BlackICE™ Quickstart Guide

How To Run BlackICE

- From the Windows **Start** menu, select **Programs**, **Network ICE**, then **BlackICE Utility**.
- If BlackICE is running in the background, a small icon is displayed in the task-bar. Click the icon to open BlackICE Defender.

NOTE: Closing or exiting BlackICE does not turn off the protection and detection features.

How To Start or Stop BlackICE

There may be special circumstances that require you to stop or start BlackICE Defender. When the BlackICE Defender intrusion detection and protection engines are stopped, the system is not protected from any network intrusions. If this is the case, then a red diagonal line is displayed over the BlackICE task-bar icon.

1. From the summary application Menu Bar, select **Tools**, and **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**.

BlackICE 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. Therefore, BlackICE Defender has four Security Levels that allow you to define how rigorously BlackICE blocks unsolicited traffic.

The security level is set on the Protection tab within the BlackICE Settings dialog box (from the Menu Bar, select **Tools**, then **Edit BlackICE Settings**). The more restrictive the security level, the more likely BlackICE will block unsolicited inbound traffic.

Levels	Description
Trusting	All ports remain open and unblocked.
Cautious	This setting only blocks inbound intrusions on System Port(s). All other ports remain unblocked. This is the default setting for BlackICE Defender.
Nervous	Blocks inbound intrusions on all System ports and TCP Application ports. This setting is preferable if you are experiencing repeated intrusions.
Paranoid	Blocks all inbound intrusions. This setting is very restrictive, but useful if your system is enduring repeated attacks.

User Interface Overview

Summary Application Tab Icons

The BlackICE user interface severity indicator displays two important factors. The first is the relative severity of the attack. The second is what action BlackICE took in response to the attack. This BlackICE response level is displayed as an overlay to the main severity icon. For example, if BlackICE blocks an attack of *critical* severity, the icon looks like this: . For more information about a specific event, select the event on the Attacks Tab in the BlackICE summary application, and click the **advICE** button. For information about the BlackICE tabs, please see the User Guide.

Severity Levels

Icons	Severity	Description
!	100 - 75	**Critical event**: These are deliberate attacks on your system.
!	74 - 50	**Serious event**: These are deliberate attempts to access information on your system without directly damaging anything.
?	49 - 25	**Suspicious event**: These are network activities that are not immediately threatening, but may indicate that someone is attempting to locate security vulnerabilities in your system.
i	24 - 0	**Informational event**: These indicate that a network event occurred that is not threatening but worthy of taking note.

Response Level Overlays

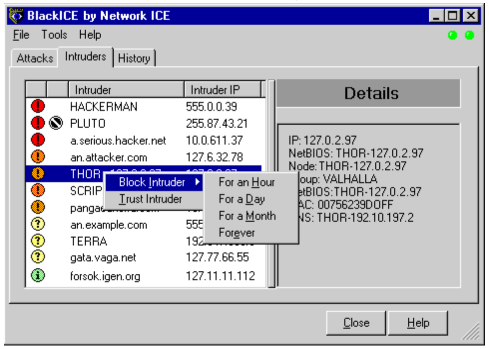
Icons	Description
\	**Attack Blocked:** *Black line overlay.* BlackICE successfully blocked the attack. Depending on the severity of the attack, BlackICE may also have blocked the attacking system. To see if BlackICE is currently blocking the intruder, double-click on the attack. The application displays the Intruders tab. If BlackICE detected and blocked the intruder, then the Blocked State column within the Intruders tab displays the Attack Blocked icon.
\	**Attack Unsuccessful:** *Gray line overlay.* The attack did not compromise the system. Therefore, BlackICE did not need to block the attack.
○	**Attack Status Unknown:** *No overlay*. A network event occurred that BlackICE may or may not have blocked. This likely does not indicate an attack, but is worth noting.
○	**Attack Possible:** *Orange overlay.* BlackICE is not sure if it was able to block the attack. The attack may have compromised the 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 may have compromised the system.

BlackICE™ Quickstart Guide

How To Block Or Trust An Intruder

BlackICE Defender does not automatically block every intruder that attacks your computer. Only attacks that are a direct and immediate threat to the functioning of your system are blocked. You can, however, manually instruct BlackICE to block or trust a system that has initiated an attack. Be careful only to trust those systems that you are certain are legitimately executing network scans, such as servers from your ISP.

1. From the **Intruders** tab, right click on the intruder you wish to block or trust. OR, from the **Attacks** tab, right click on the attack/intruder combination whose intruder you want to block or trust.
2. From the pop-up menu, select **Block Intruder** if you wish to block the intruder; or select **Trust Intruder** if you wish to trust the intruder.



		Intruder	Intruder IP
!		HACKERMAN	555.0.0.39
!	⊘	PLUTO	255.87.43.21
!		a.serious.hacker.net	10.0.611.37
!		an.attacker.com	127.6.32.78
!		THOR	
!		SCRIP	
!		pangae	
?		an.example.com	555
?		TERRA	192
?		gata.vaga.net	127.77.66.55
i		forsok.igen.org	127.11.11.112

Details

IP: 127.0.2.97
NetBIOS: THOR-127.0.2.97
Node: THOR-127.0.2.97
oup: VALHALLA
etBIOS:THOR-127.0.2.97
AC: 00756239D0FF
NS: THOR-192.10.197.2

You can manually block or trust an intruder from the Intruders tab.

3. If you selected **Block Intruder**, 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. A dialog box prompts you to confirm the selected action. Click **Yes** to block or trust the intruder.

For more information, please see Section 4 of the BlackICE Defender User Guide.

How To Configure Columns Displayed

BlackICE allows you to change which columns are displayed on the Attacks and Intruders tabs. You can also modify the size and order of these columns.

1. From the **Attacks** or **Intruders** tab, right-click on a column header, and select **Columns** from the pop-up menu. The Columns dialog box is displayed.
2. To add a column to the tab, select the column name and click **Show**. To remove a column from the tab, select the column name and click **Hide**. To arrange the order of the column on the tab, select the column name and click **Move Up** or **Move Down**.

For more information about customizing columns, please see the BlackICE User Guide.

BlackICE Alarm Preferences

In addition to examining attacks in the summary application, you can set BlackICE Defender to visually or audibly notify you in the event of an attack. Furthermore, you control the severity level when the alarm is triggered.

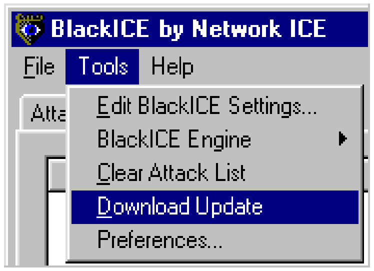
1. From the BlackICE summary application menu bar, select **Tools**, then **Preferences**. The BlackICE Preferences dialog box is displayed.
2. Select the **Visible Indicator** check box to flash the tray icon the color of the most severe attack until the summary application is opened. From the options below, select the severity level that triggers the alarm. The default setting notifies you visually if any suspicious ?, serious !, or critical ! attacks are detected.
3. Select the **Audible Indicator** check box to sound a `.wav` file of your choice whenever an event of the selected severity is detected. Enter the `.wav` file you wish to use in the **WAV File** field. Click the folder icon to browse your system and locate the path desired. To listen to the selected `.wav` file, click **Preview**.
4. Click **OK** to start implementing the attack notification settings.

How To Update BlackICE

Network ICE issues regular updates to BlackICE Defender to ensure it can detect and stop the latest attacks. BlackICE includes a feature to easily update the software.

1. Open the BlackICE application.
2. From the Menu Bar, select **Tools**, and **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, a link is displayed to download the update. Click the link to download the update.

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



For More Information

For more detailed information about BlackICE Defender, refer to the User Guide or the Online Help. The latest product documentation is available from the Network ICE website at http://www.networkice.com/Support. To access the Online Help, click on the **Help** button at the bottom of the BlackICE summary application.