BlackICE Help Index

An *Intruder* is a person who breaks into computers to steal, damage or vandalize data.

Overview

In the past, computer hacking presented a very small threat to home or small-business computer users. Hackers spent most of their time attacking large corporate networks where there were valuable things to steal or vandalize. Most home computers of five to ten years ago held few if any files of interest to a hacker. Furthermore, Internet connections in the past were slow and extremely difficult to locate for even advanced hackers.

Today, the typical home or small-business computer presents numerous opportunities for hackers. Many home computers store credit card numbers, account numbers, and confidential information for online commerce, banking, or stock trading. Furthermore, home computers are easy targets. Most home computers have little, if any, protection from hackers. Exacerbating this problem is the rise of "always-on" Internet connections such as cable modems or DSL connections. The more people there are using the Internet, the more opportunities there are for hackers to steal data or hijack systems.

Until now, detecting and stopping hackers meant purchasing expensive hardware or mastering complex networking tools. BlackICE Defender gives your home computer the same powerful intrusion detection and protection tools that big corporations use.

What is an Intrusion?

When you connect to the Internet your computer is part of a huge global network. You can send data (outbound) and receive data (inbound). When you download photos on a web site, for example, you send a request to the web server (outbound); the web server then transmits the photo data back to your computer (inbound).

Hackers exploit the capability of your computer to communicate with other computers. A hacker can use widely available networking tools to connect to your computer and send it commands. For example, a hacker could connect to your system and download an encrypted file containing your credit card number. Then, using a freely available decrypting program, the hacker cracks the file, gets the number, and goes on a buying spree at your expense.

While your link to the Internet is active, hackers can identify your system and break into it. This is why "always-on" Internet connections, such as cable modems and DSL connections, are particularly vulnerable. For a hacker to break into your system, he must first locate your computer. The more often your system is exposed to the Internet, the more likely a hacker will find it. Some hackers run continuous scans of certain areas of the Internet looking for home computers to hack.

If your Internet connection is live 24 hours a day, a hacker has more opportunities to find your system. Dial-up connections are slightly safer, but still pose a significant opportunity to hackers. While you are chatting online with a friend over a dial-up connection, a hacker somewhere on the other side of the world can locate your computer and break into it.

BlackICE Defender operates like a persistent "traffic cop." When BlackICE detects inappropriate access to your computer, it blocks access to the offending user. Other Internet access remains open and unaffected. Only the hacker is blocked. You can continue to browse the web, send e-mail, and listen to Internet radio stations while BlackICE rejects the hackers.

Many ISPs have some protection against hacking, but this protection only stops the most primitive attacks. Most novice hackers can easily break through your ISP's protection measures. When they do, your computer is vulnerable to attack. If the hacker is able to locate your system, and break through your ISP, BlackICE Defender is there to stop the intrusion before any data is compromised.

Security Levels

When BlackICE detects an attack, it can automatically block access from the hacker's system. However, not all suspicious Internet transmissions are attacks. What constitutes an attack vs. legitimate use of the Internet is not always easy to determine. Some legitimate Internet applications communicate with your computer in such a way that data is sent to you and then executed. For example, an online virus-scanning tool may appear to BlackICE as an attack, since the web site is transmitting data directly to your computer and then executing it.

Hackers often take advantage of legitimate Internet technologies to make their activities seem innocuous. One of the most common ways to hack into a computer, for example, is to exploit open "ports".

A *port* is a virtual "connection point" on your computer. When you are connected to the Internet, your computer communicates with other computers via virtual ports. For example, when you download your e-mail, your computer establishes a connection on TCP port 110 to your ISP's mail server. Port 110 is the TCP port nearly all mail servers use. After sending logon information, the mail server responds and transmits your e-mail to your computer.

Communication ports are divided into two categories: *System* and *Application*. The System Ports, or low-end ports (ports 0 – 1023), are used for services installed on a computer, such as e-mail or web browsing. The Application ports, or high-end ports (ports 1024 – 65535), are used by client applications such as chat programs or an Internet telephone.

It is generally harder to crack high-end ports since they are only open when specific applications are running. The lower ports are easier to crack since many of them are always open.

Additionally, there are different types of ports: TCP and UDP. TCP connections are the most common. They are used for web browsing, downloading files, and other networking functions. UDP ports are essentially the same as TCP ports. However, UDP connections do not have the error correction features that TCP has. UDP is most often used for streaming content like RealAudio, or games, such as Quake.

The four **Security Levels** that define how rigorously BlackICE Defender blocks unsolicited traffic are based on ports and port type. You set the security level BlackICE enforces on the system in the BlackICE Settings Protection tab. The more restrictive the security level, the more likely BlackICE will block unsolicited inbound traffic. Outbound traffic is never blocked. This ensures that web browsing and other regular Internet functions remain unaffected.

The BlackICE security levels are: *Paranoid*, *Nervous*, *Cautious* and *Trusting*. The following chart demonstrates the relative protection of these four levels.

Security Level	Port Type	Inbound Ports		Outbound Ports	
		System	Application	System	Application
Paranoid	TCP	☒	☒	☑	☑
	UDP	☒	☒	☑	☑
Nervous	TCP	☒	☒	☑	☑
	UDP	☒	☑	☑	☑
Cautious	TCP	☒	☑	☑	☑
	UDP	☒	☑	☑	☑
Trusting	TCP	☑	☑	☑	☑
	UDP	☑	☑	☑	☑

For a description of each Security Level, please see the Security Level Descriptions topic.
The security level BlackICE Defender should enforce on the system is established in the Protection Tab. On the Protection tab you can also select whether you want to allow Internet file sharing and/or NetBIOS neighborhood.

Security Level Descriptions

Paranoid: The *Paranoid* setting is very restrictive, but useful if your system is enduring frequent and repeated attacks. Under this setting BlackICE Defender blocks all unsolicited inbound traffic. This setting may restrict some web browsing and interactive content.

Nervous: This setting is preferable if you are experiencing frequent intrusions. For the *Nervous* setting, BlackICE Defender blocks all unsolicited inbound traffic except for some interactive content on web sites (such as streaming media and other "application specific" Internet usage).

Cautious: The *Cautious* setting is good for regular use of the Internet. This setting only blocks unsolicited network traffic that accesses operating system and networking services. This is the default security level setting for BlackICE Defender.

Trusting: When set to *Trusting*, all ports remain open and unblocked, and therefore this setting allows all inbound traffic. This setting is good if you have a minimal threat of intrusions.

Please see the following table for examples on how the different security levels respond to some applications. For information about how to establish the BlackICE security level, please see the Protection Tab topic.

Security Level	Examples of Some Applications		
	Blocked	**Configurable***	**Not Blocked**
Paranoid	IRC file transfer (DCC), NetMeeting, PC Anywhere, ICQ	Quake (II, III), Internet Phone, Net2Phone	FTP File transfers, Sending/receiving email, Real Audio, IRC Chat
Nervous	IRC file transfer (DCC), NetMeeting	ICQ, Internet Phone, Net2Phone	All of the above plus: PC Anywhere, Quake (II, III)
Cautious	This setting only blocks unsolicited network traffic that accesses operating system and networking services.		All of the above plus: IRC file transfer (DCC), NetMeeting
Trusting	No applications are blocked.		This setting allows all inbound traffic.

*The **Configurable** column lists applications that are normally blocked, yet can be unblocked through advanced configuration of the application or BlackICE. Please see the Network ICE advICE website for information.

NOTE: If you want to use an application that is blocked under a selected security level, Network ICE recommends lowering the security level while using that application. When finished using the application, you can reconfigure the security level back to a higher setting.

Windows Sharing Features

All Windows-based systems include resource sharing as an integral part of the operating system's networking features. This allows Windows computers to participate in corporate networks and share files between computers.

Unfortunately, the Windows sharing features can also present hackers with an opportunity to access your computer. With sharing enabled, hackers have direct access to the resources of your computer, unless they are password protected. On a corporate network, resource sharing is useful when you need to exchange files with a co-worker or print to a remote printer. But on the Internet, this presents a significant security threat.

BlackICE can block these sharing services to ensure that hackers do not exploit this fundamental component of Windows. For most home users, with a single system connected to the Internet, it is perfectly safe and advisable to block resource sharing. It will not adversely affect your system in any way. See the Protection Tab for information about how to block file sharing and the Network Neighborhood access.

However, if you have a small network at home, or are installing BlackICE on a networked computer at work, you may need to leave resource sharing open to ensure that your computer can participate on the network.

Keep in mind that if you decide to enable the sharing features of Windows, you are exposing your computer to some risk. One way to minimize this risk is to password protect all shared devices, especially hard drive folders.

One way to avert this risk entirely, while still allowing resource sharing, is to install the NetBEUI protocol on your computer(s). NetBEUI is a non-routable protocol developed by IBM Corporation in the mid-1980s. NetBEUI transmissions cannot be transmitted over the Internet and therefore they are ideal for use on a small, internal network. NetBEUI is also not subject to the restrictions of file sharing and the Network Neighborhood blocking.

With NetBEUI and TCP/IP networking protocols on your computer, BlackICE can disable Windows file sharing and the Network Neighborhood lookup while NetBEUI allows access to the computers on your internal network without exposing them to the Internet and hackers.

The Network ICE advICE site provides detailed information about how to install NetBEUI. If you choose to install NetBEUI, make sure to have it as the default protocol.

WARNING: Do not remove the TCP/IP protocol from your system. You cannot access the Internet without this protocol.

Basic Hacking

Most hackers are inexperienced kids looking for fun. They merely want to show their friends that they can hack into a system. Unfortunately, even the most inexperienced hacker can cause severe damage.

Corporations have long known about the risks hackers present to their business. However, most home office, casual computer, and Internet users are unaware of what hackers can do. Hackers can render your computer totally unusable. They can steal or delete data. Hackers that are able to steal your digital identity can make financial transactions on your behalf, such as buying or selling securities or using your credit cards. A resourceful hacker can cause tremendous financial damage to anyone who uses the Internet.

In a 1997 report to a subcommittee of the United States Senate, Robert S. Litt, Deputy Assistant Attorney General stated, “Public reports have estimated that computer crime costs us between $500 million and $10 billion dollars per year. The Computer Security Institute has surveyed 428 information security specialists in Fortune 500 companies; 42% of the respondents indicated that there was an unauthorized use of their computer systems in the last year.”

There are countless stories of hacker communities targeting companies and organizations for any number of personal and political reasons. In 1997 a London trading firm was forced to pay millions of dollars to an unknown group of extortionists who demonstrated that they could wipe out entire systems at will. These extortionists were never captured and the trading firm learned an expensive lesson in network security.

Contrary to what the movies or “cyberpunk” books might depict, not all hackers are kids trying to deface web sites or steal credit card numbers. Many hackers are dedicated criminals and corporate spies trying to steal valuable information from companies and individuals. In the race to build faster and better networks, many companies forget to erect barriers to stop the hackers. Moreover, many home users are completely unaware of the threat of hackers and thus easy targets for hacking.

How They Do It

There are three basic attacks hackers can use to gain access to a system or network:

Internal Intrusions

An internal intrusion comes from within a corporation or network. It can be as simple as a curious employee or a serious attempt to hurt a company. Internal intrusions account for the most damage to companies because they come from people who already know the company, its security policies, and vulnerabilities. BlackICE can stop some internal intrusions.

External Intrusions

External intrusions consist of people trying to break into systems from the outside. These types of events are almost always malicious in nature; and they include, for example, attacks over the internet. BlackICE Defender can stop external threats cold. Moreover, it can collect information about an external hacker to help you better defend yourself against that hacker in the future.

Social Intrusions

A social intrusion is when a hacker poses as an employee, authority figure, or friend, in an attempt to get sensitive information about you and your systems. Perhaps the most common social intrusion is people posing as a system administrator asking for your password. Fortunately, social intrusions are pretty rare and easy to identify. Unfortunately, no software can stop a hacker armed with legitimate information he stole.

Good Security Practices

You have already taken the first step toward stopping hackers with BlackICE. In addition to BlackICE Defender you should consider the following good security practices:

> **Turn computer off when not in use**. If you have a DSL or cable modem connection, turn your computer off when not using it. These "always on" connections are particularly vulnerable because they provide more opportunities for hackers to find your computer.

> **Protect passwords**. Never give out a password or any sensitive information to an unsolicited telephone call or e-mail.

> **Be careful what goes out over e-mail**. Never e-mail sensitive information such as passwords, credit card information, etc. to people unless you have software installed that can encrypt your e-mail.

> **Know the web sites you visit**. Never submit sensitive information via a web page unless the web site uses secure connections. You can identify a secure connection with a small "key" icon on the bottom of your browser (Internet Explorer 3.02 or better) or a closed "lock" (Netscape 3.0 or better). If a web site uses a secure connection, it is safe to submit information. Secure web transactions are quite difficult to crack.

> **Protect network addresses**. Never reveal your cable modem, DSL, or ISP connection's IP address or other system networking information to anyone. Your telephone company and Internet Service Provider should already have this information.

> **Be careful of files e-mailed to you from people you do not know**. One common way of getting viruses, as well as inadvertent installations of software that allow intruders easy access to your system, is to embed the software into some cute dancing baby executable or in an innocent-looking e-mail attachment. While you are laughing at the antics of some on-screen cartoon, hackers are opening up your system and looking for files to steal.

> **Change your passwords regularly**. Also, use passwords that are not easy to figure out. The most difficult passwords to crack are those with upper and lower case letters, numbers, and a symbol such as % or #.

> **Upgrade your software and operating system regularly**. Many older versions of software, especially web browsers, have well known security deficiencies. When you upgrade to the latest versions, you get the latest patches and fixes. Furthermore, make sure your computer operating systems are up to date. Microsoft, Sun, HP, Apple, Be, and Linux vendors routinely issue Service Packs that upgrade the components of their operating systems. Make sure you always have the latest service packs installed on your systems. Check your web browser's vendor's site regularly for any security patches that you may need to download and install.

> **Chat rooms**. If you use "chat rooms" or IRC sessions, be careful with any information you reveal to strangers. Hackers are notorious for "address harvesting" from chat rooms and other interactive areas.

> **Pay attention to odd computer behavior**. If your system starts exhibiting odd behavior, check the BlackICE summary application for signs of possible attacks. Some hackers set off attacks that slowly cause your system to become unstable or unusable. If this happens a lot, notify your ISP and reboot your machine. In extreme cases, hackers can damage the operating system on your computer, which would require re-installing the operating system.

> **Beware the Blue Screen of Death.** If you are using Windows NT and your system suddenly displays a blue screen, write down the information at the top of the screen. Proceed to check the BlackICE summary application to see if any attacks occurred at the time of the problem. If so, contact your ISP. Some serious Windows errors are the result of hackers or viruses on a system.

> **Always shred confidential information**, particularly about your computer, before throwing it away. A dedicated hacker will dig through the trash of companies or individuals for information that might help them access your system.

How BlackICE Defender Works

BlackICE Defender consists of an extremely powerful detection and analysis engine that constantly monitors the inbound and outbound traffic between your computer and the Internet or any other computers on a network.

When suspicious behavior is detected, BlackICE Defender springs into action, logging all possible information about the event. The information BlackICE collects regarding the attack is analyzed with sophisticated networking algorithms. If BlackICE determines that the attack poses an immediate threat to the system, then the BlackICE protection features automatically block ALL access from the attacking system.

No matter how hard the hacker tries to crack your system, he cannot avoid BlackICE. Once BlackICE Defender detects an attack, it begins to block the hacker at the "packet level". Any further transmission the hacker sends is rejected before it ever gets inside your computer.

Information about a detected attack is displayed on the BlackICE Defender's **Attacks tab**. BlackICE does not only report the attack, though, it also tells you exactly who carried it out. BlackICE performs a trace over the Internet to gather information about the hacker's system. This information is displayed on the BlackICE Defender's **Intruders tab**, and includes the attacker's IP, DNS and MAC addresses. In extreme cases, this information could be very valuable if you wish to pursue legal action against the hacker. For more information, please see the Back Tracing tab.

BlackICE also captures attack data in evidence files. These files contain data that the hacker sent to your computer. In the hands of an experienced network engineer or Internet Service Provider, evidence files may help explain what the hacker did. See the Evidence Files topic for more information.

Additionally, the **History tab** displays attacks and network traffic in colorful line graphs. This can help you spot trends and patterns in when hackers are trying to get into your computer.

For more information about BlackICE Defender features, please see How to Use BlackICE.

BlackICE Defender Features

The BlackICE Defender software consists of two components: the resident detection and protection engine that guards your computer from attacks; and the summary application, which provides a user-interface to the BlackICE software.

BlackICE Engine

BlackICE was written from the ground up to work with modern, Internet-enabled systems. Therefore, the core of the BlackICE Defender product is its powerful engine, which detects, analyzes, and stops hackers before they break into your system.

The BlackICE engine constantly monitors the ports and services on your system. If a suspicious event is detected, BlackICE analyzes the traffic using a series of advanced algorithms and dynamic filters to determine if the event is a serious attack or a legitimate use of the system. Depending on the configuration settings, BlackICE Defender can also open an evidence file to collect network traffic related to the intrusion.

As soon as an intrusion is detected, BlackICE Defender activates its protection measures. There are two parts to these BlackICE protection measures: the *standard protection filter*, and the *dynamic protection filter*.

The *standard protection filter* stops many common attacks before they can ever get started. This includes stopping corrupt packets, badly fragmented packets, and a lot of other potentially intrusive network traffic. The standard filters include configurable filters for IP addresses, TCP and UDP ports.

The *dynamic protection filter* works much like an IP address filter used on routers and other network devices. When a malicious attack is detected, BlackICE adds the hacker's IP address to a dynamic address filter table. Regardless of what the hacker does, any traffic from the hacker's IP address is rejected.

After 24 hours, the attacker's IP address is removed from the filter. Since many hackers *spoof* legitimate IP addresses, this stops the hacker but does not permanently impede legitimate traffic to your system.

It is important to note that the BlackICE Defender engine is virtually undetectable to a hacker. BlackICE runs "silently" and "invisibly" on your system. It has a small memory footprint and is therefore not easily disabled. Only a user physically located at the computer can disable BlackICE Defender.

BlackICE Summary Application

The summary application is the user interface component of BlackICE Defender. It displays all the network intrusion events on your computer. Details about the attacks on your system, information about the intruders performing these attacks, and BlackICE's response to these events, help you determine the severity and location of the intrusions. Additionally, the summary application displays the recent network traffic and attacks in graph format to allow you to view patterns or spikes in network activity.

Please see the How to Use BlackICE topic for more information about the different BlackICE summary application tabs.

BlackICE Defender. BlackICE Defender is designed for home and small-business users. BlackICE Defender is ideal for “always on” Internet connections such as cable modems and DSL. BlackICE Defender can monitor and block any intrusions from any computer, anywhere on the Internet.

BlackICE Agent. Intended for workstations on corporate networks, BlackICE Agent features the same powerful detection and protection as BlackICE Defender. However, this version integrates with an ICEcap server for the ultimate network defense against intruders.

BlackICE Sentry. This version of BlackICE is specially tuned to monitor key subnets of a network and report any suspicious activity to an ICEcap server. BlackICE Sentry is ideal for monitoring devices not covered by other versions of BlackICE or that are connected to the network via shared media.

Hacker: Generally, a hacker is anyone who enjoys experimenting with technology, including computers and networks. Not all hackers are criminals breaking into systems. Many are legitimate users and hobbyists. Nevertheless, some are dedicated criminals or vandals.

What Are Evidence Files?

Evidence files are part of BlackICE Defender's intrusion monitoring features. As a hacker attempts to break into your system, BlackICE Defender captures network traffic attributed to the hacker and places that information into an *evidence file*.

BlackICE evidence files are located in the `<installation directory>` folder. If you installed BlackICE to the Program Files directory on the C: drive (the default), for example, the evidence files would be located in `C:/Program Files/Network ICE/BlackICE`. Each file has an `*.enc` extension.

The number of evidence files BlackICE captures, the filename prefix, and the size of each evidence file are established on the BlackICE configuration Evidence Log Tab.

To view the contents of an evidence file, you need a trace file decoding application. Many networking and security product companies produce such decoders. There are also some shareware decoders available on the Internet.

If you are running Windows NT Server 4.0, you can install the Network Monitoring service. This service includes the trace file decoding application Network Monitor.

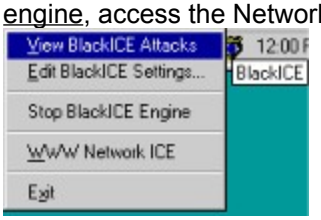
For more information about installing the Network Monitoring service or using the decoding tool, refer to the documentation included with your copy of Windows NT Server 4.0.

How to Run BlackICE Defender

> From the Windows **Start** menu, select **Programs**, **Network ICE**, then **BlackICE Utility**.

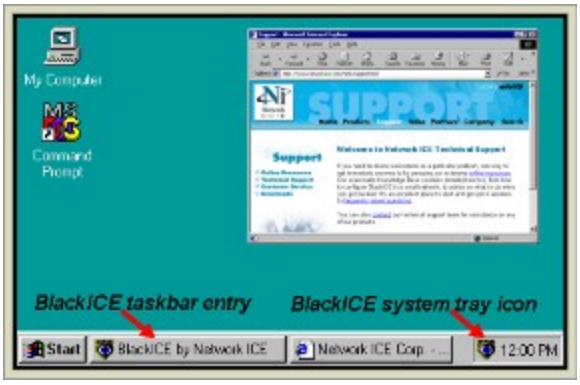
> If BlackICE is already running, a small icon is displayed in the system tray.

1. Right click on the icon. A sub-menu of choices is displayed.
2. Select **View BlackICE Attacks**.
3. You can also use this submenu to display the BlackICE settings, Start or Stop the BlackICE engine, access the Network ICE web site, or Exit BlackICE.



> A single regular click on the system tray icon also opens the utility.

> When BlackICE Defender is open, there is an entry displayed on the Windows taskbar. This entry remains in the taskbar when the application is open, minimized, or hidden. A single regular click on the taskbar entry displays the BlackICE summary application.



NOTE: Closing or exiting the summary application does not turn off the protection and detection engine of BlackICE. If you wish to stop the BlackICE engine, please see How to Stop BlackICE. If the BlackICE engine is stopped, a diagonal red line is displayed over the system tray icon. If you see this line, but do not want the engine turned off, also see How to Stop BlackICE for instructions on how to restart the BlackICE service.

How to Stop BlackICE Defender

Although it is not recommended, there may be special circumstances that require you to stop BlackICE Defender on a system. When the BlackICE Defender intrusion detection and protection engine is stopped, the system is no longer protected from any network intrusions. If this is the case, then a red diagonal line is displayed over the BlackICE system tray icon.

There are several methods to stop or, if stopped, restart BlackICE Defender. To ensure that a hacker does not stop the BlackICE Defender engine, only someone sitting at your system can do this.

NOTE: Closing or exiting BlackICE does not stop the BlackICE monitoring and protection engine.

If you wish to completely remove (uninstall) BlackICE Defender from your system, please see How To Uninstall BlackICE. For more information about the BlackICE intrusion detection and protection engine, please see the BlackICE Defender Features.

From the Summary Application

1. From the Menu Bar, select **Tools**, then **BlackICE Engine**.
2. If the BlackICE engine is currently running, then select **Stop BlackICE Engine**.

   If the BlackICE engine is currently not running, then the available option is **Start BlackICE Engine**.

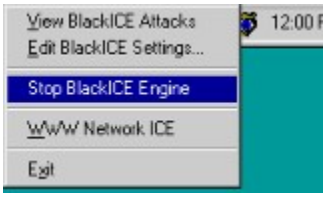
> The BlackICE engine is stopped, and the BlackICE Defender service is no longer protecting your system.

To restart BlackICE Defender, follow the same steps as above, but select the now available **Start BlackICE Engine**. BlackICE will also restart when the system is rebooted.

From the Desktop

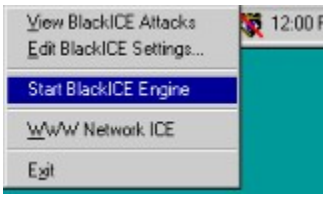
1. Right-click on the system tray icon.
2. A sub-menu of choices is displayed. Select **Stop BlackICE Engine**.

   If the BlackICE engine is currently not running, then the available option is **Start BlackICE Engine**.



> The BlackICE engine is stopped, and the BlackICE Defender service is no longer protecting your system.

To restart BlackICE Defender, select the now available **Start BlackICE Engine** from the BlackICE system tray icon sub-menu. BlackICE will also restart when the system is rebooted.



How to Configure BlackICE

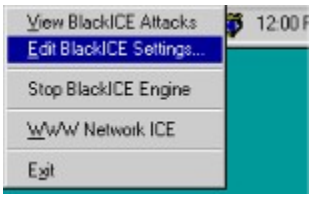
BlacKICE allows you to view and modify the configuration parameters of the application.

To customize the monitoring, detection, and use of BlackICE Defender you must use the Settings dialog box. The Settings dialog box is accessed either from the BlackICE system tray icon, or from the BlackICE Defender summary application.

> If BlackICE is not running on your system, then from the Windows **Start** menu, select **Programs**, **Network ICE**, then **BlackICE Utility**.

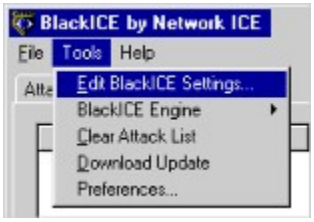
From the Windows TaskBar

1. Right-click on the BlackICE icon displayed on the system tray. A sub-menu of choices is displayed.
2. Select **Edit BlackICE Settings…**. The BlackICE Settings window is displayed.



From the BlackICE Defender Summary Application

1. Click the **Tools** option on the Menu Bar.
2. Select **Edit BlackICE Settings …** from the sub-menu. The BlackICE Settings window is displayed.



The Settings window has several tabs. For more information on the tabs and the configuration parameters that can be viewed and modified, click on the tab of interest:

Protection Tab
Back Trace Tab
Packet Log Tab
Evidence Log Tab
Trusted Addresses Tab
Blocked Addresses Tab
ICEcap Tab

How to Handle Intrusions

Intrusions are a normal part of any modern network. BlackICE Defender reports all unauthorized access to your system. However, not all unauthorized access constitutes an intrusion. Before responding to an intrusion, it is therefore best to determine if the intrusion is a real attack. When assessing an intrusion consider the following:

Intrusion Considerations

> Does the attack have a numeric severity of 59 or less? Attacks under this level are mostly probe and scan attacks. These are not particularly dangerous but may indicate a prelude to an attack. It is better to keep track of these intruders and wait for a more serious attack.

> Was BlackICE able to gather back trace information? Very clever hackers will purposefully mask DNS, NetBIOS and MAC address information. Therefore, attacks with high severities (over 59) with no back trace information may indicate the activity of an experienced hacker.

> Is the intrusion from one of your own systems? Some networking probes perform routine scans of the network to check the availability of systems. These scans are completely safe, but BlackICE will detect and report them.

> Is the intrusion from your Internet Provider? Many Internet providers perform regular scans of their network. These events are completely safe.

How to Respond

> Manually configure BlackICE Defender to block the intruder. The intruder can then no longer perform attacks against your system. See How To Block an Intruder for more information.

> Raise the BlackICE security level. See the Security Levels topic for more information.

> Go to the source. Locate the Internet Service Provider (ISP) for the hacker and report the hacker's activities. Most ISPs have terms of use that strictly prohibit hacking activities.

  It is best to send an e-mail to the ISP with your complaint. Please do not call; most ISPs and corporations do not have the staff to handle individual abuse complaints.

  You can select the corresponding attacks from the Attacks tab, or the intruder from the Intruders tab, and then copy and paste the information into the e-mail. When notifying an ISP include the following information: your name, your location, your time zone, date and time of the attack, the type of attack, the hacker's IP address, DNS and MAC address. If possible attach the *.log (back tracing) and *.enc (evidence) files applicable to the attack. These files are located in the directory where you installed BlackICE.

Additional Information About Attacks

For the most current information about each attack type, visit the NetworkICE **advICE** web site at www.networkice.com/advice. This site includes detailed information about intrusions and how to defend your system against them. From the BlackICE summary application, select the attack of interest in the Attacks tab, and then click on the **advICE** button.

Download the BlackICE User's Guide. This guide provides more detailed information about using BlackICE. You may also want to download the Network ICE Attacks and Vulnerabilities Reference Guide.

How to Block an Intruder

Under normal conditions, BlackICE Defender will allow other systems to access your computer without hindering the network traffic in any way. Most “intrusions” on systems are innocuous port scans or ping sweeps. These intrusions are not dangerous, thus BlackICE Defender does not automatically block the intruding addresses.

BlackICE Defender only blocks intruders when they initiate an attack that is an immediate threat to the computer. A LAND attack, for example, could cause a system to crash; therefore, BlackICE blocks any intruder attempting a LAND attack.

However, BlackICE provides a way to manually block any address that has initiated an attack against your computer. This lets you block out systems at your own discretion.

WARNING: Be careful which systems you block. Nearly all Internet Service Providers (ISPs) conduct routine scans to check the state of connected clients. If you block your ISPs scans they might restrict your access or even terminate your account. For help identifying your ISPs systems, contact your ISP. Typically, ISPs use DNS names that identify themselves as a member of the ISPs domain. For example, most @home systems have `.home.com` in their DNS name.

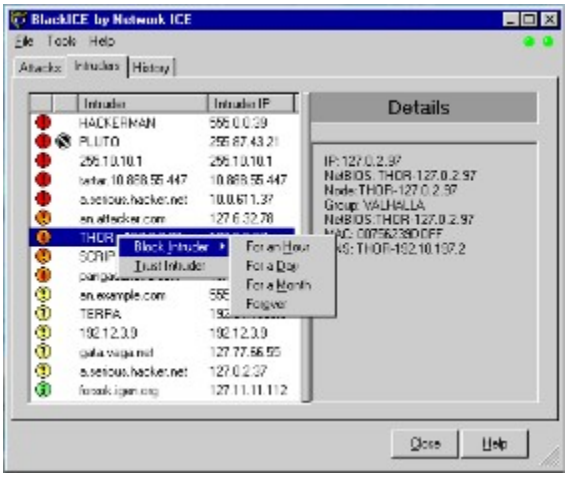
---

1. From the **Intruders** tab, right-click on the intruder you wish to block.

   OR, from the **Attacks** tab, right-click on the attack/intruder combination whose intruder you want to block.

2. From the pop-up menu, select **Block Intruder**.

3. A secondary menu pops up. Select the duration of the block: *For an Hour*, *For a Day*, *For a Month (30 days)*, or *Forever*.



4. If applicable, a confirmation dialog box is displayed. Click **Yes**, to block the intruder frot eh selected amount of time.

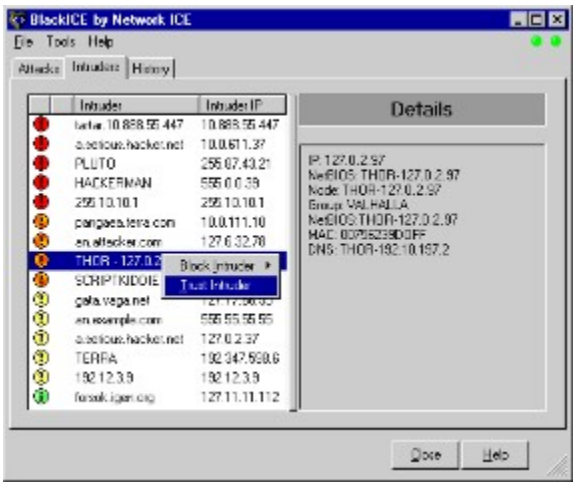
> BlackICE Defender adds the intruder to the Blocked Addresses tab. An Attack Blocked icon is displayed next to the intruder within the Intruders tab. This icon indicates that BlackICE is presently blocking all network traffic from that intruder. The icon is removed if and when the blocking expires. To unblock an intruder please see the Blocked Addresses Tab.

How to Trust an Intruder

Sometimes there may be situations in which you want to trust certain systems to ensure that BlackICE does not inadvertently block them. For example, if you have several computers networked together you may want to trust them and thus stop BlackICE Defender from reporting activity from these systems as attacks.

WARNING: When a system is trusted, BlackICE Defender ignores all attacks from that system. Since hackers often mask their true identity through "spoofed" IP addresses, a hacker could use your trusted addresses as a mechanism against you. Network ICE recommends trusting only those systems that you are certain are legitimately executing network scans such as servers from your ISP or an ICEscan server.

1. From the **Intruders** or **Attacks** tab, right-click on an intruder or attack.
2. From the pop-up menu, select **Trust Intruder**.



3. If applicable, a confirmation dialog box is displayed. Click **Yes** to trust the intruder.

> BlackICE Defender adds the intruder to the Trusted Addresses tab. To *untrust* an intruder, please see the Trusted Addresses Tab.

How to Ignore an Attack

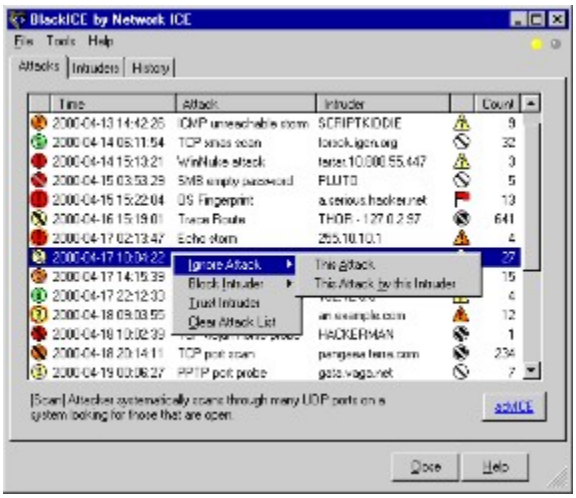
Since some intrusions on your computer may be the result of automated port scans or other legitimate Internet tools, you may want to ignore specific attacks that keep reoccurring. For example, some Internet Service Providers carry out routine port scans and ping sweeps to check the state of downstream clients.

BlackICE Defender gives you the option to ignore these attacks. You can also choose to ignore a specific attack carried out by a particular intruder.

WARNING: When an entire attack is ignored, BlackICE Defender will not log any information about that attack. Be careful which attacks you ignore, since some innocuous attacks could signal a prelude to a serious attack.

---

1. From the **Attacks** tab, right-click on the attack/intruder combination you wish to ignore.
2. From the pop-up menu, select **Ignore Attack**.
3. A sub-menu is displayed. Select how you want BlackICE to ignore the attack.
   This Attack instructs BlackICE Defender to ignore all future instances of the attack.
   This Attack by this Intruder instructs BlackICE Defender to ignore all future instances of this attack by the referenced intruder. If a different intruder executes the same attack, then that event is still logged by BlackICE Defender.



4. If applicable, a confirmation dialog box is displayed. Click **Yes** to ignore the attack.

> BlackICE Defender immediately begins ignoring the selected attack.

How to Clear the Attack List

With time, the attack list becomes rather long. Therefore, you have the option to clear the attack list either from the Menu Bar or directly from the **Attacks** tab.

NOTE: Clearing the attack list does not unblock or un-ignore any attacks or intruders.

1. From the Menu Bar, select **Tools**.

   OR, within the **Attacks** tab, right-click anywhere on the attack list.

2. From the sub-menu, select **Clear Attack List**.

3. If applicable, a file deletion confirmation dialog box is displayed. Click **OK** to delete the entire attack list.

> BlackICE Defender clears out the attack list.

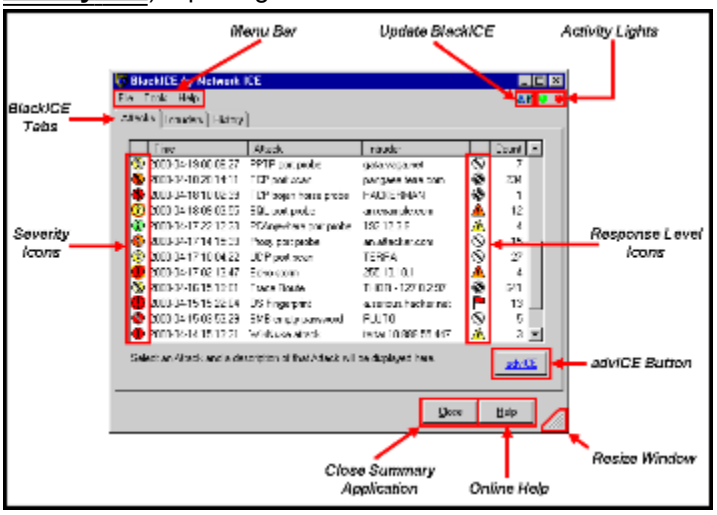
How to Use BlackICE Defender

The BlackICE software not only includes a powerful detection, analysis, and protection engine, but it also features an easy-to-use interface that displays BlackICE's activities.

The monitoring and protection engine of BlackICE Defender is always running when the computer is operating. The engine runs "invisibly" on your system to ensure that a hacker does not accidentally or purposefully disable BlackICE.

The BlackICE Defender summary application displays all the recent attacks on the system and the intruders who made those attacks. It also includes a graph of all the recent network traffic and attacks.

The BlackICE summary application consists of three tabs (the **Attacks Tab**, the **Intruders Tab**, and the **History Tab**) reporting different information about the intrusions BlackICE has detected.



How to Install BlackICE Defender

Installing BlackICE Defender only takes a few minutes. This section steps you through the process of installing the BlackICE application.

Minimum System Requirements

> **Operating Systems**: Windows NT 4.0 (Service Packs 4, 5, 6, 6a), Windows 95, Windows 98, and Windows 2000 (Service Pack 1).

> **Processor**: Pentium or better.

> **Memory**: 16 MB or more.

> **Hard Drive Space**: 10 MB free.

> **Network Protocol**: TCP/IP.

> **Network Connection**: 10/100 Ethernet LAN/WAN, cable modem, DSL router, ISDN router, or dial-up modem.

To Install BlackICE

1. Locate the Setup Application: **`BIDsetup.EXE`**.

   If you have lost your original copy of the software, you can download a new copy from the Network ICE web site at www.networkice.com.

2. Execute **`BIDsetup.EXE`**. The system must unpack the files and verify them. When that is finished, the setup application begins.

3. A welcome screen is displayed. Click **Next** to continue.

   NOTE: If setup detects an existing version of BlackICE, the setup prompts you to remove (uninstall) or continue to upgrade the previous version.

4. Review the **License Agreement**. If you accept the agreement terms, click **I Accept**. Otherwise, click **I Decline** to exit the BlackICE Defender setup application.

5. Verify the destination location (installation path) for BlackICE. This is the folder where you wish to install BlackICE Defender. If you wish to change the path and choose a different installation folder, click **Browse** and locate the path you wish to use. Click **Next** to continue.

6. In the Select Program Folder window, verify the folder where BlackICE shortcuts are located on the Windows Start menu. If you wish to use a different folder, select it from the list or enter a name in the **Program Folders** field. Do not place BlackICE shortcuts in the **Startup** folder. The setup application automatically places a shortcut in the Startup folder to launch the BlackICE user interface when the system is turned on. Click **Next** to continue.

7. Enter the **License Key** provided to you when you purchased BlackICE. If you have lost this key, contact Network ICE customer support at support@networkice.com to obtain a copy of your key. Click **Next** to continue.

8. The Start Copying Files window summarizes all the selections you have made. If you need to change any of those parameters, click **Back** to retrace the previous steps.

   If the information is correct, click **Next**.

   > The installation begins. When it is finished, the BlackICE Defender service is started.

9. The system then prompts you to read the Release Notes. If this is your first time installing this version of BlackICE Defender, it is a good idea to review this information. To review the release notes, check **I would like to view the README file**. Otherwise, leave this box unchecked.

   Click **Finish** to complete the BlackICE Defender setup.

> The BlackICE Defender setup is complete.

How to Uninstall BlackICE Defender

To uninstall BlackICE Defender follow these instructions. Once BlackICE is uninstalled, your system is no longer protected from intrusions.

1. From the **Start** menu, select **Settings**, then **Control Panel**. The Control Panel is displayed.
2. Double-click **Add/Remove Programs**. The Add/Remove Programs Properties dialog box is displayed.
3. Locate **BlackICE** in the list of programs.
4. Select **BlackICE** and click **Add/Remove**.
5. You are prompted to confirm the removal of BlackICE in the displayed Confirm File Deletion dialog box. Click **OK** to continue.
6. A status window is displayed. During the uninstallation the application may prompt you regarding the state of read-only files. Click **Yes** to remove these read-only files. You may also be prompted regarding system files, click **Yes** to remove these files as well.

   Check the **Don't Display this message again** box to stop the setup program from prompting you about such files.
7. On the Maintenance Complete dialog box displayed after the uninstall process, click **Finish** to conclude the removal.

> BlackICE Defender is removed from your system.

How to Update BlackICE Defender

Network ICE issues regular updates to BlackICE Defender to ensure that it can detect and stop the latest attacks. To update your existing installation of BlackICE Defender, you must download the update.

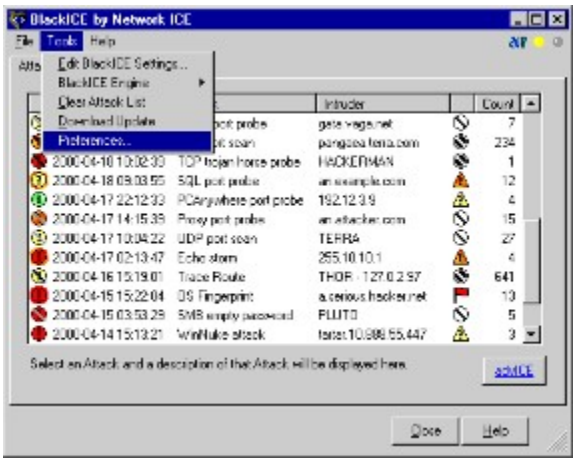
There are two ways to download a new version of BlackICE. BlackICE Defender can automatically check the Network ICE web site for updates at regular intervals; or you can manually instruct BlackICE to check for updates.

Automatically check for BlackICE Defender Updates

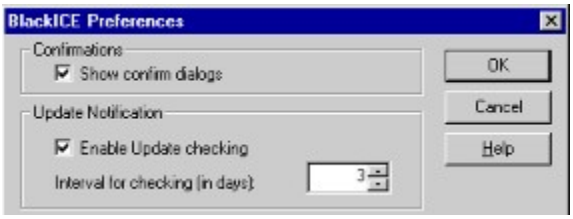
You can set BlackICE Defender to automatically notify you of any updates. In this case, the BlackICE Online Update web page automatically checks your copy of BlackICE Defender at set intervals to see if you have the most recent version. If you do not, then the BlackICE summary application displays the Network ICE logo (Ni) on the top right of the user interface. Click on this logo to download the newest version of BlackICE.

To establish the automatic update notification of BlackICE Defender, follow these steps.

1. From the BlackICE summary application Menu Bar, select **Tools,** and then **Preferences…**.



2. In the displayed BlackICE Preferences dialog box, select **Enable Update checking** to have BlackICE automatically check the Network ICE website for updates. This option is disabled by default.



3. Enter how often you want BlackICE to check for updates in the **Interval for checking** edit box (in days). The default automatic update check time is every 3 days.

   NOTE: If the update check time is 3 days, then BlackICE will check for updates when you first enable update notification, and then every 3 days after that. However, the 3 day cycle is restarted if you reboot your computer, or if you stop and then restart BlackICE Defender from within the summary application. Exiting or closing the summary application does not affect the update cycle; BlackICE will continue to check for newer versions even if closed. If a newer version of BlackICE Defender is available, then you will see the update notification icon when the summary application is opened.

4. Click **OK** to immediately implement automatic updating. The Preferences dialog box is closed and you return to the BlackICE user interface.

   NOTE: If you access the Internet via a dial-up connection, your system may automatically initiate your connection when updating BlackICE Defender.

5. BlackICE checks the Network ICE web site for updates at the selected interval. When a new version of BlackICE is available, the Network ICE logo  will be displayed on the user interface.
6. Click on the logo to connect to the Network ICE update web site.

   You will be prompted to run the setup file across the network, or given the option to download and save the update file. If you download the update, double-click the downloaded **update.exe** to update BlackICE Defender.

   If you have the latest version, the web page displays your version number and license key.

Manually Update BlackICE Defender

If you do not wish to have BlackICE Defender automatically notify you about updates, you can manually instruct BlackICE to connect to the Network ICE web site and check for new versions.

1. From the BlackICE summary application Menu Bar, click **Tools**.
2. A sub-menu is displayed. Select **Download Update**.
3. BlackICE Defender opens a web browser session and connects to the Network ICE web site. The site checks your version against the Network ICE database. If there is a newer version available, click the link.

   You will be prompted to run the setup file across the network, or given the option to download and save the update file. If you download the update, double-click the downloaded **update.exe** to update BlackICE Defender.

   If you have the latest version, the web page displays your version number and license key.

BlackICE Defender Alarm Preferences

BlackICE has several configurable settings. One of these is the attack notification preference.

In addition to examining attacks in the open summary application, you can set BlackICE Defender to visually or audibly notify you in the event of an attack. Both the audible and the visual alarm systems are configurable. You select how BlackICE notifies you, and then set the severity level that triggers the alarm.

The visual alert is a flashing system tray icon. Whenever an attack of the set severity is detected, the BlackICE tray icon flashes the color of the attack. The flashing continues until the summary application is opened. If BlackICE detects another attack before the summary application is viewed, then the tray icon flashes the color of the most severe attack. For example, if the tray icon starts to flash orange  , then a *serious* event is the most severe attack detected since the summary application was last opened.

The audible alarm consists of a `.wav` file of your choice that sounds whenever an attack of the pre-determined severity is detected.

The visual alarm option notifies you of an event when the summary application is closed, minimized, or hidden. The audible alarm is triggered regardless of the state of the BlackICE window.

Both the visual and audible attack notification settings are optional. For more information about how to establish the BlackICE Alarm settings, please see How to Set BlackICE Preferences.

How to Set BlackICE Preferences

BlackICE Defender allows you to set various parameters that affect the functions of the application. The settings that are established within the Preferences dialog box are the following:

> ***Confirmations***: When you clear the attack list, ignore an attack, trust or block an intruder, a confirmation dialog box is displayed to verify the desired change. You can turn this protection measure on or off at your discretion.
>
> ***Update Notification***: BlackICE Defender can notify you when a new version of the software is available. If you enable the update notification option, then BlackICE will check the Network ICE website for updates at regular intervals. For more information about the automatic or manual updating of BlackICE Defender, please see How to Update BlackICE.
>
> ***Attack Notification***: BlackICE alarm preferences control how and when the application notifies you of an attack. For more information about BlackICE alarms, please see the BlackICE Defender Alarm Preferences topic.

To Customize BlackICE Preferences

1. From the BlackICE summary application Menu Bar, select **Tools**.
2. A sub-menu is displayed. Select **Preferences…** The BlackICE Preferences dialog box is displayed.
3. Select the **Show confirm dialogs** check box to display confirmation dialog boxes when clearing the attack list, ignoring attacks, trusting and blocking intruders. By default this option is enabled.
4. Select **Enable Update checking** to have BlackICE automatically check the Network ICE website for updates. This option is disabled by default.
5. Enter how often you want BlackICE to check for updates in the **Interval for checking** edit box (in days). The default automatic update check time is every three days.

   NOTE: If you access the Internet via a dial-up connection, your system may automatically initiate your connection when updating BlackICE Defender.
6. Select the **Visible Indicator** check box to flash the tray icon the color of the most severe attack until the summary application is opened. This option notifies you of an event when the summary application is closed or hidden.

   From the options below, select the severity level that triggers the alarm. The default setting notifies you visually if any suspicious , serious
or critical
attacks are detected.
7. Check **Audible Indicator** to play a `.wav` file of your choice whenever an event of the selected severity is detected. The audible alarm is triggered regardless of the state of the BlackICE window.

   From the options below, select the severity level that triggers the alarm.

   > **(Critical)**: The selected alarm option is triggered only when BlackICE detects a critical event. Critical events are deliberate attacks on your system for the purpose of damaging data, extracting data, or crashing the system. Critical events have a severity number of 100 – 75.

>
(Critical and Serious): The selected alarm option is triggered when BlackICE detects a critical or serious event. Serious events are deliberate attempts to access information on your system without directly damaging anything. These events have a severity number of 74 – 50. Therefore, this option will alert you to attacks of severity 50 or above.

>

(Critical, Serious and Suspicious): The selected alarm option is triggered when BlackICE detects a critical, serious or suspicious event. Suspicious events are network activities that are not immediately threatening, but may indicate that someone is attempting to locate security vulnerabilities on your system. Suspicious events have a severity number of 49 – 25. Therefore, this option will alert you to attacks of severity 25 or above. This is the default alarm option.

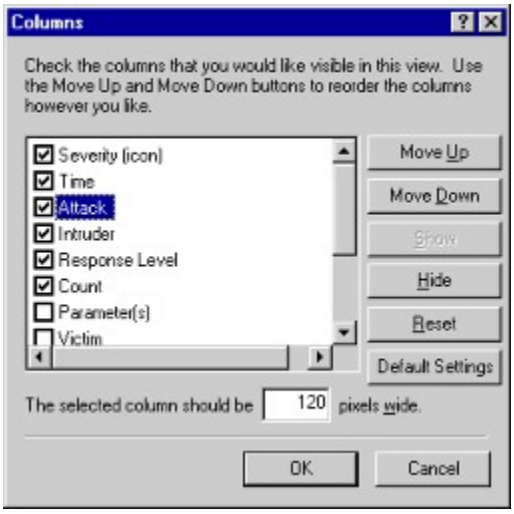
8. If the **Audible Indicator** option is checked, then the **WAV File** field displays the default alarm sound (`bialarm.wav`). To change the `.wav` file used in audible notification, click the folder icon to browse your system, and locate the path desired. The selected alarm file is now displayed in the **WAV File** field. To listen to the selected `.wav` file, click **Preview**.
9. Click **OK** to start implementing the selected preference settings.

How to Configure the Tab Columns

BlackICE allows you to configure the columns displayed on the Attacks and Intruders tabs. You can customize which columns are displayed, as well as arrange the order and size of those columns.

NOTE: Removing columns from a tab does not remove that column's information from BlackICE. It only removes the column from the displayed tab information. You can add and remove tab columns at any time.

1. From the tab within which you want to customize the columns, right-click on a column header.
2. Select **Columns...** from the pop-up menu. The Columns dialog box is displayed.



3. To add a displayed column to the tab, select the column name and click **Show**. Alternatively, you can select the check box to the left of the column name.
4. With the column name selected, click **Move Up** or **Move Down** to place the column in the position you wish it displayed on the tab. The top column is the leftmost column displayed on the tab.
5. You can manually set the width of the selected column. Enter the number of pixels in the appropriate field within **The Selected column should be … pixels wide**.

   To modify the column width within the tab, hover your mouse over the dividing line between two column headers. A cross-arrow is displayed. Click and drag the cross-arrow to increase or decrease the column size.
6. To remove a column from the tab, select the column name and click **Hide**. Alternatively, you can clear the check box to the left of the column name. Columns that are not selected in the Columns list are automatically moved to the bottom of the list when the column selection is applied.
7. If you do not wish to implement the column selection changes you just made, click **Reset** to return to the previous column selections.
8. To reset the tab to its default columns, in their default order and width, click **Default Settings**.
9. When you are finished customizing the column list, click **OK**.

> Your column changes are displayed. Columns can be moved, added or removed from the tab at any time.

BlackICE System Activity Lights

In the upper, right corner of the BlackICE Summary Application there are two Activity Lights. These lights display the inbound and outbound network traffic on your system. The light on the left is outbound traffic (transmissions from your system to another), while the light on the right is inbound traffic (transmissions coming to your system).

As network packets leave and are received by your computer, these lights blink. If there is a lot of traffic, the light(s) may stay on steadily while the traffic passes through your network interface.

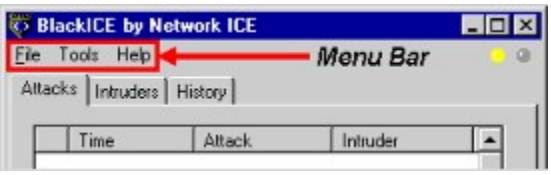
In addition to displaying network traffic, these lights also show the type of traffic. A green light indicates normal, informative, and safe network traffic, while a red light indicates packets from a hacker conducting a critical level attack.

The table below summarizes the colors of the System Activity Lights display.

Icon	Description
	No System Activity: *Gray light*. No network traffic.
	Normal System Traffic: *Green light*. BlackICE Defender detects normal, non-threatening network activity.
	Suspicious Event Detected: *Yellow light.* BlackICE is detecting network activity that, although not immediately threatening, may indicate an attempt to locate security vulnerabilities on your system. Look on the Attacks tab to obtain more information about the event.
	Serious Event Detected: *Orange light.* BlackICE is detecting a deliberate attempt to access information on your system. A serious event does not directly damage your system. If you see this color on the right light, please go the Attacks tab to obtain more information about the event.
	Critical Event Detected: *Red light.* BlackICE is detecting a deliberate attack on your system. Critical events are attacks that try to damage data, extract data, or crash your system. These events always trigger BlackICE protection measures. If you see this color on the right light, please go the Attacks tab to obtain more information about the event.

Menu Bar Commands

This menu is displayed above the BlackICE Defender summary application tabs.



The **Menu Bar** offers the following commands:

File

Allows you to **Exit** BlackICE Defender. Click **Exit** to close the BlackICE summary application. The BlackICE notification icon is removed from the taskbar. The intrusion-monitoring engine remains active.

Tools

Shows you a menu that lets you edit the BlackICE Defender settings (configure the application); start or stop the BlackICE engine; clear the attack list; download the latest version; or change other various preferences.

Help

Shows you a menu that offers links to the online help system, the World Wide Web page for Network ICE, or information about BlackICE.

Help Menu Commands

The **Help** menu offers commands that provide assistance using and troubleshooting BlackICE Defender.

BlackICE Help Topics

Displays the BlackICE Application Help Index tab (this help system).

Online Support

Opens a web browser session and displays the Network ICE Support Frequently Asked Questions (FAQ) web page. Your system must be connected to the Internet to display this page.

WWW Network ICE

Opens a web browser session and displays the Network ICE home page. Your system must be connected to the Internet to display this page.

About Network ICE BlackICE

Displays the version number of this application.

Tools Menu Commands

The **Tools** menu offers the following commands. These commands let you modify several different options within the BlackICE Defender application.

Edit BlackICE Settings…

Select to configure the BlackICE application.

BlackICE Engine

Depending on the current state of the BlackICE engine, this option displays a sub-menu to start or stop BlackICE.

Clear Attack List

Allows you to clear the entire attack list.

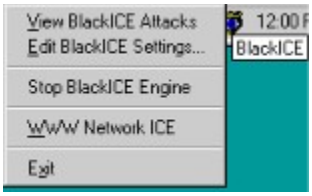
Download Update

Select to connect to the Network ICE web site and download the latest version of BlackICE Defender.

Preferences

Displays a sub-menu that includes several BlackICE Defender options.

System Tray Icon Menu



The **System Tray Icon** menu offers the following commands, which provide you assistance with this application:

View BlackICE Attacks

Select to open the BlackICE application.

Edit BlackICE Settings…

Select to configure the BlackICE application.

Stop *or* Start BlackICE Engine

Depending on the current state of the BlackICE engine, select this option to start or stop the engine.

WWW Network ICE

Links you to the World Wide Web page for Network ICE.

Exit

Exit the BlackICE summary application. The BlackICE system tray icon is removed from the taskbar. The intrusion-monitoring engine remains active.

Attacks Tab

The **Attacks** tab summarizes all intrusion and BlackICE system events on your computer. The tab displays such information as: the time, type, and severity of an attack; the intruder's name and IP address; and how BlackICE Defender has responded to the attack.

By default, the information in the Attacks tab is sorted first by time then by severity. Clicking a column header re-sorts the list by that column. Clicking the column header again toggles the sort order (ascending or descending). Alternatively, you can right-click on the column header to display a pop-up menu that allows you to sort the column in ascending or descending order. For more information see the How to Configure Tab Columns topic.

When you select an attack in the Attacks tab, a brief description of the attack is displayed at the bottom of the tab. If you want further information, or wish to see suggested remedies for the selected attack, click on the **advICE** button.

Double-clicking the event on the Attacks tab displays the corresponding attack's intruder on the Intruders tab. The Intruders tab aggregates all known information about the intruder.

Attacks Tab Columns

The **Attacks** tab consists of several configurable columns that display event information. Adding, removing or reordering these columns can customize the look of the tab. By default, only five columns are displayed; the other tab columns are optional. To display different columns on the tab, right-click on a column header and select **Columns…**. For detailed instructions, please see the How to Configure Tab Columns topic.

See the Attacks tab component name below for more information about the different columns:

Severity Icon

This is a visual representation of two important factors: the severity of the attack; and the action BlackICE took in response to the attack (the response level). Each event is indicated with one of four severity levels, overlaid with one of five response levels. For example, if BlackICE blocks a suspicious attack, then a black diagonal line is displayed over the *suspicious event* icon to create the following image: .

BlackICE generates internal system events (such as software errors or issues) that are also displayed on the Attacks tab Attack List. The severity attached to these system events are meant to indicate the level of urgency associated with the event. Therefore, if a BlackICE system event is of *critical* severity, then you should resolve that issue as soon as possible.

Time

Date and time of the attack/event listed in the format: YYYY-MM-DD-hh:mm:ss. The time is in a 24-hour format for the time zone applicable to your system.

Attack

The name of the attack. For more information about a particular attack, select the attack in the list. A brief description of the attack is displayed at the bottom of the screen.

For a full description of an attack, as well as suggested remedies, select the attack of interest and click the **advICE** button. For extra options on how to respond to an attack or how to report an intruder, see How to Handle Intrusions.

Intruder

The best name BlackICE Defender can gather from the attacking system. This column displays the NetBIOS (WINS) name or DNS name for the attacking system. If BlackICE cannot determine a name, then it displays the intruder's IP address.

For more information about a particular intruder, double-click an event on the Attacks tab. The

application displays the Intruders tab, which aggregates all known information about each intruder who has provoked an event on your system.

Count

When an intruder executes the same attack several times in a row, BlackICE Defender displays how many times that attack occurred. The count is therefore the number of repeatedly executed instances of an attack. The time stamp of the attack indicates the most recent occurrence.

Response Level Icon

This is a visual representation of the protection BlackICE provided against the attack. Each event is indicated with one of five response levels.

Parameter(s)

When an intruder carries out an event, BlackICE can often determine details about that attack. For example, if the attacked port is identified, the Parameter field lists the port number as well as any other information BlackICE could gather. For details about a specific attack's parameters, visit the Network ICE advICE web site. The Parameter(s) column cannot re-sort the Attacks list.

Victim

This column displays the NetBIOS (WINS) name or DNS name of the attacked system (the victim). In most cases this is your system. If BlackICE cannot determine a name, it displays the victim's IP address.

Victim IP

The IP address of the attacked system.

Intruder IP

The IP address of the attacking system.

For more information about a particular intruder, double-click an event on the Attacks tab. The application displays the Intruders tab, which aggregates all known information about each intruder who has provoked an event on your system.

Attack ID

Internal number BlackICE uses to reference each unique attack signature.

Severity (numeric)

This is the numeric representation of the severity of the attack.

Other Attacks Tab Elements

Attack Description

Below the attack list, BlackICE Defender displays a brief description of the selected attack. For additional information about the attack, click **advICE**.

advICE

Opens a browser session that accesses the advICE section of the Network ICE web site. Select the particular attack of interest and click **advICE**. Information about that specific intrusion is displayed.

NOTE: If your Internet connection is via dial-up modem, and you are not currently connected, the modem will dial out to the Network ICE website when you click **advICE**.

Close

Closes the BlackICE Defender summary application. The detection and protection engine remains active.

Help

Displays the online help for the Attacks tab.

Attacks Tab Right-Click Options

Right-click on a list item to Ignore an Attack, Trust an Intruder, Block an Intruder, or Clear the Attack List.

Severity Indicator Column (Icons)

The following icons indicate the severity of an attack. There are four severity levels: critical, serious, suspicious and informational.

In the Attacks tab, each event (attack) is also overlaid with one of five response levels.

Icon	Severity	Description
	100 –75	**Critical Event**: *Red exclamation point*. These are deliberate attacks on your system for the purpose of damaging data, extracting data, or crashing the system. Critical events always trigger protection measures.
	74 – 50	**Serious Event**: *Orange exclamation point*. These are deliberate attempts to access information on your system without directly damaging anything. Some serious events trigger protection measures.
	49 – 25	**Suspicious Event**: *Yellow question mark*. These are network activities that are not immediately threatening, but may indicate that someone is attempting to locate security vulnerabilities in your system. For example, hackers often scan the available ports or services on a system before attacking it. Suspicious events do not trigger protection measures. Not all suspicious events are indicative of a true attack. For example, many Internet Service Providers have scanning programs installed on their servers to check if a connection is still valid. This is a completely safe and legitimate scan from your ISP, but BlackICE still reports it as a suspicious event. After a few weeks of collected information you may notice recurring scans from one location. Note the intruder's IP address(es) and contact your ISP. It is likely that these scans are a standard part of your ISP's service and pose no threat to your system.
	24 – 0	**Informational Event**: *Green "i"*. These indicate that a network event occurred that is not threatening but worthy of taking note. Informational events do not trigger protection measures.

Response Level Icons

The following icons indicate the protection BlackICE provided against the attack. There are five response levels.

For more information about an attack, select the attack and click the Attacks tab **advICE** button.

Icon	Description
	**Attack Blocked**: BlackICE successfully blocked the attack. Depending on the severity of the attack, BlackICE also may have blocked the attacking system. To see if BlackICE is currently blocking the intruder, double-click on the attack. The application displays the Intruders tab. If BlackICE detected and blocked the intruder, then the Blocked State column within the Intruders tab displays the Attack Blocked icon.
	**Attack Unsuccessful**: Other defenses of your computer, such as the

operating system, successfully blocked the attack. Therefore, BlackICE did not need to block the event. The attack did not compromise your system.

Attack Status Unknown: BlackICE triggered protection measures as soon as it identified the attack, but some attacking packets may have made it through to your computer. It is unlikely that the attack compromised your system.

Attack Possible: Similar to the Attack Status Unknown response, BlackICE triggered protection measures as soon as it identified the attack. However, some attacking packets were able to get into your computer. The attack may have compromised your system.

Attack Successful: BlackICE detected abnormal traffic entering or exiting the system as a result of the attack. However, the protection measures of BlackICE could not block the attack. The attack has compromised the system.

Severity Icon Response Level Overlays

Response levels indicate the protection BlackICE provided against an attack. The BlackICE response levels are displayed as an overlay to the severity icon. For example, if BlackICE blocks an attack of *critical* severity, then a black diagonal line  is displayed over the *critical event* icon  to create the following image:  .

The five response levels can also be displayed as separate icons in their own Attacks tab column.

Icon	Description
	**Attack Blocked**: *Black line overlay*. BlackICE successfully blocked the attack. Depending on the severity of the event, BlackICE may also have blocked the attacking system. To see if BlackICE is currently blocking the intruder, double-click on the attack. The application displays the Intruders tab. If BlackICE detected and is presently blocking the intruder, then the Blocked State column within the Intruders tab displays the following icon:  .
	**Attack Unsuccessful**: G*ray line overlay*. Other defenses of your computer, such as the operating system, successfully blocked the attack. Therefore, BlackICE did not need to block the event. The attack did not compromise your system.
	**Attack Status Unknown**: *No overlay*. BlackICE triggered protection measures as soon as it identified the attack, but some attacking packets may have made it through to your computer. It is unlikely that the attack compromised your system.
	**Attack Possible**: *Orange Overlay*. Similar to the Attack Status Unknown response, BlackICE triggered protection measures as soon as it identified the attack. However, some attacking packets were able to get into your computer. The attack may have compromised your system.
	**Attack Successful**: *Red overlay.* BlackICE detected abnormal traffic entering or exiting the system as a result of the attack. However, the protection measures of BlackICE could not block the attack. The attack has compromised the system. For information about the attack, select the attack and click the Attacks tab **advICE** button.

Intruders Tab

The **Intruders** tab aggregates information about all the intruders who have provoked events on your system. This tab is designed to help you determine the severity and location of each intruder.

By default, the information in the Intruders tab is sorted first in alphabetic order by intruder and then in descending order of severity. Clicking a column header re-sorts the list by that column. Clicking the column header again toggles the sort order (ascending or descending). Alternatively, you can right-click on the column header to display a pop-up menu that allows you to sort the column in ascending or descending order For more information see the How to Configure Tab Columns topic.

When you select an intruder in the Intruders tab, all the information discovered about the intruder is displayed on the right side of the window (the Details display). The slider bar between the Intruder list and the Details display allows you to customize the size of the tab.

To display the activities of the intruder, double-click the entry on the screen. The attacks attributed to the selected intruder are displayed on the Attacks tab.

Intruders Tab Columns

The **Intruders** tab consists of several configurable columns that display intruder information. Adding, removing or reordering these columns can customize the look of the tab. By default, only three columns are displayed; the other tab columns are optional. To display different columns on the tab, right-click on a column header and select **Columns…**. For detailed instructions, please see the How to Configure Tab Columns topic.

See the Intruders tab component name below for more information about the different columns:

Severity Icon

This is a visual representation of the severity of the attack. Each entry is associated with one of four severity levels. The severity level reflects the most severe attack attributed to the Intruder.

Intruder

The best name BlackICE Defender can gather from the attacking system. This column displays the NetBIOS (WINS) name or DNS name for the attacking system. If BlackICE cannot determine a name, then it displays the intruder's IP address.

For details about a particular intruder, select the intruder on the list. A description of all the information discovered about the attacking system is displayed on the right side of the window (the Details window). For information about the intruder's attacks, double-click on the intruder. The attacks attributed to the selected intruder are displayed on the Attacks tab.

Blocked State Icon

If the Attack Blocked icon is displayed, then BlackICE is presently blocking all network traffic from that intruder. If there is no icon, then the intruder is not blocked.

To see the start and end time of the block; to check if the block is manual or automatic; or for information on how to unblock the intruder, please see the Blocked Addresses tab.

Severity (numeric)

A numeric representation of the highest severity rating attributed to the intruder.

Intruder IP

The IP address of the attacking system.

Other Intruders Tab Elements

Details

BlackICE displays all the back tracing information it has collected about the intruder next to the Intruder List. When BlackICE Defender back traces an intruder it attempts to gather the IP address, DNS name, NetBIOS (WINS) name, Node Name, Group name and MAC address. Savvy hackers

will likely block BlackICE from acquiring this information.

Back trace information is stored in standard text files in the Hosts folder in the directory where BlackICE is installed. Each file is prefixed with the intruder's IP address. For more information about back tracing, please see the Back Trace Tab.

Close

Closes the BlackICE Defender summary. The detection and protection engine remains active.

Help

Displays the online help for the Intruders tab.

Intruders Tab Right-Click Options

Right-click on a list item to Block an Intruder or to Trust an Intruder.

History Tab

The **History** tab displays the recent activity on your system. By use of graphs, the History tab illustrates your network's traffic and the detected attacks in relation to time. These graphs are a good way to check for trends in hacking or scanning. For example, if many hacks are grouped together in the late hours of the night, then there is a good chance that someone is trying to break into your system at that time.

To see details about the attacks plotted, single-click any point in either the **Attacks** or **Network Traffic** graphs. This takes you to the Attacks tab. The Attacks tab displays the attacks in descending time order and focuses your attention on the attack that comes closest in time to the selected point in the graph. In a situation where a peak is displayed in the Attacks graph, you can click on the peak and zero in on what attacks occurred during that time.

History Tab Features

See the History tab component name below for more information:

Interval

The Interval box displays the current interval unit in Minutes, Hours or Days. Use the option buttons to select the interval for both graphs.

Min displays the last 90 minutes of activity; ***Hour*** displays the last 90 hours of information, ***Day*** displays the last 90 days. BlackICE Defender automatically displays the most informative interval.

Total in 90...

This box displays summary statistics for the selected interval. Three statistics are displayed:

> ***Critical:*** The total number of detected events/attacks rated as *critical* for the selected interval. The events of this type are tracked on the Attacks graph with a red line.

> ***Suspicious:*** The total number of detected events/attacks rated as *serious and suspicious*. The events of this type are tracked on the Attacks graph with a yellow line.

> ***Traffic:*** The total amount of network traffic, measured in number of packets. Traffic is tracked on the Network Traffic graph with a green line.

In 90...

This box displays the highest amount of network traffic, measured in number of packets, for the selected interval (**High Traffic…**).

Attacks Graph

This graphically displays the critical and suspicious attacks over time. The critical attacks are tracked on the graph as a red line; the suspicious attacks are tracked as a yellow line. To see the total number of events for the selected interval, see the *Total In 90…* box.

Network Traffic Graph

This graphically displays the network traffic over time. Traffic is tracked on the Network Traffic graph with a green line. To see the total amount of network traffic, measured in number of packets, for the selected interval, see the *Total In 90…* box.

Close

Closes the BlackICE Defender summary application. The detection and protection engine remains active.

Help

Displays the online help for the History tab.

***I**nternet **R**elay **C**hat.* IRC was developed in the late 1980s as a way for multiple users on a system to "chat" over the network. Today IRC is a very popular way to "talk" in real time with other people on the Internet. However, IRC is also one avenue hackers use to get information from you about your system and your company. Moreover, IRC sessions are prone to numerous attacks that, while not dangerous, can cause your system to crash.

***N**etwork **B**asic **I**nput / **O**utput **S**ystem*. NetBIOS is an extension of the DOS BIOS that enables a PC to connect to and communicate with a LAN.

***I**nternet **P**rotocol* (IP) specifies the format of packets, also called *datagrams,* and the addressing scheme. Most networks combine IP with a higher-level protocol called Transport Control Protocol (TCP), which establishes a virtual connection between a destination and a source. IP by itself is something like the postal system. It allows you to address a package and drop it in the system, but there's no direct link between you and the recipient. TCP/IP, on the other hand, establishes a connection between two hosts so that they can send messages back and forth for a period of time. Current IP standards use 4 numbers between 0 and 255 separated by periods to create the 32-bit numeric IP address. For example, an IP address could be: 38.158.99.13.

***B**lue **S**creen **o**f **D**eath.* When a Windows NT based system encounters a serious error, the entire operating system halts and displays a screen with information regarding the error. The name *Blue Screen of Death* comes from the blue color of the error screen.

***P**acket **In**ternet **G**roper.* PING is a utility to determine whether a specific IP address is accessible. It works by sending a packet to the specified address and waiting for a reply. PING is used primarily to troubleshoot Internet connections.

***I**nternet **C**ontrol **M**essage **P**rotocol*. ICMP, an extension to the Internet Protocol (IP), supports packets containing error, control, and informational messages. The PING command, for example, uses ICMP to test an Internet connection.

***T**ransmission **C**ontrol **P**rotocol*. TCP is one of the main protocols in TCP/IP networks. Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

***S**erver **M**essage **B**lock.* SMB is a message format used by DOS and Windows to share files, directories and devices. NetBIOS is based on the SMB format, and many network products use SMB. These SMB-based networks include LAN Manager, Windows for Workgroups, Windows NT, and LAN Server. There are also a number of products that use SMB to enable file sharing among different operating system platforms. A product called *Samba,* for example, enables UNIX and Windows machines to share directories and files.

***D**istributed **C**omputing **E**nvironment.* DCE is a suite of technology services developed by The Open Group for creating distributed applications that run on different platforms. DCE services include: Remote Procedure Calls (RPC), Security Service, Time Service, Threads Service, and Distributed File Service. DCE is a popular choice for very large systems that require robust security and fault tolerance.

***S**imple **N**etwork **M**anagement **P**rotocol.* SNMP is a set of protocols for managing complex networks. The first versions of SNMP were developed in the early 80s. SNMP works by sending messages, called *protocol data units (PDUs)*, to different parts of a network. SNMP-compliant devices, called *agents,* store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

SNMP 1 reports only whether a device is functioning properly. The industry has attempted to define a new set of protocols called *SNMP 2* that would provide additional information, but the standardization efforts have not been successful. Instead, network managers have turned to a related technology called RMON that provides more detailed information about network usage.

***C**ommon **G**ateway **I**nterface*. CGI is a specification for transferring information between a World Wide Web server and a CGI program. A CGI program is any program designed to accept and return data that conforms to the CGI specification. The program could be written in any programming language, including C, Perl, Java, or Visual Basic.

CGI programs are the most common way for Web servers to interact dynamically with users. Many HTML pages that contain forms, for example, use a CGI program to process the form's data once it's submitted. The use of CGI is what is called a *server-side* solution, because the processing occurs on the Web server.

***A**pplication **P**rogram **I**nterface*. API is a set of routines, protocols, and tools for building software applications. A good API makes it easier to develop a program by providing all the building blocks. A programmer puts the blocks together.

Most operating environments, such as MS-Windows, provide an API so that programmers can write applications consistent with the operating environment. Although APIs are designed for programmers, they are ultimately good for users because they guarantee that all programs using a common API will have similar interfaces. This makes it easier for users to learn new programs.

***R**emote **P**rocedure **C**all.* RPC is a type of protocol that allows a program on one computer to execute a program on a server computer. Using RPC, a system developer need not develop specific procedures for the server. The client program sends a message to the server with appropriate arguments and the server returns a message containing the results of the program executed.

Finger: A UNIX program that takes an e-mail address as input and returns information about the user who owns that e-mail address. On some systems, finger only reports whether the user is currently logged on. Other systems return additional information, such as the user's full name, address, and telephone number. Of course, the user must first enter this information into the system. Many e-mail programs now have a finger utility built into them.

***S**imple **M**ail **T**ransfer **P**rotocol.* SMTP is a protocol for sending e-mail messages between servers. Most e-mail systems that send mail over the Internet use SMTP to send messages from one server to another; the messages can then be retrieved with an e-mail client. In addition, SMTP is generally used to send messages from a mail client to a mail server.

A *Shell* is the command processor interface. The command processor is the program that executes operating system commands. The shell, therefore, is the part of the command processor that accepts commands. After verifying that the commands are valid, the shell sends them to another part of the command processor to be executed.

A *Cookie* is a string of characters saved by a web browser on the user's hard disk. Many web pages send cookies to track specific user information. Cookies can be used to retain information as the user browses a web site. For example, cookies are used to 'remember' the items a shopper may have in a shopping cart.

***D**omain **N**ame **S**ystem*. DNS is a database of domain names and their IP addresses. DNS is the primary naming system for many distributed networks, including the Internet.

A *firewall* is a hardware or software barrier that restricts access in and out of a network. Firewalls are most often used to separate an internal LAN or WAN from the Internet. A gateway can serve as a firewall between two or more networks.

***F**ile **T**ransfer **P**rotocol*. FTP is a common protocol for exchanging files between two sites across a network. FTP is popular on the Internet because it allows for speedy transfer of large files between two systems. Like all networking protocols, it too has some significant vulnerabilities.

***M**edia **A**ccess **C**ontrol **Address**.* A unique identification code used in all networked devices. The MAC address defines a specific network node at the hardware level and cannot be altered by any software.

Protocol: A “language” for communicating on a network. Protocols are sets of standards or rules used to define, format, and transmit data across a network. There are many different protocols used on networks. For example, most web pages are transmitted using the HTTP protocol.

A *router* is a device that connects two networks together. Routers monitor, direct, and filter information that passes between these networks. Because of their location, routers are a good place to install traffic or mail filters. Routers are also prone to attacks because they contain a great deal of information about a network.

SATAN is a UNIX program that gathers information on networks and stores it in databases. It is helpful in finding security flaws such as incorrect settings, software bugs and poor policy decisions. It shows network services that are running, the different types of hardware and software on the network, and other information. It was written to help users find security flaws in their network systems.

SPAM is unwanted e-mail, usually in the form of advertisements.

Spoofing: To *spoof* is to forge something, such as an IP address. IP spoofing is a common way for hackers to hide their location and identity.

Telnet is a program that connects a computer to a server on a network. It allows a user to control some server functions and to communicate with other servers on the network. Telnet sessions generally require a valid username and password. Hackers commonly use Telnet to hack into corporate network systems.

***T**ransmission **C**ontrol **P**rotocol.* TCP is one of the main protocols in TCP/IP networks. Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

Trojan Horse: Like the fabled gift to the residents of Troy, a *Trojan Horse* is an application designed to look innocuous. Yet, when you run the program it installs a virus or memory resident application that can steal passwords, corrupt data, or provide hackers a back door into your computer. Trojan applications are particularly dangerous since they can often run exactly as expected without showing any visible signs of intrusion.

User **D**atagram **P**rotocol. UDP is a connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive datagrams (packets) over an IP network. UDP is used primarily for broadcasting messages over a network.

BackOrifice: BackOrifice is a remote administration tool that allows a user to control a computer across a TCP/IP connection using a simple console or GUI application. BackOrifice is a potentially disastrous Trojan horse since it can provide the user unlimited access to a system.

A *worm* is a program that seeks access into other computers. Once a worm penetrates another computer it continues seeking access to other areas. Worms are often equipped with dictionary-based password crackers and other cracker tools that enable them to penetrate more systems. Worms often steal or vandalize computer data.

Whois is an Internet utility that returns information about a domain name or IP address. For example, if you enter a domain name such as *microsoft.com,* whois will return the name and address of the domain's owner (in this case, Microsoft Corporation).

Back Trace Tab

When BlackICE Defender's monitoring engine detects a suspicious event, it immediately starts collecting information. One method BlackICE uses to locate an intruder is a networking procedure called *back tracing*.

Back tracing is the process of tracing a network connection back to its origin. When somebody connects to your computer via a network such as the Internet, your system and the intruder's system exchange packets. Before an intruder's packets reach your system, they travel through several routers. BlackICE can strip information off these packets and determine each router the intruder's packets had to travel or "hop" through. Eventually, BlackICE Defender can "hop" all the way back to the intruder's system.

There are two ways that BlackICE can back trace information: *directly* or *indirectly*.

An *indirect trace* uses protocols that do not make contact with the intruder's system, but collect information indirectly from other sources along the path to the intruder's system. On the other hand, a *direct trace* goes all the way back to the intruder's system to collect information. Direct traces generally gather more reliable information than indirect traces.

Hackers cannot detect any indirect tracing. However, direct traces can be detected and blocked by the hacker. Fortunately, most hackers are not experienced enough to block direct traces.

The Back Trace tab allows you to view and modify the configuration parameters that control the back tracing functions of BlackICE Defender.

Indirect Trace Parameters

The Indirect Trace parameters establish how BlackICE Defender executes indirect back tracing. Because indirect back tracing does not make contact with the intruder's system it does not acquire much information. Therefore, it is best for lower severity attacks.

Threshold

Indicates the attack severity level that triggers an indirect trace of the attack. Severity refers to the numeric level of each attack. The default attack severity for the indirect trace threshold is 30. For example, if an event of attack severity 50 is detected, then BlackICE triggers an indirect trace of the attack; but if the event has an attack severity less then 30, then BlackICE does not trigger a back trace.

DNS LookUp

When checked, BlackICE queries available DNS (Domain Name Service) servers for information about the intruder. The DNS Lookup is enabled by default.

Direct Trace Parameters

The Direct Trace parameters establish how BlackICE Defender executes direct back tracing. Because direct back tracing makes contact with the intruder's system it acquires a great deal of information. Therefore, it is best used for high severity attacks.

Threshold

Indicates the attack severity level that triggers a direct trace of the intruder. The default attack severity for the direct trace threshold is 60. In this case, if an event of attack severity 50 is detected, then BlackICE does not trigger a direct trace of the attack; but if the event has an attack severity greater than 60, then BlackICE does trigger a direct back trace.

NetBIOS NodeStatus

When checked, BlackICE performs a NetBIOS lookup on the intruder's system. The NetBIOS Node Status is enabled by default.

OK

When you have finished configuring BlackICE, click **OK** to implement all the changes in the

configuration tabs. The configuration dialog box is closed and you return to the previous screen.

Cancel

To close the configuration dialog box without implementing the changes entered, click **Cancel**. The configuration dialog box is closed and you return to the previous screen.

Apply

To implement the changes entered into the configuration tabs without closing the configuration dialog box, click **Apply**.

Help

For help on the opened configuration tab, click **Help**.

Back Trace Threshold Parameters

The Back Trace Threshold establishes the severity level (numeric severity) at which BlackICE initiates a back trace. Severity refers to the level of each attack. The following list summarizes how BlackICE Defender categorizes severities.

Icon	Severity	Description
	100-80	**Critical Event**: This is a deliberate attack on your system for the purpose of damaging data, extracting data, or crashing the system. Critical events always trigger protection measures.
	80-40	**Serious Event**: This is a deliberate attempt to access information on your system, yet it does not directly damage anything. Some serious events trigger protection measures.
	40-20	**Suspicious Event**: This is network activity that is not immediately threatening but may indicate that someone is attempting to locate security vulnerabilities in your system. For example, hackers often scan the available ports or services on a system before attacking it. Suspicious events do not trigger protection measures, and not all suspicious events are indicative of a true attack.
	20-0	**Informational Event**: This indicates that a network event occurred to your computer that is not threatening. Informational events do not trigger protection measures.

Packet Log Tab

The Packet Log tab allows you to configure the packet logging features of BlackICE Defender.

When packet logging is enabled, BlackICE Defender records the system traffic into log files. Files are filled until a maximum size is reached. Then a new file is generated until the maximum number of files are used. Then BlackICE Defender starts over, replacing the first log file with a new file.

It is important to note that packet logging keeps track of ALL system traffic, not just intrusions. Therefore, packet logs can become very large and consume a great deal of hard disk space. However, if you are having repeated intrusions on a system, packet logging can help gather additional information about activity on the system.

Packet logs are encoded as “sniffer” style trace files. You will need a decoding application such as Network Monitor, which is included with Windows NT Server, to view the contents of these files. The file extension for all packet log files is **`*.enc`**.

BlackICE Defender also captures network traffic that is specifically related to an intrusion in Evidence Files.

Logging Enabled

When selected, BlackICE captures packet logs. Packet logging is disabled by default.

File Prefix

Specifies the prefix for the packet log file names. BlackICE Defender automatically places an incremented counter in the filename. For example, if you enter `ABC` the file names will be `ABC0001.enc`, `ABC0002.enc`, etc. The default file prefix is `log`.

Maximum Size (kbytes)

Specifies the maximum size, in kilobytes, for each log file. The default value is 0 kilobytes. To ensure that the file fits on a floppy disk, consider using a maximum size of 1400 kilobytes.

Maximum Number of Files

Specifies the maximum number of log files to generate. The default value for the maximum number of files to log is 10.

OK

When you have finished configuring BlackICE, click **OK** to implement all the changes in the configuration tabs. The configuration dialog box is closed and you return to the previous screen.

Cancel

To close the configuration dialog box without implementing the changes entered, click **Cancel**. The configuration dialog box is closed and you return to the previous screen.

Apply

To implement the changes entered into the configuration tabs without closing the configuration dialog box, click **Apply**.

Help

For help on the opened configuration tab, click **Help**.

Evidence Log Tab

BlackICE Defender captures evidence files anytime your system is attacked. These files are located in the ***<installation directory>*** folder. For example, if you installed BlackICE to the Program Files directory on the C: drive (the default), then the evidence files are located in **C:/Program Files/Network ICE/BlackICE**. The file extension for all evidence log files is ***.enc**.

Evidence files are encoded as "sniffer" style trace files. To view the contents of these files, you need to have a decoding application, such as Network Monitor (included with the Windows NT Server).

The Evidence Log tab controls the size and grouping of each evidence file set. For more information, please see the Help section on Evidence Files.

NOTE: Evidence files are not the same as packet logs. Packet logs are a summary of ALL inbound and outbound traffic on the system. An evidence file zeros in on the traffic associated with specific attacks.

Logging Enabled

When selected, BlackICE Defender collects evidence files for suspicious events. Evidence logging is enabled by default.

File Prefix

Specifies the prefix for the evidence file names. Enter **%d** after the selected prefix to place a date stamp (format YYYYMMDD) and number (NN) in the file name. For example, if you enter evd%d (the default file prefix), then the file names will look like this: evdYYYYMMDD-NN.enc. The time is in 24-hour format in Greenwich Mean Time (GMT).

Maximum Size (kbytes)

Controls how big each evidence file can get. It is best to keep this value under 2048 kilobytes (2 MB). The default is 1400 kilobytes.

Maximum Number of Files

Limits how many files BlackICE will generate in the specified collection time period (as defined by the Maximum Number of Secs value). For example, if the Maximum Number of Secs is 86400 seconds (24 hours) and the Maximum Number of Files is 32 (the default value), then BlackICE will not generate more than 32 evidence files in any given 24 hour period.

Maximum Number of Secs

Sets a time period for evidence file collection. This value (in seconds) is used to limit how many files BlackICE generates in the given period. For example, if this value is set to 86400 seconds (the default), the Maximum Number of Files is set to 32, and the Maximum Size is set to 1024, then BlackICE is limited to capturing 32, 1MB evidence files every 24 hours.

OK

When you have finished configuring BlackICE, click **OK** to implement all the changes in the configuration tabs. The configuration dialog box is closed and you return to the previous screen.

Cancel

To close the configuration dialog box without implementing the changes entered, click **Cancel**. The configuration dialog box is closed and you return to the previous screen.

Apply

To implement the changes entered into the configuration tabs without closing the configuration dialog box, click **Apply**.

Help

For help on the opened configuration tab, click **Help**.

Protection Tab

The Protection tab establishes the Security Level BlackICE Defender should enforce on the system. There are four pre-set security levels, as defined below. For more information about how security levels work, please see the Security Levels topic. For instructions on how to configure the protection tab, see To Set the Security Level below.

Paranoid: The *Paranoid* setting is very restrictive, but useful if your system is enduring frequent and repeated attacks. Under this setting BlackICE Defender blocks all unsolicited inbound traffic. This setting may restrict some web browsing and interactive content.

Nervous: This setting is preferable if you are experiencing frequent intrusions. For the *Nervous* setting, BlackICE Defender blocks all unsolicited inbound traffic except for some interactive content on web sites (such as streaming media and other "application specific" Internet usage).

Cautious: The *Cautious* setting is good for regular use of the Internet. This setting only blocks unsolicited network traffic that accesses operating system and networking services. This is the default security level setting for BlackICE Defender.

Trusting: When set to *Trusting*, all ports remain open and unblocked, and therefore this setting allows all inbound traffic. This setting is good if there is minimal threat of intrusions.

Please see the following table for examples on how the different security levels respond to some applications.

Security Level	Examples of Some Applications		
	Blocked	Configurable*	Not Blocked
Paranoid	IRC file transfer (DCC), NetMeeting, PC Anywhere, ICQ	Quake (II, III), Internet Phone, Net2Phone	FTP File transfers, Sending/receiving email, Real Audio, IRC Chat
Nervous	IRC file transfer (DCC), NetMeeting	ICQ, Internet Phone, Net2Phone	All of the above plus: PC Anywhere, Quake (II, III)
Cautious	This setting only blocks unsolicited network traffic that accesses operating system and networking services.		All of the above plus: IRC file transfer (DCC), NetMeeting
Trusting	No applications are blocked.		This setting allows all inbound traffic.

Allow Internet File Sharing: Internet file sharing allows you to share files with others across the Internet. For example, you can transfer files from home to your work computer. With Internet file sharing enabled, you can connect to your computer over the Internet and upload or download files. However, Internet file sharing makes your computer very vulnerable to simple intrusions.

To prevent systems from connecting to your computer and accessing your shares over the Internet, keep this check box clear. Blocking Internet file sharing ensures that hackers cannot download files off your computer. See the Windows Sharing Features topic for more information.

Allow NetBIOS Neighborhood: Select this check box to report your system (NetBIOS) name to the Windows Network Neighborhood. Clear the check box to hide your system name from this feature. If you have a network at home that uses NetBIOS names to access file shares, then you need to keep this option enabled. Otherwise, you have to use IP addresses to access the file shares. By default, this check box is clear.

NOTE: If you enable the Internet file sharing but not the NetBIOS Neighborhood, you must use an IP address to remotely access your system.

OK

When you have finished configuring BlackICE, click **OK** to implement all the changes in the configuration tabs. The configuration dialog box is closed and you return to the previous screen.

Cancel

To close the configuration dialog box without implementing the changes entered, click **Cancel**. The configuration dialog box is closed and you return to the previous screen.

Apply

To implement the changes entered into the configuration tabs without closing the configuration dialog box, click **Apply**.

Help

For help on the opened configuration tab, click **Help**.

To Set the Security Level

1. In the Protection tab, select the **Security Level** you wish to use. The default Security Level is **Cautious**.
2. If you wish to enable (unblock) file sharing over the Internet, select the **Allow Internet File Sharing** check box. By default, Internet file sharing is not selected.
3. Check **Allow NetBIOS Neighborhood** if you want your system to appear in the Network Neighborhood window. Clear this check box to hide your system from browsing.
4. Click **Apply** to begin using the new security level.

WARNING: Enabling Internet file sharing makes your computer very vulnerable to simple intrusions. However, if you want to transfer files from home to your work computer, this option must be enabled. Network ICE does not recommend leaving Internet file sharing enabled for extended periods of time.

Trusted Addresses Tab

The Trusted Addresses tab allows you to identify network addresses to exclude from all BlackICE monitoring and protection. When an address is trusted, BlackICE Defender considers all network traffic from that address to be safe.

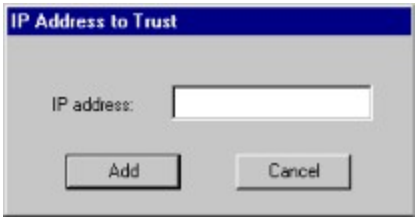
NOTE: Be very careful which systems you tell BlackICE Defender to trust. A trusted system is completely free from any monitoring or protection. This should only be used for trusted network management servers, ISP servers, or other devices that may inadvertently trigger BlackICE events. Please see How to Trust an Intruder for more information.

IP addresses of trusted systems

Lists all the trusted systems' IP addresses. The default setting has no entries.

Add

Click **Add** to place a new trusted address in the list. The IP Address to Trust dialog box is displayed. Enter the IP address of the system you wish to exclude from all BlackICE monitoring and protection (the trusted system) and click **Add** or [ENTER]. The new trusted address is added to the list.



IP Address to Trust dialog box

Delete

Use this button to *untrust* an IP address. Select the address in the list that you no longer want to trust and click **Delete**. The address is immediately deleted from the trusted addresses list. BlackICE Defender can now again monitor and protect you from that system. This action cannot be reversed.

To change or edit an address, delete the existing record and add a new one.

OK

When you have finished configuring BlackICE, click **OK** to implement all the changes in the configuration tabs. The configuration dialog box is closed and you return to the previous screen.

Cancel

To close the configuration dialog box without implementing the changes entered, click **Cancel**. The configuration dialog box is closed and you return to the previous screen.

Apply

To implement the changes entered into the configuration tabs without closing the configuration dialog box, click **Apply**.

Help

For help on the opened configuration tab, click **Help**.

Blocked Addresses Tab

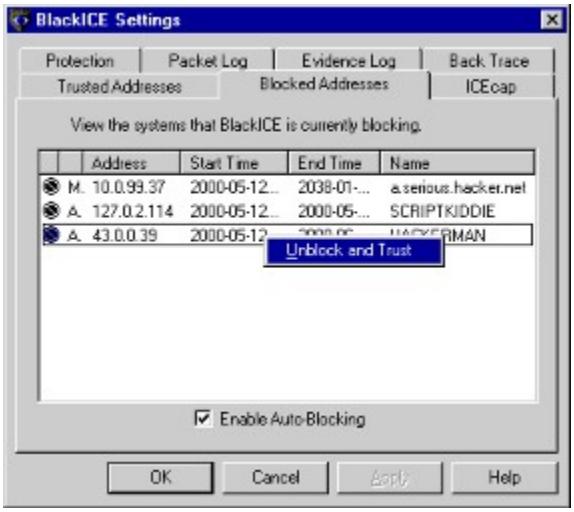
The Blocked Addresses tab shows you the addresses that BlackICE Defender is blocking. BlackICE rejects all network traffic from these blocked IP addresses.

Whether automatically blocked by BlackICE Defender, or manually blocked by the user, these blocked systems all have a specific end time. The end time is the expiration date of the block, and can range from a few minutes to several years. For more information about blocking intruders, please see How to Block an Intruder.

A blocked address can be converted into a trusted address if necessary. This option is handy if BlackICE Defender inadvertently blocks a system that is legitimately using your computer. However, you should only trust addresses that are from known systems. Advanced hackers can masquerade as a trusted address to crack into your system, so use this feature carefully.

To convert a blocked address, right-click on the address entry and select **Unblock and Trust** from the pop-up menu. The selected address is immediately removed from the Blocked Addresses tab, and trusted. Note that once **Unblock and Trust** is selected, this action cannot be reversed. If you only wish to unblock an address and not trust it, you can delete the trusted address from the Trusted Addresses tab.

Clicking a column header sorts the block list by that column. Click again to toggle between ascending and descending sort orders.



Blocked State Icon

The Attack Blocked icon indicates that BlackICE is presently blocking all network traffic from the intruder.

Block Type

How the address was blocked. If **Auto** is displayed, then BlackICE Defender automatically blocked the intruder. If **Manual** is displayed, then the user blocked the intruder manually.

Address

The IP address of the blocked system. The default setting has no entries.

Start Time

The date and time the address was first blocked. The format is: `YYYY-MM-DD hh:mm:ss`. The time is in 24-hour format for the time zone applicable to your system.

End Time

The date and time the address block will expire. The format is: `YYYY-MM-DD hh:mm:ss`. The time is in 24-hour format for the time zone applicable to your system.

Name

The best name BlackICE discovered for the blocked system. This may be a DNS or NetBIOS (WINS) name. If BlackICE Defender cannot determine the name of the system, then the IP address of the intruder is displayed.

Enable Auto-Blocking

When selected, BlackICE Defender automatically blocks hackers when they attempt to break into your system. To stop auto-blocking, clear this check box. Attacks will then still be reported and logged, but not automatically blocked.

If Auto-Blocking is not selected, then you must manually block intruders to protect your system. See How to Block an Intruder for more information.

OK

When you have finished configuring BlackICE, click **OK** to implement all the changes in the configuration tabs. The configuration dialog box is closed and you return to the previous screen.

Cancel

To close the configuration dialog box without implementing the changes entered, click **Cancel**. The configuration dialog box is closed and you return to the previous screen.

Apply

To implement the changes entered into the configuration tabs without closing the configuration dialog box, click **Apply**.

Help

For help on the opened configuration tab, click **Help**.

ICEcap Tab

NOTE: Because BlackICE Defender does not integrate with ICEcap, the ICEcap tab features are unavailable (dimmed).

ICEcap is a server-based Network ICE product that aggregates and compiles information from multiple BlackICE Agent and Sentry installations on a network. ICEcap is intended for use on internal networks (or LANs) where more than one system is connected to the Internet.

ICEcap affords a strategic view of the network. For example, one of the most common ways for a hacker to find holes in a network is to systematically sweep through all the TCP ports open on each system. To an individual system, this is not considered a serious attack. But, because the ICEcap server has a "network wide" view of the intrusions and issues, it can help identify "strategic" attacks and trends.

ICEcap works as a single information source. You can log-on to the server using a standard web browser and in minutes see all the attacks on all the systems on the network. This information can be displayed for many different intervals, allowing you to spot trends. ICEcap can also initiate down-stream protection on any BlackICE Agent installation.

The ICEcap tab is used to establish the parameters for BlackICE Agent and Sentry to report events to the ICEcap server. BlackICE Defender does not integrate with an ICEcap server. For more information about how BlackICE Agent and ICEcap can help manage a network, download a copy of the ICEcap documentation from Network ICE at www.networkice.com.

OK

When you have finished configuring BlackICE, click **OK** to implement all the changes in the configuration tabs. The configuration dialog box is closed and you return to the previous screen.

Cancel

To close the configuration dialog box without implementing the changes entered, click **Cancel**. The configuration dialog box is closed and you return to the previous screen.

Apply

To implement the changes entered into the configuration tabs without closing the configuration dialog box, click **Apply**.

Help

For help on the opened configuration tab, click **Help**.

Product Documentation

The latest product documentation is available from the Network ICE web site at www.networkice.com/Support.

Technical Support

Web:	www.networkice.com/Support
E-mail:	support@networkice.com

For updates and upgrade information, please visit the Network ICE web site. For information on how to download the latest update of BlackICE Defender from the summary application, please see the How to Update BlackICE topic.