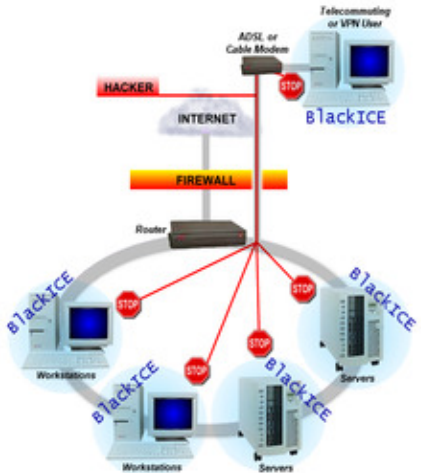
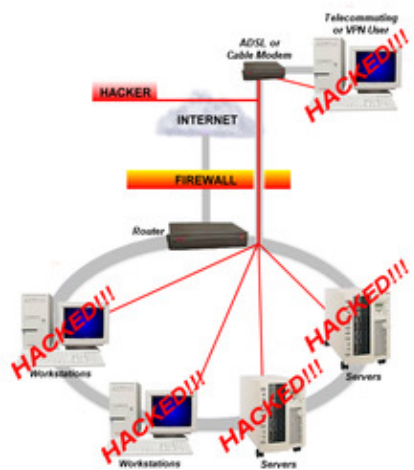


\$#K BlackICE Help Index

<p> Introducti^Kon Overview? Basic Hacking How BlackICE Works Security Levels Good Security Practices What Are Evidence Files? </p>	<p> Menus Control Menu Help Menu Taskbar Menu Application Tabs Attacks Tab Intruders Tab History Tab </p>
<p> How To ... Use BlackICE Run BlackICE Disable BlackICE Configure BlackICE Handle Intrusions Block an Intruder Trust an Intruder Ignore an Attack Clear out the Attack^K List Install BlackICE Uninstall BlackICE </p>	<p> Configuration Tabs Back Trace Tab Packet Log Tab Evidence Log Tab Protection Tab Trusted Addresses Tab Blocked AddressesTab ICEcap Tab </p>
<p> \$# An <i>Intruder</i> is a person who breaks into computers to steal, damage or vandalize data. </p>	
<p> \$# Overview In the past, it was relatively easy to stop hackers since most systems had few if any connections to other computers or networks. Older networks were simpler and thus easier to protect. Even as networking became common in the 1980s, systems were not connected to public networks, such as the Internet. Thus there were few hackers and few security incidents. However with the rise of the Internet and ubiquity of corporate computer networks in the 1990s, hackers have more opportunity than ever to break into systems. Additionally, with many people using the internet for their daily financial and consumer activities, there is more sensitive information available. Until now, most intrusion detection and protection was handled by expensive networking devices such as routers and firewalls. For corporations with simple, single Internet connections a firewall could handle external threats pretty well. However, few firewalls can stop internal hackers. As corporations implemented firewalls and other Internet protection measures, hackers had to find ways around these systems. The new targets for hackers are systems and connections few IT managers even perceive as threats. One of the most common ways to get into a network these days is to hijack a telecommuter's connection. Once inside the corporate firewall, a hacker can freely exploit internal servers and workstations. </p>	

BlackICE distributes powerful intrusion detection and protection throughout your network. The BlackICE agent is small enough to run on all your workstations and servers, yet robust enough to identify and stop over 200 different hacks. When you deploy BlackICE to your corporate network, you're erecting an enterprise-wide web that can identify and stop hackers before they break into any system. Furthermore, if you are using an ICEcap reporting and management console, you can deploy and manage all your BlackICE agents from a single console.



Without BlackICE

With BlackICE.

The figure on the left illustrates a common network. Hackers can exploit VPN and telecommuter connections to break into the network and bypass the firewall. Once inside, the hacker can break into any system including the telecommuter's home computer. The figure on the right demonstrates how BlackICE can protect the entire network. With BlackICE running on all the workstations and the telecommuter's computer, each computer has its own protection shield. The hacker still may be able to break through the firewall, but once inside there is nothing to steal. Each computer can block the intruder independently.

\$#

Security Levels

When BlackICE detects an attack, it automatically blocks access from the hacker's system. However, not all suspicious network traffic is an attack. What constitutes an attack vs. legitimate use of the network or 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 on-line 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 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 email to your computer.

Communication ports are divided into two categories: *System* and *Application*. The System Ports, or low-end

ports, are used for services installed on a computer, such as e-mail or web browsing. The Application ports, or high-end ports, are used by client applications such as chat programs or the 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.

There are two categories of ports for Internet connections: TCP and UDP. TCP connections are the most common. They are used for web browsing, downloading files, etc. UDP ports are essentially the same as TCP. However, UDP connections do not have the error correction features that TCP has. UDP is used for streaming content like RealAudio.

BlackICE has four Security Levels that define how rigorously it blocks unsolicited traffic for ports and port type. Inbound traffic is blocked on the security level you select. 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.

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

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

* File Sharing is blocked, unless specifically turned on. For more information about Internet file sharing, see the **Protection Tab** topic.

NOTE: Blocking Internet File Sharing prohibits anyone on your internal network from accessing shared resources on a system such as shared printers, folders, or drives.

For a description of each Security Level, please see the **Security Level Descriptions** topic.

\$# Security Level Descriptions

Trusting: When set to *Trusting*, BlackICE only blocks file sharing over the Internet, unless it is specifically enabled on the Protection tab (See the **Protection Tab** topic for more information.) Blocking file sharing ensures that hackers cannot download files off your computer. All other ports remain open and unblocked. Even though Internet file sharing is disabled, file sharing on an internal network remains unaffected. This setting is good to use if you have a slower Internet connection and little threat of attack.

Cautious: The *Cautious* setting is best for regular use of the Internet. This setting only blocks inbound intrusions on System Port(s). All other ports remain unblocked and therefore should not interfere with any Internet usage.

Nervous: The *Nervous* setting is good if you are experiencing repeated intrusions. For this setting, BlackICE blocks inbound intrusions on all the System ports and **TCP** Application ports. This setting may restrict some interactive content on web sites. Streaming media and other application specific Internet usage remains unaffected.

Paranoid: The *Paranoid* setting is very restrictive, but useful if your system has endured numerous attacks. Under this setting BlackICE blocks all inbound intrusions. This setting may restrict some web browsing and interactive content.

For more information about setting security levels, see the **Protection Tab** topic.

\$# Basic Hacking

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

Corporations have long known about the risks hackers present to their business. However, most home office and casual computer and Internet users are unaware 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. Because of the poor reporting and centralized planning related to computer crime, the actual damage attributable to hackers is very difficult to determine.

However, 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 foreign 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.

Of recent concern is *cyberterrorism*. What terrorists cannot accomplish with propaganda or cruise missiles, they sometimes can with computers. Many rogue states are or suspected to be engaged in terrorist activities designed specifically to disrupt or destroy the ability of a country and its corporations to function.

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 your corporation. It can be as simple as a curious employee or a serious attempt to hurt the 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 include people trying to break into your systems from outside your company. These types of attacks are less common but almost always malicious in nature. BlackICE 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 you should consider the following good security practices:

> **Establish a good security plan.** A good network takes into account what hackers can do and prepares for attacks. The best defense against hackers and crackers is information. Encourage your company or organization to develop a comprehensive security plan if you do not already have one.

- > **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 email.** Never e-mail sensitive information such as passwords, credit card information, etc. to people without encrypting the information first.
- > **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 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 IP address or other system networking information to people outside your company.
- > **Be careful of files e-mailed to you from people you do not know.** One common way of getting BackOrifice on a system is to include it as a Trojan horse with other files.
- > **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.
- > **Chat rooms.** If you use chat rooms or IRC sessions, be careful with any information you reveal to strangers.
- > **Foreign sites.** Use caution when accessing e-mail or web sites that originate in foreign countries, especially Russia and the former Soviet states. Russia has a very active hacker subculture. Furthermore, many domestic hackers use off-shore accounts and connections to hack because it is more difficult to backtrace these accounts.
- > **Pay attention to odd computer behavior.** If your system starts exhibiting odd behavior, contact your ISP. Some hackers will set off attacks that cause your system to slowly 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 and contact your ISP immediately. 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. Some hackers dig through the trash of companies or individuals for information that might help them in a social intrusion.
- > **Install ICEcap.** Network ICE's ICEcap is a powerful reporting and management console that centralizes, aggregates, and manages BlackICE agents on your network. Using ICEcap you can remotely distribute BlackICE agents as well as issue network-wide protection measures to all those agents. Furthermore, ICEcap aggregates intrusion information from all BlackICE agents. This can help you spot trends and stop hackers who are carefully probing your network for a security breach. For more information about ICEcap, visit the Network ICE web site at www.networkice.com.
- > **Install ICEscan.** Network ICE's ICEscan remotely analyzes network devices and resources for common security breaches. When used in conjunction with an ICEcap server, system administrators can spot many security problems before hackers exploit them. For more information about ICEscan, visit the Network ICE web site at www.networkice.com.

\$# How BlackICE Works

BlackICE consists of an extremely powerful detection and analysis engine that monitors all network ports and protocols for suspicious traffic. When a possible attack is detected, BlackICE springs into action logging information about the event. Information about the

attacker is displayed in the **Intruders tab**. Information about the type of attack the intruder attempted is displayed in the **Attacks tab**.

The information BlackICE collects regarding an attack is analyzed using sophisticated networking algorithms. If the attack is determined to be an intrusion, BlackICE automatically blocks any access from the hacker's machine (**IP address**). No matter how hard the hacker tries to crack your system, he cannot get around BlackICE. BlackICE blocks the hacker's access at the network transport. In other words, any transmission the hacker sends to your computer is rejected before it ever gets inside the computer. When BlackICE reports an attack it not only logs the type of attack, but who initiated the attack. BlackICE backtraces hackers when they try to break into your computer. Backtracing allows you to know exactly who is attacking you. In extreme cases, you could use this information if you need to pursue legal action against a hacker.

BlackICE also captures a complete record of the attack in Evidence files. These files contain all the data the hacker sent to your computer. In the hands of an experienced network engineer or Internet Service Provider, evidence files show exactly what the hacker attempted. See the **Evidence Files** topic for more information. Additionally, the **History tab** displays attacks and network traffic in colorful line graphs. This can help spot trends and patterns in the activities of hackers.

If you are using BlackICE on your company LAN, you can also configure BlackICE to report events to an ICEcap server. ICEcap is a powerful reporting and management console for corporate networks. ICEcap can aggregate information from multiple computers running BlackICE. This helps identify more attacks and monitor intrusion information on an enterprise-wide level. ICEcap can also issue enterprise wide protection measures to all BlackICE agents.

For proactive security assessment and monitoring, Network ICE's ICEscan can regularly scan your network for security problems. This information is also reported to the ICEcap server for analysis and review.

For more information about ICEscan and ICEcap, visit the Network ICE web site at www.networkice.com.

\$#BlackICE Detect. Intended for home and small-office use, BlackICE Detect can quickly detect and alert you to attacks on your system.

\$#BlackICE Defender. BlackICE Defender features the same powerful detection abilities as BlackICE Detect, however BlackICE Defender protects against intrusions. When attacks are detected, BlackICE Defender automatically blocks the attacker from gaining access to your system.

\$#BlackICE Pro. Intended for workstations on corporate networks, BlackICE Pro 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.

\$#BlackICE Auditor. The Auditor series is designed for professional security consultants to perform short term (120 days or less) security audits on a network enterprise. BlackICE Auditor is functionally identical to BlackICE Pro, except with a limited usage license.

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

\$# What Are Evidence Files?

Evidence files are part of BlackICE's intrusion monitoring features. As a hacker is attempting to break into your system, BlackICE can capture all network traffic attributed to the hacker and place that information into an *evidence file*.

BlackICE evidence files are located in the `<installation directory>/Network ICE/BlackICE` 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.

How many evidence files BlackICE captures, the filename prefix, and the size of each evidence file is established in the BlackICE configuration. See the [Evidence Log Tab](#) for more information.


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

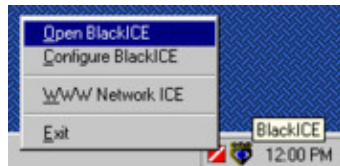
For more information about installing the Network Monitoring service or using the decoding tool, refer to the documentation included with your copy of Windows NT Server 4.0.

\$# How To Run BlackICE

BlackICE consists of two main components: an invisible intrusion detection and protection engine and a summary application (the user interface which displays attacks, intruders, etc.) When BlackICE is installed in your computer the detection and protection engine is always running. To see what intrusions the engine has detected and/or stopped, you must open the summary application.

If the BlackICE summary application has already been started, a small icon  is displayed in the task-bar.

1. Right click on the icon. A sub-menu of choices is displayed.
2. Select **Open BlackICE**.
3. You can also use this submenu to access the Network ICE web site, to [configure BlackICE](#) or to Exit BlackICE.



4. A single regular click on the task-bar icon opens the application as well.

If the tool is not already running, from the **Start** menu, select **Programs**, then select **Network ICE**, then select **BlackICE Utility**.

NOTE: Exiting the Summary application (blackice.exe) does not shut down the intrusion and protection engine. If you wish to completely disable BlackICE you must shut down the BLACKD service. [See How to Disable BlackICE](#) for more information.

\$# How To Disable BlackICE

Although it is not recommended, there may be special circumstances that require disabling BlackICE on a system. Before disabling BlackICE due to network problems, check the Network ICE Knowledge Base. There are many circumstances where a few minor configuration changes will clear up any network or Internet access problems.

There is no mechanism to remotely disable BlackICE. This ensures hackers do not disable the software. You must disable BlackICE manually from each workstation.

WARNING: When BlackICE is disabled, the system is not protected from network intrusions.

For Windows NT Workstation or Server

1. From the **Start** menu, select **Settings**.
2. Double-click **Services** on the **Control Panel**. The Services dialog box is displayed.
3. Locate the BlackICE service and click **Stop**.

Windows NT stops the service. BlackICE will restart when the system is rebooted or restarted from the Services dialog box. You can change the BlackICE service to Manual start up to permanently disable BlackICE.


For a Windows 95/98 System

1. If the BlackICE Utility is running, exit from the program.
2. Press [CTRL] [ALT] [DEL] keys simultaneously.
3. A Close Program dialog box is displayed.
4. Select *BlackICE* or *BLACKD* in the list and click **End Task**.

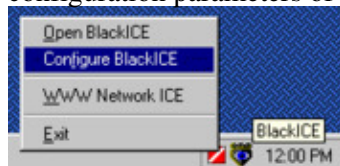
Windows 95/98 stops the BlackICE detection and protection engine. BlackICE will restart when the system is rebooted.

\$# How To Configure BlackICE

You can access the Configuration dialog box two ways: from the Windows task-bar or from the BlackICE summary application.

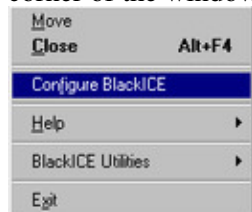
> If the BlackICE summary application has already been started, a small icon  is displayed in the task-bar.

1. Right click on the icon. A sub-menu of choices is displayed.
2. Select **Configure BlackICE**. The Configure BlackICE command allows you to view and modify the configuration parameters of the application.



> If the tool is not already running, from the **Start** menu, select **Programs**, then select **Network ICE**, then select **BlackICE Utility**. This opens BlackICE and places the BlackICE icon on your taskbar. Right click on the icon and proceed as specified above.

> If you are in the BlackICE Summary Application, right click on the BlackICE icon in the upper, left corner of the window. Select **Configure BlackICE** from the pop-up menu.



The Configuration dialog box 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:

Back Trace Tab

Packet Log Tab

Evidence Log Tab

Protection Tab

Trusted Addresses Tab

Blocked Addresses Tab

ICEcap Tab

\$# How To Handle Intrusions

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

Intrusion Considerations

> Does the attack have a priority 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. Most hackers do port scans but never follow up on them.

> 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 them and report them.

> Is the intrusion from your Internet Provider? Many Internet providers perform regular scans of their network. These too are completely safe, although BlackICE will report them.

How to Respond

> If you have a small network, configure each computer to block the attacker.

> If you have a large network, use the ICEcap management console to distribute blocking commands to all the BlackICE agents on your network.

> Configure your corporate firewall to block the intruder.

> Make sure BlackICE is installed on all your Windows-based systems including VPN and telecommuter systems. For areas of your network where UNIX, BeOS, Linux, or Apple operating systems are used, install BlackICE Sentry to monitor the network subnet.

> You may also want to locate the Internet service provider (ISP) for the hacker. One way to stop hackers is to contact their ISP and report their activities. Most ISPs have terms of use that strictly prohibit hacking activities. When notifying an ISP, make sure to include the following information: Your name, your location, date and time of the attack, your timezone, the hackers IP address, DNS address, MAC address, and type of attack. If possible attach the *.log and *.enc file applicable to the attack. These files are located in the directory where you installed BlackICE.

Additional Information About Attacks

For information about each attack type, visit the **NetworkICE advICE** web site. This site includes detailed information about each attack type and how to defend your systems against each attack.

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

For the most current information about intrusions and how to stop hackers, please visit the advICE database at the Network ICE website: <http://www.networkice.com/advise>.

\$# How to Block an Intruder

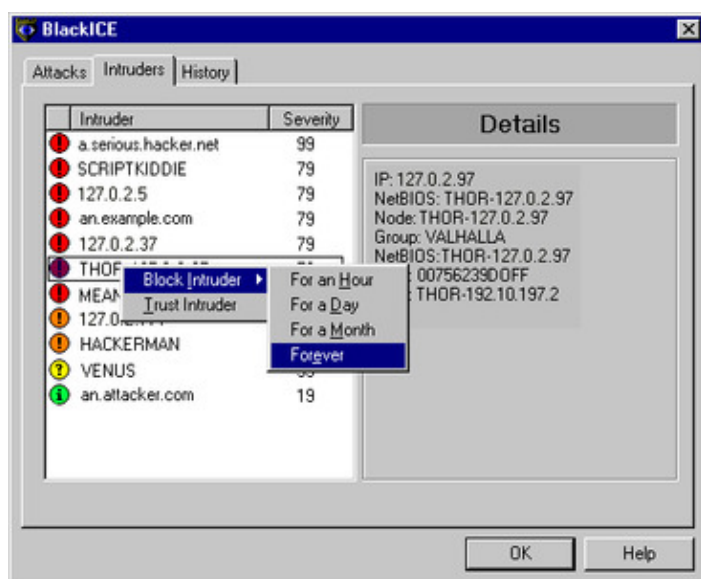
Under normal conditions, BlackICE will allow other systems to access your computer without hindering the network traffic in any way. Most intrusions on systems are innocuous port scans or ping sweeps. These intrusions are not dangerous and thus BlackICE does not automatically block these addresses. Furthermore, some internal systems may generate periodic port scans and ping sweeps to see if devices on your network are alive.

BlackICE only blocks an intruder when he/she initiates an attack that is an immediate threat to your computer. For example, an exploit of a DNS cache will usually cause BlackICE to block the attacker.

However, you can manually instruct BlackICE to block an intruder. BlackICE can only manually block addresses that have initiated an attack.

If you need to issue enterprise-wide protection measures using BlackICE, ICEcap from Network ICE can automatically distribute blocking instructions to all the BlackICE agents on your network. See the ICEcap Administration Guide for more information.

1. From the **Intruder** tab, right click on the intruder you wish 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*.



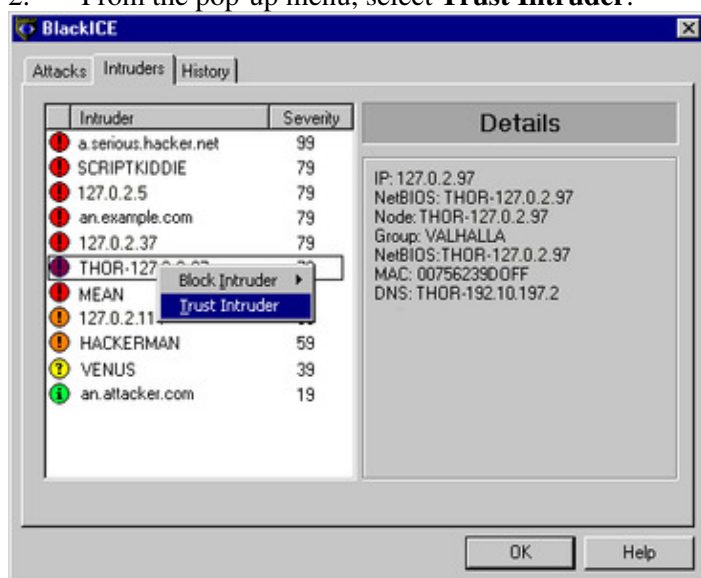
BlackICE adds the intruder to the Blocked Addresses tab. To unblock an intruder please see the [Blocked Addresses Tab](#) in the [Configure BlackICE](#) section.

\$# How to Trust an Intruder

If your network has servers or devices that generate regular scans or probes of networked systems, you may want to trust these systems to ensure BlackICE does not inadvertently block them. For example, if you are using ICEScan from Network ICE to test for vulnerabilities, this system will generate false attacks on BlackICE systems, since it is executing many of the same attacks a hacker would. By trusting the ICEScan system, you can stop BlackICE from reporting ICEScan tests as attacks.

WARNING: When a system is trusted, BlackICE will ignore 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 regularly carry out scans. If you need to issue enterprise-wide trusting measures using BlackICE, ICEcap from Network ICE can automatically distribute trusting instructions to all the BlackICE agents on your network. See the ICEcap Administration Guide for more information.

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



BlackICE adds the intruder to the Trusted Addresses tab. To untrust an intruder please see the [Trusted Addresses Tab](#) in the [Configure BlackICE](#) section.

\$# How to Ignore an Attack

Since some intrusions on a network may be the result of automated port scans or other legitimate network 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.

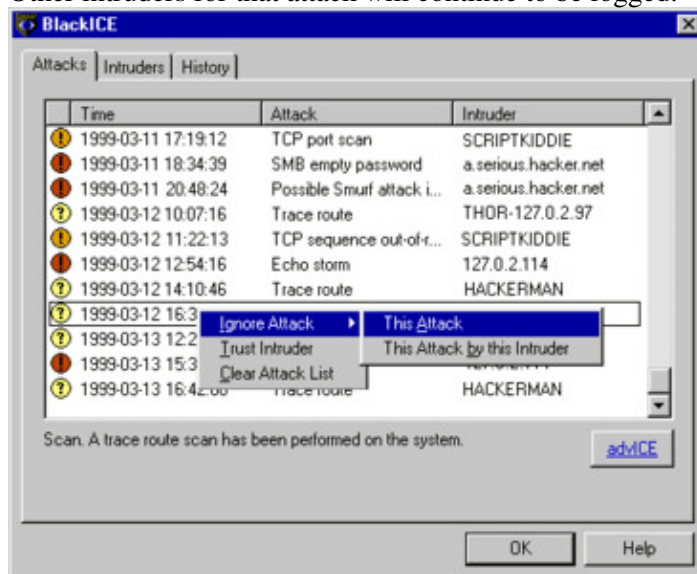
BlackICE allows you to specify an attack or an attack by a specific intruder to ignore.

WARNING: When an entire attack is ignored, BlackICE 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 display, select how you want BlackICE to ignore the attack.

This Attack instructs BlackICE to ignore all future instances of the attack.

This Attack by this Intruder instructs BlackICE to ignore all future instances by the referenced intruder. Other intruders for that attack will continue to be logged.



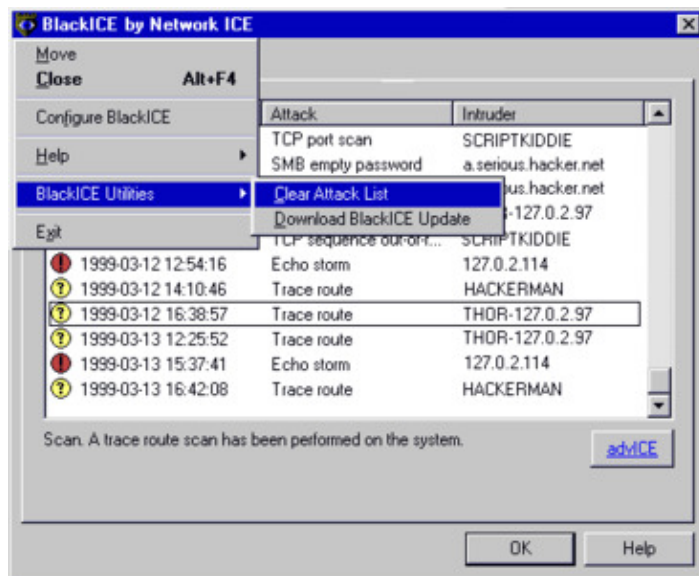
BlackICE begins immediately ignoring the selected attack.

\$#K How Clear the Attack List

After a while the attack list may become rather long. Use this feature to clear out the attack list.

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

1. From BlackICE Summary Application, click on BlackICE icon in the left corner.
2. From the pop-up menu, select **BlackICE Utilities**.
3. A sub-menu is displayed, select **Clear Attack List**.



BlackICE clears out the attack list.

\$# How To Use BlackICE

BlackICE consists of two main components: an invisible detection and protection engine and a summary application.

The detection and protection engines of BlackICE are always running when the computer is operating. These engines are invisible to anyone using the computer to ensure that they are not accidentally or purposefully disabled. Once BlackICE is installed, there is no need to worry about intrusion detection and monitoring. BlackICE works silently whenever the computer is operating.

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

The BlackICE summary application consists of three tabs (the **Attacks Tab**, the **Intruders Tab**, and the **History Tab**), each displaying a different aspect of the intrusion detection and protection.

\$# How To Install BlackICE

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

Minimum System Requirements

> **Operating Systems:** Windows NT Workstation 4.0, Windows NT Server 4.0, Windows 95 or Windows 98.

NOTE: BlackICE has not been tested on Windows 2000 or Windows NT 5.0 systems.

> **Processor:** Pentium or better.

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

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

> **Network Connection:** 10-BASE-T, ADSL, ISDN, cable modem, or regular modem connection using the TCP/IP protocol.

How To Install BlackICE

1. Run **Bisetup.EXE**. If you are running **Bisetup.EXE**, the application must unpack the setup files and verify them first. Once that is finished, **Setup.EXE** runs.

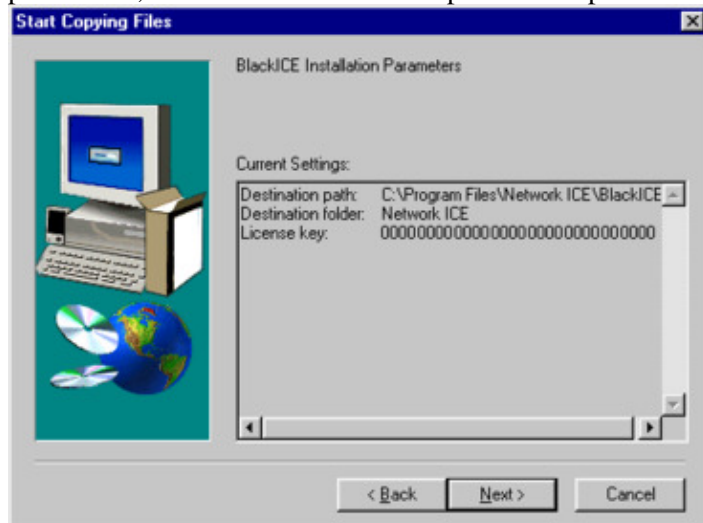
If setup detects an existing version of BlackICE, the setup prompts you to uninstall or continue to upgrade the previous version.

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

3. Review the Licensing Agreement. If you accept the agreement terms, click **Yes**. Otherwise, click **No** to exit the BlackICE setup application.

4. Verify the installation path for BlackICE. If you wish to change the path, click **Browse** and locate the path you wish to use. Click **Next** to continue.

5. 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. BlackICE automatically places a shortcut here to start BlackICE when the system is first started. Click **Next** to continue.
6. Enter your license key. This key was sent to you when you purchased your copy of BlackICE. If you have lost your key, please contact Network ICE Technical Support.
7. The next window summarizes all the selections you have made. If you need to change any of those parameters, click **Back** to retrace the previous steps.



BlackICE Installation Parameters window

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

8. The installation begins. When it is finished, the BlackICE 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, it is good idea to review this information. To review the release notes, click **Yes**. Otherwise, click **No**.
- > The BlackICE setup is complete.

\$# How To Uninstall BlackICE

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

1. From the **Start** menu, select **Settings**. The **Control Panel** is displayed.
2. Double-click **Add/Remove Programs**. The Add/Remove Programs Properties dialog box is displayed.



The Add/Remove Programs dialog box (for Windows NT).

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. Click **Yes** to continue.
6. An UNInstallShield application begins. This application will remove the BlackICE files, registry entries and other features.



UNInstallShield Application removing BlackICE.

7. When the application is completed, click OK.
8. You may need to manually delete the BlackICE folders where you installed the application.

\$# **Control Menu Commands**

This menu is displayed when the BlackICE icon in the upper left corner of the application window is clicked.



The **Control** menu offers the following commands:

Move

Allows you to move the BlackICE application window.

Close

Closes the BlackICE summary application, however the BlackICE notification icon remains active in the windows taskbar. The intrusion monitoring engine always remains active.

Configure BlackICE

Select to configure the BlackICE application.

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.

BlackICE Utilities

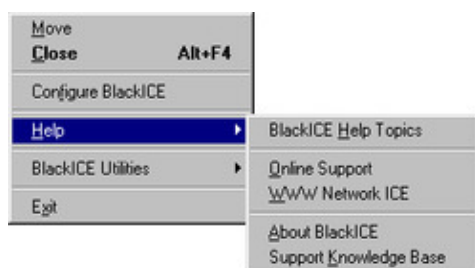
Shows you a sub menu that lets you clear the attacks list or download the latest version of BlackICE.

Exit

Closes the BlackICE summary application. The BlackICE notification icon is removed from the taskbar. The intrusion monitoring engine remains active.

\$# **Help Menu Commands**

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



BlackICE Help Topics

Displays this help system.

Online Support

Opens a web browser session and displays the Network ICE Support 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.

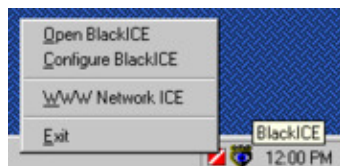
About Network ICE BlackICE

Displays the version number of this application.

Support Knowledge Base

Opens a web browser session and displays the Network ICE Knowledge Base web site. Your system must be connected to the Internet to display this page. This site contains up-to-date information about using and troubleshooting BlackICE and all Network ICE products.

\$# Taskbar Menu Commands



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

Open BlackICE

Select to open the BlackICE application.

Configure BlackICE

Select to configure the BlackICE application.

WWW Network ICE

Link to the World Wide Web page for Network ICE.

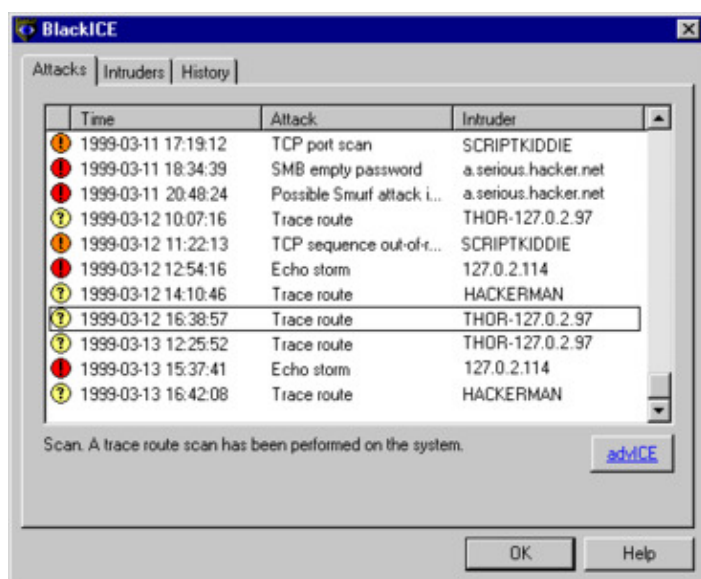
Exit

Exit the BlackICE summary application.

\$# Attacks Tab

The Attacks tab displays a list of the intrusions that BlackICE has detected. This tab summarizes all intrusion events on your system, displaying the time, type of event, and the intruder **s name**.

The information in the Attacks tab is sorted by time first then by severity. To re-sort the list, click a column header; to toggle the sort order (ascending or descending) click the column header again.



Detected events are listed as critical, serious, suspicious, or informational on the Attacks tab.

Icon

This is a visual representation of the severity of the attack. Each event is indicated with one of four severity levels.

Time

Date and time of the attack 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 Attack Column shows the name of the attack. For more information about a particular attack, select the attack in the list and 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, see [How to Handle Intrusions](#) for more information.

Intruder

This is the name of the attacker. The Intruder column displays the best name BlackICE can gather from the attacking system. It displays the NetBIOS (WINS) name, DNS name, or IP address for the attacking system. If BlackICE cannot determine a name, it displays unknown.

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

Status Bar

Summary description of the attack.

advICE

Opens a web browser window and connects to the advICE section of the Network ICE web site. Select the particular attack of interest and click the advICE button. Information about that specific intrusion is displayed.

OK

The BlackICE summary application is closed. The detection and protection engine remains active.

Help





Opens this online help system.

Other Functions

Right-click on a list item to Ignore an Attack, Trust an Intruder, or clear the attack list.

\$# Indicator Column (Icons)

The icons on the left hand side of the dialog box indicate the severity of the attack. There are four security levels: critical, serious, suspicious and informational.

Icon	Description
	<p>Critical Event: <i>Red exclamation point.</i> This is a deliberate attack on your system for the purpose of damaging data or crashing the system. Critical events trigger protection measures.</p>
	<p>Serious Event: <i>Orange exclamation point.</i> This is a deliberate attempt to access information on your system, yet it does not directly damage anything. Serious events can trigger protection measures, if applicable.</p>
	<p>Suspicious Event: <i>Yellow question mark.</i> 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.</p> <p>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 would still report it as a suspicious event. After a few weeks of information is collected, you may notice recurring scans from one location. Note the <u>IP address(es)</u> where the scans originate and contact your ISP. It is likely these scans are a standard part of your ISP's service and pose no threat to your system.</p>
	<p>Informational Event: <i>Green exclamation mark.</i> This indicates that a network event occurred to your computer that is not threatening but worthy of taking note. Informational events do not trigger protection measures.</p>

\$#

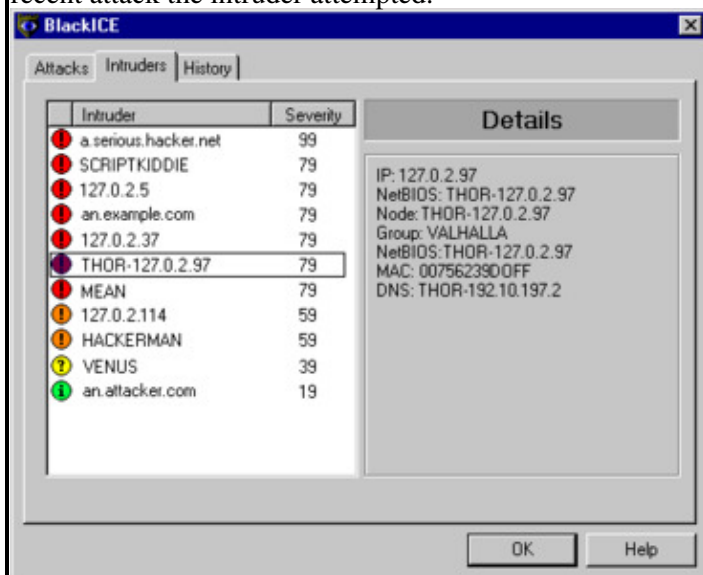
Intruders Tab

The Intruders Tab aggregates information about all the intruders who have provoked events on your system. This tab displays all the backtrace information BlackICE has gathered about an intruder as well as a severity rank.

The information in the Intruders tab is sorted by severity first then by Intruder.

Clicking a column header re-sorts the list by that column, and clicking that column header again toggles the sort order (ascending or descending).

Double-click an intruder entry to view the [Attacks tab](#) focused on the most recent attack the intruder attempted.



See the Intruders Tab component name below for more information:

Icon

This is a visual representation of the severity of the attack. The severity level (one of four) reflects the most severe attack attributed to the Intruder.

Intruder

The Intruder column displays the best name BlackICE can gather from the attacking system. It displays the [NetBIOS](#) (WINS) name, [DNS](#) name, or [IP address](#) for the attacking system. If BlackICE cannot determine a name, it displays unknown .

For more information on a particular [intruder](#), select the intruder in the list and a description of all the information discovered about the intruder is displayed on the right side of the window (the details window).

Severity

A numeric representation of the highest severity attack detected and attributed to the Intruder.

Details Window

Summary of all the known information about the Intruder selected.

OK

The BlackICE summary application is closed. The detection and protection engine remains active.

Help

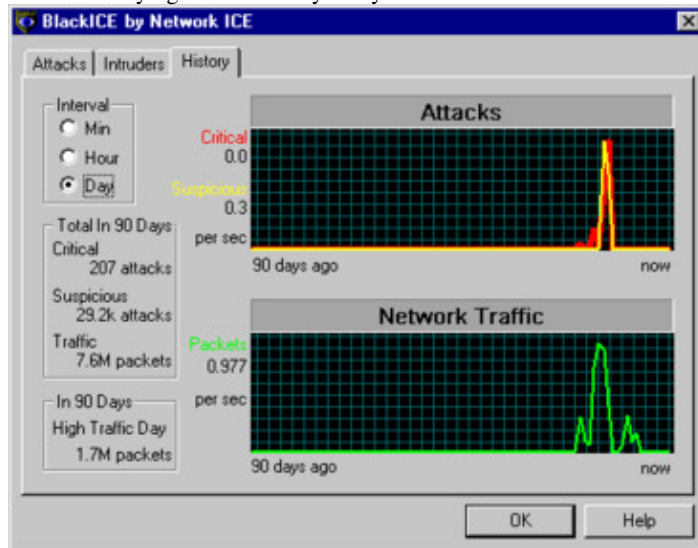
Opens this online help system.

Other Functions

Right-click on a list item to Block an Intruder, Trust an Intruder, or clear the attack list.

History Tab

The History Tab displays intrusion and network traffic statistics in a graphical form. The 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, there is a good chance that someone is trying to break into your system at that time.



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 automatically displays the most informative interval.

Total in 90...

This box displays summary statistics for the time period represented by the graphs. Three statistics are displayed: the total amount of critical attacks detected, the total amount of suspicious attacks detected and the total traffic going through the network.

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

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

In 90...

This box displays the **High Traffic Interval** for the time period represented by the graphs. This is the highest amount of network traffic, measured in number of packets, for the selected interval.

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.

For more information about the attacks, single-click any point in the Attacks graph. This takes you to the

Attacks tab which displays the attacks in descending time order and focuses your attention on the attack which 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.

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.

For more information about the attacks, single-click any point in the Network Traffic graph. This takes you to the Attacks tab which displays the attacks in descending time order and focuses your attention on the attack which comes closest in time to the selected point in the graph.

OK

The BlackICE summary application is closed. The detection and protection engine remains active.

Help

Opens this online help system.

\$#Internet Relay Chat. IRC is a way for multiple users on a system to chat over the network. It 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, and IRC sessions are prone to numerous attacks that, while not dangerous, can cause your system to crash.

\$#Network Basic Input / Output System. NetBIOS is an extension of the DOS BIOS that enables a PC to connect to and communicate with a LAN.

\$#Internet Protocol (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, such as 38.158.99.13.

\$#Blue Screen of Death. 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.

\$#Packet Internet Groper. 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

\$#Internet Control Message Protocol. 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

\$#Transmission Control Protocol. 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.

\$#Server Message Block. 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.

\$#Distributed Computing Environment. 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.

\$#Simple Network Management Protocol. 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.

\$#Common Gateway Interface. 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.

\$#Application Program Interface. 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

\$#Remote Procedure Call. 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.

\$#Simple Mail Transfer Protocol. 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.

\$#Domain Name System. 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 "wall" that contains a network restricting access in and out of the 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.

\$#File Transfer Protocol. 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 its share of vulnerabilities.

\$#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.

\$#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.

\$#BackOrifice: Back Orifice is a remote administration tool which 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 which 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).

\$#K Back Trace Tab

When BlackICE's powerful monitoring engine detects a suspicious event, it immediately starts collecting information. One way BlackICE can locate an intruder is using a networking procedure called *Backtracing*.

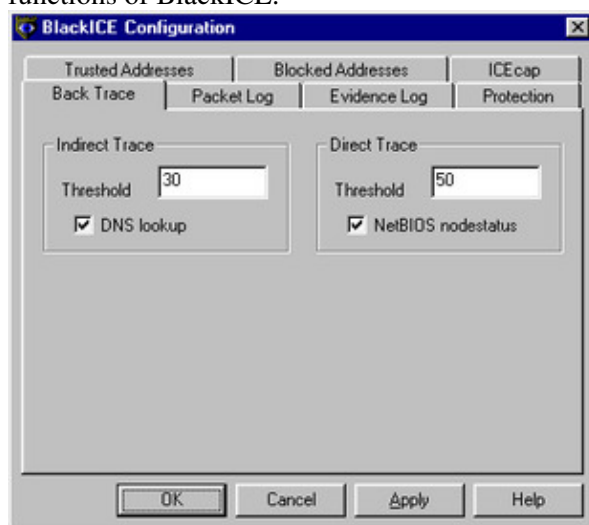
Backtracing is when BlackICE follows a network connection back to its origin. When somebody connects to your computer via a network such as the Internet, your system and the intruder's system exchange packets. Before an intruder's packets reach your system, they travel through several routers. BlackICE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

There are two ways that BlackICE can backtrace 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 backtracing functions of BlackICE.



Indirect Trace Parameters

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

Threshold

Indicates the attack severity level that will trigger an indirect trace of the attack. The default attack severity for the indirect trace threshold is 30.

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 executes direct backtracing. Because direct backtracing makes contact with the intruder's system it acquires a great deal of information. Therefore, direct tracing is best used for higher severity attacks.

Threshold

The attack severity level that triggers a direct trace of the intruder. The default attack severity for the direct trace threshold is 60.

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**.

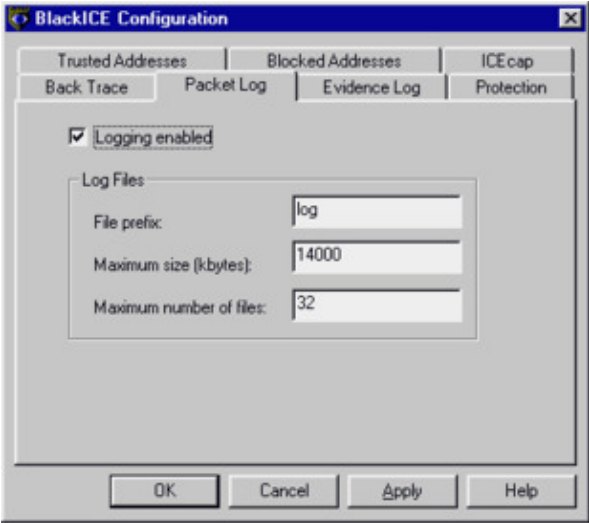
Help

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

\$# Backtrace Threshold Parameters

The Backtrace threshold establishes the severity level where BlackICE initiates a backtrace. Severity refers to the level of each attack. The following list summarizes how BlackICE categorizes severities.

Icon	Severity	Description
	100-80	Critical Event: This is a deliberate attack on your system for the purpose of damaging data or crashing the system.
	80-40	Serious Event: This is a deliberate attempt to access information on your system, yet it does not directly damage anything. These events can trigger protection measures, if applicable.
	40-20	Suspicious Event: This is network activity that is not immediately threatening but may indicate that someone is attempting to locate security

		<p>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.</p>
<p style="text-align: center;">①</p>	20-0	<p>Informational Event: This indicates that a network event occurred to your computer that is not threatening. Informational events do not trigger protection measures.</p>
<p>\$#</p> <h3>Packet Log Tab</h3> <p>The Packet Log tab allows you to configure the packet logging features of BlackICE.</p> <p>When packet logging is enabled, BlackICE records all system traffic into log files. These files can be useful if a network administrator needs to reconstruct what happened in relation to an attack.</p> <p>Packet logs are filled until a maximum size is reached. Then a new file is generated until the maximum files are used. Then BlackICE 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 system resources. However, if you are having repeated intrusions on a system, packet logging can help gather additional information about activity on the system.</p> <p>BlackICE captures network traffic specifically connected to an intrusion in the <u>Evidence Files</u>.</p> 		

Logging Enabled

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

File Prefix

Specifies the prefix for the packet log file names. Use **%d** to place an incremented counter in the file name. For example, if you enter **ABC%d** the file names will be **ABC0001.log**, **ABC0002.log**, etc. The default file prefix is **log**.

Maximum Size (kbytes)

Specifies the maximum size, in kilobytes, for each log file. The default value for the maximum log file size is 0.

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**.

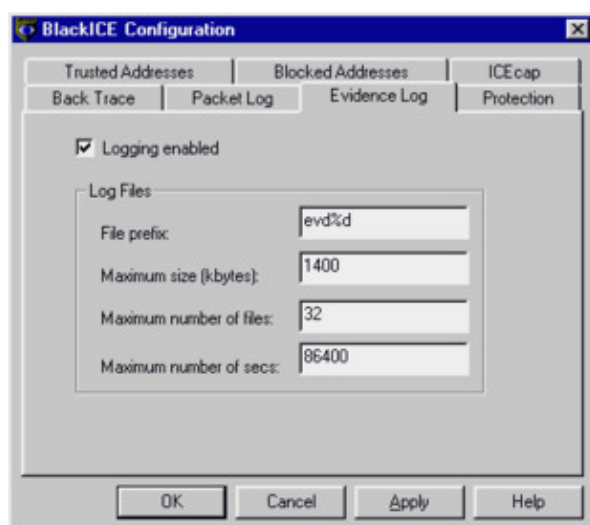
Help

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

\$# Evidence Log Tab

BlackICE constantly monitors your system. When suspicious activity is detected, BlackICE immediately begins to collect information about the event. This information can be placed in Evidence Files. An evidence file is a raw dump of all network traffic from a suspected intruder.

Evidence files are not the same as Packet Logging. Evidence collection is performed for a specific attack and it is a raw dump of all network traffic. An evidence file is therefore applicable to only one intruder/attack combination. Evidence files contain large amounts of information about an intruder. Therefore, BlackICE captures evidence files in a round-robin fashion. It collects files until the maximum number of files are used, then recycles to the first file and replaces it with a new one. To determine the most recent evidence file, check the date and time of the file. For more information, please see the Help section on Evidence Files.



Logging Enabled

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

File Prefix

Specifies the prefix for the evidence file names. Use `%d` to place an incremented counter in the file name. For example, if you enter `ABC%d` the file names will be `ABC0001.log`, `ABC0002.log`, etc. The default file prefix is `evd%d`.

Maximum Size (kbytes)

Specifies the maximum size, in kilobytes, for each evidence file. The default is 1400 kbytes.

Maximum Number of Files

Specifies the maximum number of log files to generate. When BlackICE reaches the maximum file, it recycles to the beginning of the file list. The default value for the maximum number of evidence files to log is 32.

Maximum Number of Secs

Specifies the maximum time period the evidence file reflects. For example, the default setting is 86400 seconds. This would result in a separate evidence file for each 24 hour period.

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 should enforce on the system. There are four pre-set security levels, as defined below.

Trusting: When set to *Trusting*, BlackICE only blocks file sharing over the Internet, unless Internet file sharing is specifically enabled on the Protection tab. Internet file sharing allows the user to share files on their disk with others across the Internet. Blocking Internet file sharing ensures that hackers cannot download files off your computer. All other ports remain open and unblocked. File sharing on an internal network remains unaffected even though Internet file sharing is disabled. This setting is good to use if you have a slower

Internet connection and little threat of attack.

Cautious: The *Cautious* setting is best for regular use of the Internet. This setting only blocks inbound intrusions on System Port(s). All other ports remain unblocked and therefore should not interfere with any Internet usage.

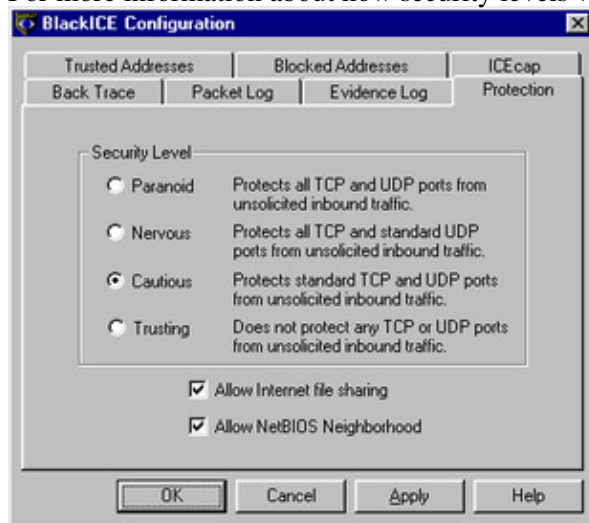
Nervous: The *Nervous* setting is good if you are experiencing repeated intrusions. For this setting, BlackICE blocks inbound intrusions on all the System ports and TCP Application ports. This setting may restrict some interactive content on web sites. Streaming media and other application specific Internet usage remains unaffected.

Paranoid: The *Paranoid* setting is very restrictive, but useful if your system has endured numerous attacks. Under this setting BlackICE blocks all inbound intrusions. This setting may restrict some web browsing and interactive content.

Allow Internet File Sharing: When checked, BlackICE will allow Internet access to directory or drive shares on your system, when unchecked, BlackICE blocks the access of any shares over Internet connections. It is best to leave this option off unless you need to access a system across the Internet. When this option is enabled, it can open your system up to hackers.

Allow NetBIOS Neighborhood: This option blocks or allows the reporting of a system to the Network Neighborhood in Windows. If you are on a corporate network and people need access to your system, it is best to leave this option enabled (checked). If you wish to block other network users from seeing your system in the Network Neighborhood, uncheck this option.

For more information about how security levels work, see the [Security Levels](#) topic.



To Set the Security Level

1. Select the **Security Level** you wish to use. The default Security Level is **Cautious**.
2. If you wish to enable file sharing over the Internet, check the appropriate box. Internet file sharing is disabled by default.
3. If you wish to block the reporting of your system to the Windows Network Neighborhood, uncheck the **Allow NetBIOS Neighborhood**. Otherwise, leave this option checked.
4. Click **Apply** to begin using the new security level.

WARNING: Enabling Internet file sharing makes your computer very vulnerable to simple intrusions. However, when enabled you can connect to your computer over the Internet and upload or download files. For example, 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.

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**.

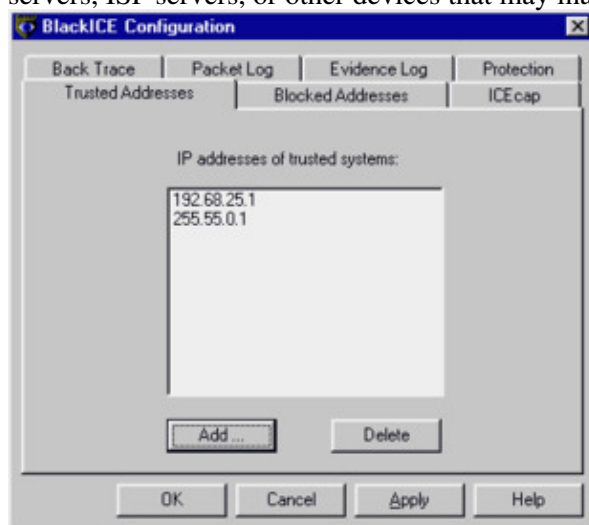
Help

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

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 excluded, BlackICE considers all network traffic from that address to be safe.

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

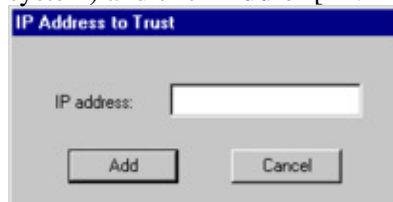


IP addresses of trusted systems

Displays a list of the IP addresses of trusted systems. 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

Select an address in the list you wish to delete and click **Delete**. The address is deleted immediately from the trusted addresses list. This action cannot be reversed.

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**.

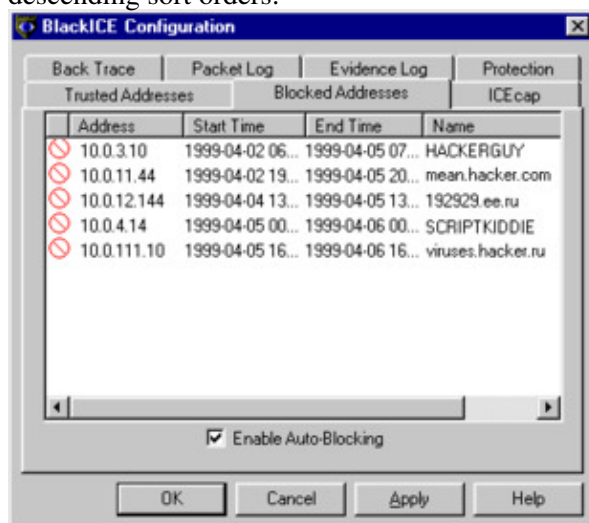
\$# Blocked Addresses Tab

The Blocked Addresses tab shows you the network addresses that BlackICE is blocking. BlackICE rejects all network traffic from blocked IP addresses. This identifies the current hackers.

Blocked addresses have a specific end time, which can be a few minutes or a few days.

Blocked addresses can be converted to Trusted Addresses if necessary. To convert a blocked address, right-click on the address entry and select **Unblock and Trust**. The address is no longer blocked. You may delete the converted address from the Trusted Addresses tab if desired. Note that once **Unblock and Trust** is selected, the action cannot be reversed.

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



Address

Displays a list of IP addresses that are blocked by BlackICE. The default setting has no entries.

Start Time

Date and time the block was initiated. The format is: YYYY-MM-DD-hh:mm:ss. The time is in a 24-hour format for the time zone applicable to your system.

End Time

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

Name

The best name BlackICE has for the referenced address. The name is a DNS or NetBIOS (WINS) name. If BlackICE cannot determine the name of the system, the column is left blank.

Enable Auto-Blocking

Leave this box checked to have BlackICE automatically block hackers when they attempt to break into your system. Unchecking this box disables auto-blocking. Attacks are still reported and logged, but not blocked.

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

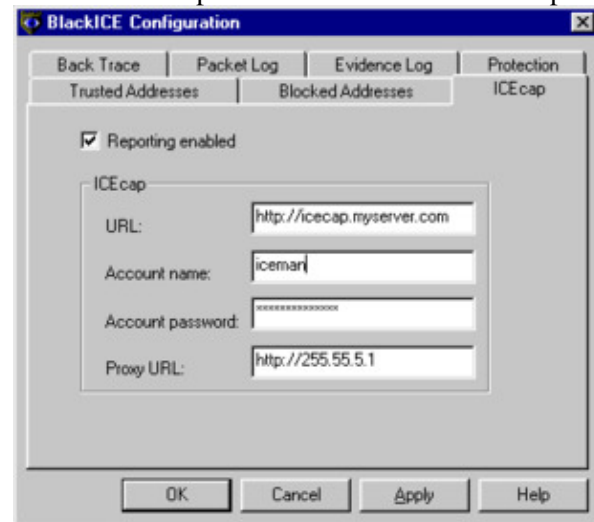
For help on the opened configuration tab, click **Help**.

ICEcap Tab

BlackICE can integrate with an ICEcap server for centralized reporting and analysis of network intrusions. ICEcap is intended for use on internal networks (or LANs) where more than one system is connected to the Internet. For more information about how BlackICE and ICEcap can help manage your network, download a copy of the ICEcap documentation from Network ICE at

www.networkice.com

Depending on the features enabled in your license key, the ICEcap tab may be disabled. This tab allows you to establish the parameters for BlackICE to report events to an ICEcap server.



Reporting Enabled:

Check this box to activate ICEcap reporting. Uncheck to turn off ICEcap reporting.

URL

The fully qualified URL for the ICEcap Server in the format `http://<ICEcap server name>:<TCP port number>`. For example, if ICEcap was on a server named ICECAP using TCP port 8082, the entry would be: `http://ICECAP:8082` (the default).

Account Name

The ICEcap account number to use when uploading data. Refer to your ICEcap documentation for more information about account numbers. The default account name is `default`.

Account Password

Enter the current password BlackICE is using to report information to ICEcap. . Changing the password here does not change the account password in ICEcap, or change the passwords in other BlackICE installations. If BlackICE is not reporting any information to ICEcap, leave this field blank.

Proxy URL

If there is a proxy server between the BlackICE system and the ICEcap server, enter the fully qualified URL for the proxy server.

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**.
