also see the details of network settings by pressing the Details button. You will can change these settings at any time while using NCF. For more info please refer to 7.6 Settings For a Home or Office Network.

To continue the installation press Next.

After the auto-configuration is complete, you will see the Installation Complete dialog window:

After clicking the Finish button, the installation procedure is complete and the dialog window prompting you to restart the computer appears:

IMPORTANT: Do not launch NCF manually using the Start button or Windows Explorer right after installing it. You must reboot your computer before NCF can start to protect your system.

Uninstalling NCF

Before installing a newer version of NCF, you MUST uninstall an earlier version and reboot.

To uninstall NCF:

1. Right-click on NCF's system tray icon and select Exit and Shutdown Novell Client Firewall.
2. On the Windows task bar, click Start > Programs
3. Select Novell Client Firewall
4. Select Uninstall Novell Client Firewall.
5. This displays the dialog window shown here:
6. To assist Novell by mentioning the reason you decided to uninstall NCF, please select Yes, I want to send a feedback, otherwise select No, I do not want to send a feedback.
7. If you chose to send a feedback your default browser opens the "Assist Agnitum" web page with three questions describing the possible reasons you are uninstalling the software:
8. Checkmark the appropriate answers, add any comments, your e-mail address (optional) and press the Send button. Close the browser window and continue uninstalling NCF.

   You will see this window:
9. If you want to leave the NCF configuration files on your hard disk for a future reinstall of NCF then press the Next button.
10. If you prefer to completely remove NCF and all its components including the configuration files then check-mark "I want to remove Novell Client Firewall and its configuration files" and press Next.

    The following window appears:
11. If you are new to Windows, it is recommended that you select Automatic then press the Next button. This skips the steps that ask you for decisions. If you are familiar with Windows and you want to choose the items to uninstall, select Custom before pressing the Next button. The Repair option is used to reinstall the NCFso it is complete and fully operational.

    The next dialog window is shown here:
12. Clicking the Finish button of this window starts the uninstall process and displays the following dialog that shows the progress of the uninstall:

13 The program will prompt you to restart your system in order to complete the installation:

14 Press OK to restart or Cancel if you want to restart your computer later.

NOTE: To avoid software conflicts, restart your system after the uninstall process completes.

Starting NCF

Once installed, the NCF starts automatically when Windows is loaded. In this way, NCF starts protecting your computer immediately before other programs can compromise your system.

When NCF starts, its icon is placed in the system tray, on the right-hand end of the Windows Task Bar.

If, for some reason, NCF does not start when Windows loads, you can start it by following these steps:

1 In the Windows task bar, click Start > Programs.

2 Select Novell Client Firewall > Novell Client Firewall.

When NCF is running its icon is displayed in the system tray. If you do not see the NCF icon in the system tray, then you know that NCF is not protecting your computer unless you specifically set it up to run in background mode. For more info please refer to 5.2 Initial Settings.

Stopping NCF

Closing NCF's main window does not shut down the firewall. Its icon remains in the system tray.

There are two ways to shut down NCF:

Right-click on its system icon in the system tray to display the context menu. Select Exit and Shutdown Novell Client Firewall.

You can also shut down NCF when its main window is displayed by going to the File menu and select Exit and Shutdown.

Both ways close the interface and stop the firewall so NCF is no longer protecting your system.

When NCF is shut down its icon disappears from the system tray indicating that the firewall is no longer protecting your computer.

Automatic Update

With Automatic Update, you never have to be concerned about the latest Internet threats. NCF provides you with a convenient way of keeping itself updated via the Internet. Each day, Automatic update checks for newer components and plug-ins and if it finds any, it retrieves them for you.

If, for some reason, you would like to check for newer components manually, you could run the Update procedure by clicking on the Update button on NCF's toolbar as shown here:

Alternatively, you could manually check for any updated components by:

1 On the Windows* task bar, click Start > Programs.

2 Select Novell Client Firewall > Update.

Either of these two methods produces the following dialog:

3 Select either:

- Automatic to have the system find all the components to be updated. Automatic is recommended so that all the components that have an update available will be updated together.
- Custom for you to specify each component you want to be updated. Only advanced users should use this choice for debug purposes.

Of course, with either Automatic or Custom, components are updated only if updates are available for them.

4 Clicking the Settings button displays this dialog:

The options are:

- Auto Detect uses the proxy settings already specified in Microsoft Internet Explorer.
- Use proxy server lets you specify the parameters of the proxy server that is to be used by NCF's Automatic Update. The Server and Port fields become visible when you choose this option. Enter the name of your proxy server and its port number (port 8080 is the default). If your proxy server requires authorization, please check the appropriate checkbox and enter your username and password. If you are unsure what type of proxy you use or you do not know your username and password, please consult your system administrator.
- Do not use proxy server if your system is not connected to the Internet through a proxy server.

5 If you selected Custom update, you will see this dialog:

Any line in the components list that starts with a plus sign is a grouping of components. You can see the listing of these components by clicking on the plus sign. In the picture above, clicking on the first plus sign produces the following display:

6 As you can see, the plus sign was changed to minus sign when it was clicked to show the full listing.

A red checkmark is a component that our engineers have determined must be updated for NCF to avoid compatibility problems between modules and other selected components.

Check the components you want to update. Deselect the components you do not want to update. It is recommended to update all components unless you are an advanced user and have some reason not to.

When this dialog window first appears, all the components are checked by default.

After all the components to be updated are selected, click the Next button.

Here is the next dialog showing the downloading progress:

7 When the download is complete, this dialog is automatically replaced without your having to click the Next button.

This is the last dialog that is displayed during the Update process:

This dialog gives you the following choices:

- Yes, I want to restart my computer now to restart your computer immediately.
- No, I will restart my computer later gives you the opportunity of saving any incomplete work before restarting your computer. Be sure to restart your computer as soon as possible to take advantage of the increased protection afforded by the updated components you just downloaded.

NOTE: Please note: The NCF version is changed only after a reboot of your computer. If you simply restart NCF, it will be the same version. To see what version is active, select from the menus Help -> About.

If there are no updates available, this dialog window is shown:

4 Initial Options

The following are discussed here:

Language

If you prefer a language other than English, the first thing to do is:

1. Double click the icon on the taskbar. NCF's main window is displayed and looks like this:
2. Click on the View menu at the top of this window.
3. Select Language from this menu.
4. Choose your language from the list that's displayed.

You will see this message informing you that you'll need to reboot your computer before the new language takes effect:

Operational Modes

NCF gives a wide choice of protection levels all the way from totally blocking all Internet access of every application on your computer to allowing full access to every application. For your convenience, NCF has different operational modes to conform to the protection level you prefer.

The operational modes are:

- Block all-All network connections are disabled.
- Block most-All network connections are disabled except those apps you enable.
- Rules Wizard-You enable or disable apps when they are first run.
- Allow most-All network connections are enabled except those apps you disable.
- Disable mode-All network connections are enabled.

The default mode is Rules Wizard. The NCF icon in the system tray shows NCF's mode.

To change the operational mode:

1. Right click on the system tray icon
2. The following menu appears. Go to the Policy and select the operational mode by clicking on it.

Rules Wizard

Rules Wizard is the operational mode that lets you decide each application's permissions to use the Internet. NCF asks you whenever an application (app) first tries to send or receive data. Rules Wizard is the default operational mode and is recommended for most users.

You can choose to make a rule for an app. If a rule is made then Rules Wizard is not displayed again for that app. If no rule is made for an app then Rules Wizard will display again the next time that app tries to send or receive data.

Don't be concerned about setting rules for apps. You can easily change or delete an application's rules at any time.

This is the Rules Wizard dialog:

It shows you the application (Internet Explorer, in this example), whether the app wants to send or receive data, the type of service the app is attempting to establish and the address the data is about to go to or be received from.

You are then given the following choices:

- Allow all activities for this application-For applications you trust completely. The application is then included in the Trusted applications list. (See Options menu, Applications tab.)
- Block all activities for this application- For applications which you know should not have network access. The application is included in the Blocked applications list. (See Options menu, Applications tab.)
- Create rule using preset-NCF lets you create rules using presets for most common applications or the presets that best suit an application (Internet Explorer, in our example above). NCF is designed to offer the preset that best suits your application. The application will be included in the Partially allowed applications list. (See Options menu, Applications tab.) It is recommended that you select the preset offered by NCF, however advanced users can click on the drop-down menu and select other presets or even create their own rule sets by selecting "Other".
- Allow Once- For applications of which you are doubtful. The next time this application tries to establish a network connection, the same warning is displayed. No rule is created for the application.
- Block Once- For applications of which you are uncertain and distrust. The next time this application tries to establish a network connection, the same warning is displayed. No rule is created for the application.

Automatic Updates

NCF can update itself automatically from Novell's web site. This ensures that you get maximum protection from the latest threats discovered to be going around. Once a day, NCF checks the site for an updated version of itself and if there is one it is downloaded and installed on your computer. You are notified each time this happens and can cancel the update if you prefer.

If for some reason you need to turn off automatic updating, click on NCF's Tool menu then on Automatically check for Update to remove the checkmark.

You can manually check for an update at any time by clicking on Run Update in the right-side panel or on the button on the toolbar.

Whether checking manually or automatically, if there is an update, NCF displays this dialog:

Automatic-All new modules are downloaded and installed. This is recommended for maximum protection.

Custom-You can specify the modules you want updated.

If you select Custom before clicking the Next button you will see this dialog:

Check-marked items will be updated and unchecked items will not be. Clicking on the box toggles the check-mark on and off. This applies only to the black check boxes. A red check box shows the modules that are needed to complete the update and will be downloaded with a checked item.

If updates are available the next screen is:

If no updates are found or none are requested this is displayed:

5 Advanced Settings

The following are discussed here:

Safeguarding Your Files

Trojan horses are the most dangerous threats to your computer files and your confidential information such as your passwords, credit card data and personal correspondence. A Trojan is a program installed on your computer that gives full access to hackers. The same Trojan can be used secretly by many hackers. It's not just one Trojan to one hacker. It's one Trojan to many hackers.

A Trojan on your computer can let a hacker view, copy or erase any folder and any file on your computer just as though he or she were sitting at your computer using its keyboard and mouse. Any file on your computer can also be sent to any e-mail address or posted on the Internet.

There are many ways a system can be infected with a Trojan and because a Trojan is not the same as a virus (a self-replicating program segment) it is not always detected by anti-virus software. NCF was designed to nullify the malicious actions of Trojans.

NCF's settings for maximum protection from Trojans:

- Rules Wizard mode informs you of any program trying to send data from your computer.
- Stop all mode effectively disconnects your computer from the Internet, which can be set very easily whenever you are not working on the Internet.
- Make your computer invisible to hackers. Click on the Options menu, then on the System tab. Select Stealth in the Answer Type field.
- Ensure NetBIOS is turned off (disabled) unless your computer is on a local network and needs to share its files. If you need to use NetBIOS press the Settings in the LAN Settings field and make sure NetBIOS is checkmarked for your local network like on this picture:

  To add another remote computer or network for which you want to allow NetBIOS communications, press the Add button to get the following dialog:

  To only add a specific remote computer you should know its unique IP address. Enter its IP address in this window. Do the same with IP ranges to add specific networks. Each of the three types of specification shows an example of the format of the input data you should enter.

- In Options, click on the Plug-Ins tab and select Attack Detection. Click on the Settings button then set the options as you see fit in this dialog:

NOTE: Note: You can see the Internet address from which your computer is being attacked in the NCF Log Viewer. To open the NCF Log Viewer for a specific plug-in, click on the plug-in icon in the NCF Left Panel and then press the Show Detailed Log button in the Information Panel. The User Guide covers these logs in detail.

A Web Site's Hidden Programs

A web site can use programs to make its pages more interesting or useful. Examples include animations, calendars, specialized calculators and helpful menus. Most of the time these embedded programs perform a useful or aesthetic function.

However, some hackers found ways to make embedded programs destructive so NCF gives you the option of disabling each questionable component individually.

To do this:

1. Double-click the icon in the system tray to display NCF's main window.
2. Right-click on Active Content to show its menu, which looks like this:

Clicking on Properties shows the same options organized differently:

The image shows three web sites listed under Web Pages (www.asite.com, www.othersite.com and www.yetanother.com). These sites can be configured individually by highlighting each one and configuring its Active Content objects settings.

To add a new address to this list, click the Add button and enter the new address.

After adding the site, you can see it listed with the other sites under Web pages. You can configure the settings for this site by highlighting it on the list and changing its Active Content objects status.

E-mail Threats

Active content can be embedded in e-mails as easily as it can in web pages. Disabling these components for your e-mail is done the same as with web pages. See previous section for how this is done.

Another threat e-mail can bring to your computer are programs disguised as innocent e-mail attachments. This is a very common way of installing malicious Worms and Trojan horses, seemingly helpful programs that can crash your computer and/or open your computer system to direct hacker control. To safeguard against this, you can specify how NCF should handle each type of file attachment. This is done by right-clicking on Attachments Filter and selecting Properties like this:

This gives you the following dialog:

The New button lets you add file types to be inspected by NCF and gives you this dialog:

After adding the file, you need to select the action for NCF to take when this file type arrives into your inbox as an email attachment. It is recommended that you choose Rename It to quarantine the file so you can safely save it to your hard disk and scan with anti-virus software before opening that attachment.

Ad Blocking

Advertising pays the expenses of many web sites so they can give their info or software away for free. However, often ads greatly slow down the connection, are offensive and/or simply irritating.

To have NCF block ads on the web pages you are browsing, right-click on Ads under Plug-Ins in the left panel. Then select Properties to get the following dialog:

Ensure the Enable HTML ad string blocking checkbox is checked.

To add an address to the list of ad servers, enter it in the field above the list and click the Add button. To edit an address, select it on the list, then edit it in the field above the list and click the Modify button. To delete an address, select it and click the Remove button.

The Default button restores the list to what it was when NCF was first installed.

To prohibit ads of specific sizes click the Image Size tab to get this dialog:

This dialog works similarly to the previous.

Note: Blocking ads by image size blocks the display of all images having the specified sizes that are links (i.e. within <a tags), whether they are linked to another site or a page within the web site.

Content Blocking

NCF can block specific web sites as well as any web page that contains a word or phrase you specify.

To have NCF block objectionable content:

Right-click on Content in the left panel of NCF's main window, then select Properties to get this dialog:

This dialog works very similarly to the ad blocking dialogs.

To block specific web sites click on the Blocked Sites tab for this dialog:

This dialog works similarly to the ad blocking dialogs.

Setting a Password

If you have children and don't want them to change the settings you made, you can set a password for NCF.

This is done from the General Options by selecting Enable in the Password protection field as shown here:

Skip the field Enter the old password if you have not already set one. This is used only if you are changing passwords.