



INTERNET
SECURITY
SYSTEMS™

BLACKICE
SERVER PROTECTION™

Getting Started Guide

Version 3.6



Internet Security Systems, Inc.
6303 Barfield Road
Atlanta, Georgia 30328-4233
United States
<http://www.iss.net>

© Internet Security Systems, Inc. 1998-2003. All rights reserved worldwide. Customers may make reasonable numbers of copies of this publication for internal use only. This publication may not otherwise be copied or reproduced, in whole or in part, by any other person or entity without the express prior written consent of Internet Security Systems, Inc.

Patents pending.

Internet Security Systems, the Internet Security Systems logo, Internet Scanner, System Scanner, Database Scanner, Wireless Scanner, Online Scanner, SiteProtector, ADDME, AlertCon, ActiveAlert, FireCell, FlexCheck, Secure Steps, SecurePartner, SecureU, X-Force, and X-Press Update are trademarks and service marks, and SAFEsuite and RealSecure registered trademarks, of Internet Security Systems, Inc. Network ICE, the Network ICE logo, and ICEpac are trademarks, BlackICE a licensed trademark, and ICEcap a registered trademark, of Network ICE Corporation, a wholly owned subsidiary of Internet Security Systems, Inc. SilentRunner is a registered trademark of Raytheon Company. Acrobat and Adobe are registered trademarks of Adobe Systems Incorporated. Certicom is a trademark and Security Builder is a registered trademark of Certicom Corp. Check Point, FireWall-1, OPSEC, Provider-1, and VPN-1 are registered trademarks of Check Point Software Technologies Ltd. or its affiliates. Cisco and Cisco IOS are registered trademarks of Cisco Systems, Inc. HP-UX and OpenView are registered trademarks of Hewlett-Packard Company. IBM and AIX are registered trademarks of IBM Corporation. Intel and Pentium are registered trademarks of Intel. Lucent is a trademark of Lucent Technologies, Inc. ActiveX, Microsoft, Windows, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation. Net8, Oracle, Oracle8, SQL*Loader, and SQL*Plus are trademarks or registered trademarks of Oracle Corporation. Seagate Crystal Reports, Seagate Info, Seagate, Seagate Software, and the Seagate logo are trademarks or registered trademarks of Seagate Software Holdings, Inc. and/or Seagate Technology, Inc. Secure Shell and SSH are trademarks or registered trademarks of SSH Communications Security. iplanet, Sun, Sun Microsystems, the Sun Logo, Netra, SHIELD, Solaris, SPARC, and UltraSPARC are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the United States and other countries. Adaptive Server, SQL, SQL Server, and Sybase are trademarks of Sybase, Inc., its affiliates and licensors. Tivoli is a registered trademark of Tivoli Systems Inc. UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd. All other trademarks are the property of their respective owners and are used here in an editorial context without intent of infringement. Specifications are subject to change without notice.

Disclaimer: The information contained in this document may change without notice, and may have been altered or changed if you have received it from a source other than ISS or the X-Force. Use of this information constitutes acceptance for use in an "AS IS" condition, without warranties of any kind, and any use of this information is at the user's own risk. ISS and the X-Force disclaim all warranties, either expressed or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall ISS or the X-Force be liable for any damages whatsoever, including direct, indirect, incidental, consequential or special damages, arising from the use or dissemination hereof, even if ISS or the X-Force has been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages, so the foregoing limitation may not apply.

Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Internet Security Systems, Inc. The views and opinions of authors expressed herein do not necessarily state or reflect those of Internet Security Systems, Inc., and shall not be used for advertising or product endorsement purposes.

Links and addresses to Internet resources are inspected thoroughly prior to release, but the ever-changing nature of the Internet prevents Internet Security Systems from guaranteeing the content or existence of the resource. When possible, the reference contains alternate sites or keywords that could be used to acquire the information by other methods. If you find a broken or inappropriate link, please send an email with the topic name, link, and its behavior to support@iss.net.

February 19, 2003



Contents

Chapter 1: Setting Up BlackICE Server Protection	1
Overview	1
System Requirements	3
Downloading BlackICE Server Protection	4
Installing BlackICE Server Protection	5
Stopping BlackICE Server Protection	8
Restarting BlackICE Server Protection	10
Updating BlackICE Server Protection	12
Removing BlackICE Server Protection	15
Getting Help	17
Chapter 2: BlackICE Server Protection Basics	19
Overview	19
Choosing a Protection Level	20
Choosing the Information You Need	22
Managing Notification Settings	25
Customizing Your Firewall	26
Setting Up Application Protection	29
Responding to BlackICE Alerts	32
Index	35



Chapter 1

Setting Up BlackICE Server Protection

Overview

Introduction

BlackICE Server Protection is a comprehensive server security solution that helps you protect your server from:

- theft of passwords, credit card information, personal files, and more
- computer downtime and system crashes
- hackers using your server to launch attacks against other systems

How BlackICE works

BlackICE Server Protection protects your server using these features:

Firewall Capabilities: BlackICE Server Protection provides powerful firewall capabilities. The BlackICE Server Protection firewall inspects all inbound and outbound traffic on your server for suspicious activity. BlackICE blocks unauthorized activity without affecting legitimate traffic.

Intrusion Detection: BlackICE Server Protection contains an advanced intrusion detection system that alerts you to attacks and blocks threats to your server. BlackICE Server Protection captures information about an attacker and logs suspicious activity, which preserves evidence of the attack.

Application Protection: BlackICE Server Protection prevents your server or other computers on a network. Application Protection consists of two main features:

- **Communications Control:** helps you prevent unauthorized applications from communicating on the Internet and can even prevent intruders from using your server to launch attacks against other systems. It does this by letting you control which applications have access to a local network or the Internet.

- **Application Control:** helps you prevent unknown and possibly destructive applications from damaging your server. Application Control gives you control over which applications may launch. BlackICE Server Protection goes beyond the capabilities of other products by preventing unauthorized applications from launching other applications or services.

Optimized for servers

BlackICE Server Protection 3.6 includes the same powerful intrusion detection, firewall and application protection features as BlackICE PC Protection. However, BlackICE Server Protection is specially tuned to detect and stop attacks common to heavily used web, file, database, and application servers.

BlackICE Server Protection includes these additional features:

- Optimization for multiple connections from numerous remote computers.
- Blocks server-specific events such as the Code Red attack against Microsoft IIS Web servers.
- More detailed reporting about attacks common to servers.

In this chapter

This chapter contains the following topics:

Topic	Page
System Requirements	3
Downloading BlackICE Server Protection	4
Installing BlackICE Server Protection	5
Stopping BlackICE Server Protection	8
Restarting BlackICE Server Protection	10
Updating BlackICE Server Protection	12
Uninstalling BlackICE	18
Getting Help	17

System Requirements

Introduction

BlackICE Server Protection is designed for computers that run any supported version of the Windows operating system.

BlackICE Server Protection system requirements

The following table lists the minimum system requirements for BlackICE Server Protection:

Component	Minimum Requirement
Operating System	Windows NT 4.0 (Service Pack 5 or later), Windows 2000 (Service Pack 2 or later)
Processor	Pentium or equivalent CPU
Memory	Minimum 16 MB RAM (64 MB or more recommended)
Hard Drive Space	10 MB free
Network Protocol	TCP/IP
Internet/Network Connection	10/100 Ethernet LAN/WAN, cable modem, DSL router, ISDN router, wireless network or dial-up modem

Table 1: *System requirements for BlackICE Server Protection*

Downloading BlackICE Server Protection

Introduction

You must purchase and download BlackICE Server Protection before you can install it. If you have previously purchased BlackICE Server Protection but you have misplaced your copy of the software, you can download a replacement copy. This topic describes how you can download BlackICE Server Protection.

License key

You will need a valid license key to download a replacement copy of BlackICE Server Protection. If you have misplaced the license key, contact customer support at support-L1@networkice.com to obtain a copy. Include this information in your email:

- Your name, address and telephone number
- The date you purchased BlackICE
- Your order and customer number
- All email addresses you used when you registered BlackICE

Downloading BlackICE

To download BlackICE Server Protection:

1. In the address field of your Web browser, type <http://www.blackice.iss.net>, and then press ENTER.
Your browser displays the BlackICE products home page.
2. Do you want to purchase or replace BlackICE Server Protection?
 - If you are purchasing BlackICE, go to Step 3.
 - If you are downloading a replacement copy, go to Step 5.
3. Click the **Buy Now** link, and then follow the instructions on the page to complete your purchase.
Your product downloads to your server.
4. Go to “Installing BlackICE Server Protection” on page 5.
5. To download a replacement copy of BlackICE Server Protection, click **Update Center**.
6. Click **BlackICE Server Protection 3.6**.
7. Follow the instructions on the page to complete the download.
8. Go to “Installing BlackICE Server Protection” on page 5.

Installing BlackICE Server Protection

- Introduction** This topic describes how to install BlackICE Server Protection after you have downloaded the product from the Web.
- Reference:** For information about how to download BlackICE Server Protection, see “Downloading BlackICE Server Protection” on page 4.
- Prerequisites** Before you install BlackICE Server Protection you must do the following:
- Scan your server for viruses. Because BlackICE creates a baseline record of your system during the installation, you should ensure that the baseline record does not include viruses.
 - Disable the real-time scanning function of any anti-virus detection software running on your server to avoid unwanted interactions during the installation. You can enable this anti-virus function after the installation is completed.
 - Know your license key number.
Reference: For more information about license keys, see “License key” on page 4.
- Installation Procedure** To install BlackICE Server Protection:
1. Locate the directory to which you downloaded BlackICE Server Protection.
 2. Double-click `BISPSetup.exe`.
The InstallShield Wizard for BlackICE Server Protection appears.
 3. Click **Next**.
If the setup program detects an existing version of BlackICE, the program prompts you to uninstall or upgrade the existing version.
 - To update BlackICE, select **Upgrade to version 3.6**.
 - To remove BlackICE from your hard drive, select **Uninstall BlackICE**.
 4. Read the End User License Agreement, and then click **I Accept** if you accept its terms.
The BlackICE Server Protection License window appears.

5. Enter your license key for BlackICE Server Protection.

Reference: For more information, see “License key” on page 4.

6. Click **Next**.

The Choose Destination Location window appears.

7. Select an installation folder.

Note: ISS recommends that you use the default destination location. If you choose to install BlackICE in a directory that is not the default directory, you must make sure the system has full read-write access to the installation directory. For information about setting permissions, see the Microsoft Windows documentation.

8. Click **Next**.

The Select Program Folder window appears.

9. Enter a name for the BlackICE shortcuts folder.

Important: The setup application places a shortcut in the Startup folder automatically, so that BlackICE starts protecting your computer as soon as you start the computer. Do not place BlackICE shortcuts in the Startup folder yourself.

10. Do you want to install BlackICE Server Protection with the Application Protection feature enabled?

- If *yes*, select **AP On**, and then click **Next**.

BlackICE is installed with the Application Protection component available. Go to Step 11.

Note: BlackICE now estimates how much time it will take to build a baseline record of the application files installed on your computer. This can take several minutes.

- If *no*, select **AP Off**, and then click **Next**.

BlackICE is installed with Application Protection disabled. Go to Step 12.

For more information about Application Protection, see “Setting Up Application Protection” on page 29.

11. Will a user be present at the computer on which you are installing BlackICE Server Protection?

- If *yes*, select **Attended**, and then click **Next**.

BlackICE configures the Application Protection component to alert you before stopping unauthorized programs or blocking unauthorized network access.

- If *no*, select **Unattended**, and then click **Next**.

BlackICE configures Application Protection to automatically stop unauthorized programs and network connections from this computer.

The Start Copying Files window summarizes your selections.

12. Click **Finish**.

BlackICE Server Protection service starts automatically.

13. Review the Readme text and then close the Readme file.

Stopping BlackICE Server Protection

Introduction

When you close the BlackICE window, BlackICE Server Protection continues to monitor your system. To stop BlackICE from monitoring for intrusions and to stop protecting your server against unknown or modified applications, you must manually stop the BlackICE intrusion detection and application protection features.

Note: Stopping BlackICE is not the same as removing it. For information about removing BlackICE Server Protection, see “Uninstalling BlackICE” on page 18.

Stopping BlackICE from the console

To stop BlackICE from the BlackICE Server Protection window:

1. From the menu bar, click **Tools** → **Stop BlackICE Engine**.

BlackICE stops monitoring incoming traffic, and a red diagonal line appears over the BlackICE icon. 

2. From the menu bar, click **Tools** → **Stop BlackICE Application Protection**.


BlackICE stops monitoring your system for unauthorized applications and applications connecting to a network.

Stopping BlackICE from the desktop

To stop BlackICE Server Protection from the desktop:

1. Right-click the BlackICE icon. 

2. Select **Stop BlackICE Engine**.

BlackICE stops monitoring incoming traffic, and a red diagonal line appears over the BlackICE icon. 

3. Right-click the BlackICE icon.

4. Select **Stop BlackICE Application Protection**.

BlackICE stops monitoring your system for unauthorized applications and applications connecting to a network.

Stopping BlackICE from the control panel (Windows NT)

To stop BlackICE from the Windows NT control panel:

1. Click **Start**→**Settings**→**Control Panel**.

2. Double-click **Services**.

The Services window appears.

3. Select **BlackICE**, and then click **Stop**.

BlackICE stops monitoring incoming traffic, and a red diagonal line appears over the BlackICE icon. 

4. Select **RapApp**, and then click **Stop**.

BlackICE stops monitoring your system for unauthorized applications and applications connecting to a network.

5. Click **Close**.

Stopping BlackICE from the control panel (Windows 2000)

To stop BlackICE from the Windows 2000 control panel:

1. Click **Start**→**Settings**→**Control Panel**.

2. Double-click **Administrative Tools**.

3. Double-click **Services**.

The Services window appears.

4. In the right pane, right-click **BlackICE**, and then select **Stop**.

BlackICE stops monitoring incoming traffic, and a red diagonal line appears over the BlackICE icon. 

5. In the right pane, right-click **RapApp**, and then select **Stop**.

BlackICE stops monitoring your system for unauthorized applications and applications connecting to a network.

Restarting BlackICE Server Protection

Introduction

You can restart BlackICE Server Protection after you have stopped it, or you can restart your server and let BlackICE Server Protection restart automatically.

Note: If you have stopped BlackICE Server Protection manually, it does not resume monitoring your system when you open the BlackICE Server Protection window on the desktop. To resume monitoring for intrusions and resume protecting your server from unknown or modified applications, you must restart your system or follow one of the following procedures.

Restarting BlackICE from the main window

To restart BlackICE from the BlackICE Server Protection window:

1. From the menu bar, click **Tools** → **Start BlackICE Engine**.

BlackICE resumes monitoring incoming traffic, and the red diagonal line disappears from the BlackICE icon. 

2. From the menu bar, click **Tools** → **Start BlackICE Application Protection**.

BlackICE resumes monitoring your system for unauthorized applications and applications connecting to a network.

Restarting BlackICE from the desktop

To restart BlackICE from the desktop:

1. Right-click the BlackICE icon. 

2. In the pop-up menu, select **Start BlackICE Engine**.

BlackICE resumes monitoring incoming traffic, and the red diagonal line disappears from the BlackICE icon. 

3. Right-click the BlackICE icon.

4. In the pop-up menu, select **Start BlackICE Application Protection**.

BlackICE resumes monitoring your system for unauthorized applications and applications connecting to a network.

Restarting BlackICE from the control panel (Windows NT)


To restart BlackICE from the Windows NT control panel:

1. Click **Start**→**Settings**→**Control Panel**.

2. Double-click **Services**.

The Services window appears.

3. Select **BlackICE**, and then click **Start**.

BlackICE resumes monitoring incoming traffic and the red line disappears from the BlackICE icon. 

4. Select **RapApp**, and then click **Start**.

BlackICE resumes monitoring your system for unauthorized applications and outgoing transmissions.

5. Click **Close**.

Restarting BlackICE from the control panel (Windows 2000)

To restart BlackICE from the Windows 2000 control panel:


1. Click **Start**→**Settings**→**Control Panel**.

2. Double-click **Administrative Tools**.

3. Double-click **Services**.

The Services window appears.

4. In the right pane, right-click **BlackICE**, and then select **Start**.

BlackICE resumes monitoring incoming traffic and the red line disappears from the BlackICE icon. 

5. In the right pane, right-click **RapApp**, and then select **Start**.

BlackICE resumes monitoring your system for unauthorized applications and outgoing transmissions.

Restarting BlackICE by restarting your server

When you restart your server, BlackICE automatically resumes monitoring unless you have disabled Application Protection.

Reference: For information on enabling and disabling Application Protection, see the online Help or the *BlackICE Server Protection User Guide*.

Updating BlackICE Server Protection

Introduction

ISS provides frequent updates to help BlackICE protect your computer from the latest attacks. You can download two kinds of updates:

- Software updates to improve BlackICE performance, fix bugs, or add features.
- Security content updates to enable BlackICE to protect against new kinds of intrusions.

Update notification

You can find out when an update is available in one of two ways:

- BlackICE can automatically check the ISS Web site for both kinds of updates at regular intervals. A small icon in the upper right corner of the BlackICE window indicates that an update is available.
- You can manually instruct BlackICE to check for updates.

Checking for updates automatically

If your computer is always on and connected to a network, it's a good idea to automatically check for software updates.

To check for updates automatically:

1. Click **Tools**→**Edit BlackICE Settings**.
2. Select the **Notifications** tab.
3. In the Update Notification area, select **Enable checking**.
4. In the **Interval for checking (in days)** box, select how often you want BlackICE to check for updates.
5. Click **OK**.

Important: BlackICE starts counting again if you restart the computer or stop and restart BlackICE. If you turn off your server frequently, ISS recommends that you check for updates manually.

Downloading a software update

To use a software update, you must download and install it.

Note: If you have not chosen to have BlackICE check for software updates automatically, use this procedure to check for an update manually.

To check for an update manually:

1. Click **Tools**→**Download Installable Software Update**.

The application connects to the update Web site and the site checks your version number.

2. Is a later version available?

- If *yes*, click the update link, and then go to Step 3.
- If *no*, the Web page displays your version number and license key.

3. Do you want to run the setup file across the network?

- If *yes*, double-click the `update.exe` file.
- If *no*, save the `update.exe` file to your computer, and then double-click the file when you want to install the update.

Downloading a Security Content Update

To use a security content update, you must download and install it.

Note: If you have not chosen to have BlackICE check for security content updates automatically, use this procedure to check for an update manually.

To download a security content update:

1. Click **Tools**→**Download Installable Security Content Update**.

The application connects to the update Web site. If an update is available, the Windows File Download dialog appears.

2. Do you want to run the setup file across the network?

- If *yes*, click **Open**.

Windows downloads and starts the `pamupdate.exe` file. Go to Step 4.

- If *no*, click **Save** and choose a destination on your computer.

Windows stores the `update.exe` file to your computer

3. To install the update, double-click the `pamupdate.exe` file.

4. Click **Next**.

5. Read the License Agreement.

- If you accept the agreement, select **I Accept**, and then click **Next**.

BlackICE stops the intrusion detection service, installs the update, and restarts the service.

- If you do not accept the agreement, select **I Do Not Accept**.

The security content installation stops.

6. Click **Finish**.

Removing BlackICE Server Protection

Introduction

Before you remove BlackICE Server Protection, be sure to record your license key and store it in a safe place. You must re-enter your license key when you reinstall BlackICE.

Note: When you uninstall BlackICE, your system is no longer protected from intrusions.

Uninstalling BlackICE from the Windows Control Panel

To uninstall BlackICE from the Windows Control Panel:

1. Click **Start** → **Settings** → **Control Panel**.
2. Double-click **Add/Remove Programs**.
3. Locate the BlackICE program, and then click one of the following options based on your platform:
 - On Windows NT, click **Add/Remove**.
 - On Windows 2000 or Windows XP, click **Change/Remove**.

The uninstall program asks you to confirm that you want to delete the program files.

4. Click **Yes**.
5. Do you want to remove the remaining intrusion files and delete the directory?
 - If *yes*, click **Yes**.
 - If *no*, click **No**.
6. Did the system encounter errors?
 - If *yes*, read the uninstallation log. You may have to delete the BlackICE folders manually.
 - If *no*, go to Step 7.
7. Click **Finish**.

The system removes BlackICE from your server.

Unable to uninstall

If you are unable to remove BlackICE Server Protection from your server using the Windows Add/Remove Programs utility, you can use the `biremove` utility. The `biremove.exe` program deletes all the files in the BlackICE directory.

Important: Use the `biremove` utility only if you are unable to remove BlackICE Server Protection through the Windows Add/Remove utility. This utility removes both the user interface component (`blackice.exe`) and the intrusion detection engine (`blackd.exe`).

Uninstalling BlackICE using the `biremove` utility

To remove BlackICE Server Protection using the `biremove` utility:

1. Locate the `biremove.exe` file on the BlackICE CD or in the BlackICE folder on your server drive.

Important: Before proceeding, `biremove.exe`, back up any files in the BlackICE folder you do not want to delete.

2. Double-click `biremove.exe`.

The system starts the `biremove` utility.

3. Open the folder that contains the `biremove.exe` file.
4. In the folder, open the log file `AgentRemove-your system name.log`, where *your system name* is the name of the computer running BlackICE Server Protection.
5. Does the log file include the entry `AgentRemove() successful on your system name`?
 - If yes, the utility has removed the BlackICE program successfully.
 - If no, copy the `Retcode` from the entry `AgentRemove() failed on your system name`. `Retcode =` and report the `Retcode` to BlackICE Technical Support (see “Getting Help” on page 17 for contact information).
6. Delete the BlackICE directory from your system.

Getting Help

Introduction You can find detailed information about using BlackICE Server Protection by using the online Help, downloading documents from ISS, or requesting technical support.

BlackICE Help To access the Help, do one of the following:

- On the menu bar, select **Help**→**BlackICE Help Topics**.
- In any BlackICE window, click **Help**.
- On a BlackICE configuration tab, click the question mark in the upper right corner, then click any screen option for a quick explanation of its use.

From the Web site For the latest information about BlackICE Server Protection, go to <http://www.iss.net>, and then click **Products and Services**→**Home and Small Office Protection**→**BlackICE**. Here you can search the following online resources:

- BlackICE Knowledge Base, which contains answers to frequently asked questions (FAQs)
- product documentation
- product updates and upgrade information

Technical Support For technical support, email support-l1@networkice.com.

Telephone support is not available for BlackICE Server Protection.

Chapter 2

BlackICE Server Protection Basics

Overview

Introduction

BlackICE Server Protection protects your server from most types of intrusions as soon as you install it. There are, however, many features of BlackICE Server Protection you can customize. This chapter explains how to customize .

Note: This chapter provides only limited information about certain customizable features available in BlackICE Server Protection. The *BlackICE Server Protection User Guide* provides detailed information. Consult the *User Guide* if you are unsure about how to customize BlackICE.

In this chapter

This chapter contains the following topics:

Topic	Page
Choosing a Protection Level	20
Choosing the Information You Need	22
Managing Notification Settings	25
Customizing Your Firewall	26
Setting Up Application Protection	29
Responding to BlackICE Alerts	32

Choosing a Protection Level

Introduction Protection levels are pre-designed sets of security settings developed for different types of Web use. The protection level you choose determines how aggressively BlackICE blocks network communications with your server. You can change the protection level at any time, simply by selecting a different level.

Default setting BlackICE Server Protection is initially configured to monitor your server at the Trusting protection level.

Protection levels **Paranoid:** BlackICE blocks all unsolicited inbound traffic. This setting is very restrictive, but is useful if your system faces frequent or repeated attacks. This setting may restrict some Web browsing and interactive content.

Nervous: BlackICE blocks all unsolicited inbound traffic except for some interactive content on Web sites (such as streaming media and other application-specific uses of the Internet). This setting is preferable if you are experiencing frequent intrusions.

Cautious: BlackICE blocks unsolicited network traffic that accesses operating system and networking services. This setting is good for regular use of the Internet.

Trusting: All ports are open and unblocked and BlackICE allows all inbound traffic. This setting is acceptable if you have a minimal threat of intrusions.

Note: BlackICE Server Protection is set to the Trusting Paranoid protection level by default. You must customize your protection level immediately after installing BlackICE.

Choosing a protection level

To choose a protection level:

1. Click **Tools** → **Edit BlackICE Settings** → **Firewall**.
2. Select the appropriate protection level.
3. Do you want BlackICE to temporarily block all communications from computers that attempt intrusions?

- If *yes*, select **Enable Auto-Blocking**.
 - If *no*, clear **Enable Auto-Blocking**.
4. Do you want to be able to share files and printers with other users on a network?
 - If *yes*, select **Allow Internet File Sharing**.
 - If *no*, clear **Allow Internet File Sharing**.
 5. Do you want this computer to appear in the Network Neighborhood window of other computers on a network?
 - If *yes*, select **Allow NetBIOS Neighborhood**.
 - If *no*, clear **Allow NetBIOS Neighborhood**.
 6. Click **Apply**.

Customizing protection levels

You can customize a protection level after you choose it. For more information about customizing a protection level, see the Help or the *BlackICE Server Protection User Guide*.

Choosing the Information You Need

Introduction

You probably will not need to inspect all the information that BlackICE gathers about the Internet traffic that reaches your server. This topic describes some of the ways you can customize which events you see.

Filter events

You can configure BlackICE to display only those events that present a certain level of risk to your system. For example, BlackICE determines port scans from your ISP to be of only informational interest. You can have BlackICE omit those events from the Events tab.

Filtering the Events list

To filter events:

1. Click **View** → **Filter by Event Severity**.
2. Select the least severe events you want BlackICE to show.

Tip: If you select **Suspicious**, all suspicious, serious, and critical attacks appear. If you select Informational, all intrusions appear.

Note: When the list is filtered, the Filter by Event Severity list shows only the severity icons for the events you choose to see. For example, if the list is filtered to show only serious and critical events, the suspicious and informational icons do not appear.

Freeze events

Sometimes BlackICE records events so quickly that you can have trouble keeping track of them as they appear on the Events tab. When this happens, you can freeze the Events tab and respond to the events at your convenience. Freezing the Events list only stops BlackICE from refreshing the tab information, it does not stop the monitoring, detection, and protection features of BlackICE Server Protection.

Note: Remember to unfreeze the application after you view the events so that BlackICE can show any new attacks. When you restart the computer, BlackICE resets itself to an unfrozen state.

Freezing the Events tab

To freeze the Events tab:

- Click **View** → **Freeze**.

- Clear events** Even if you are filtering out low risk events, your events list can grow very long. You can clear individual events from the Events tab, or you can clear the whole events list.
- Clearing an individual event** To clear an individual event:
- Right-click the event, and then select **Delete**.
- Clearing the Events list** To clear the Events list:
- Note:** Clearing the event list does not stop BlackICE from trusting, blocking or ignoring events or intruders.
1. Click **Tools** → **Clear Files**.
The Files to Delete window appears.
 2. Do one of the following:
 - Select **Attack-list.csv** to delete all intrusion records from the Events tab.
 - Select **Evidence logs** to delete all evidence log data.
 - Select **Packet logs** to delete all packet log data.
 3. Click **OK**.
A message informs you that you are about to delete the list.
 4. Click **OK**.
- Display relevant information** You can configure BlackICE to show only the information you are most interested in. For example, if you find that multiple attacks on your server use the same protocol, you can have BlackICE display the Protocol column in the Events tab.

Choosing columns to display

To select columns to display:

1. On the Events or Intruders tab, right-click the column header, and then select **Columns**.

The Columns window appears.

2. Follow the instructions on the Columns window to customize the appearance of the columns.
3. Click **OK**.

Managing Notification Settings

- Introduction** BlackICE can notify you of events by making a sound or by showing an alert icon in your system tray. The alert icons indicate the seriousness of the event.
- Default setting** BlackICE Server Protection is configured to display a visible indicator of all events it detects.
- Procedure** To set BlackICE alarm preferences:
1. Click **Tools** → **Edit BlackICE Settings**.
 2. Select the **Notifications** tab.
 3. In the Event Notification area, do one or both of the following:
 - Select **Visible Indicator**, and then select the severity option level to trigger a visible alarm.
 - Select **Audible Indicator**, and then select the severity option level to trigger a .wav file.

Note: If you select the Audible Indicator option, the **WAV File** field shows the default alarm sound (biaalarm.wav). To change the .wav file used in audible notification, click the folder icon and locate the desired file.
 4. Click **Apply**.
 5. Click **OK**.

Customizing Your Firewall

Introduction

BlackICE Server Protection identifies and blocks most intrusions according to your preset protection level, but you may still notice activity that is not explicitly blocked. This topic describes how to block intrusions from a specific intruder and how to ignore certain types of events. This topic also lists other firewall settings you may want to customize.

Caution: Do not block port scans from your own ISP. This can violate your ISP term of service and you may be disconnected.

Block intruders

You can block any intruder listed on your events list by adding the intruder's IP address to your firewall. After you block an intruder, BlackICE blocks any traffic from that intruder's IP address your server.

Blocking an intruder or an event

To block an intruder or an event:

1. Do one of the following:
 - On the **Intruders** tab, right-click the intruder.
 - On the **Events** tab, right-click the event.
2. On the pop-up menu, select **Block Intruder**.
3. On the pop-up menu, select the duration of the block.

Note: A month is defined as 30 days.
4. Click **Yes**.

Ignore events

To help reduce the amount of information BlackICE displays, you can choose to ignore events that do not present a threat to your server. For example, your ISP may carry out routine port scans for its own management purposes. If BlackICE displays many port scan events from your ISP, you may want to configure BlackICE to ignore all events of this type from this intruder.

Note: When you configure BlackICE to ignore events, BlackICE does not log any information about those events.

Ignoring an event

To ignore an event:

1. On the **Events** tab, right-click the event, and then select **Ignore Event**.
2. From the pop-up menu, select one of the following:
 - **This Event:** BlackICE ignores all future instances of the selected event.
 - **This Event by this Intruder:** BlackICE ignores all future instances of this event by this intruder.
3. Click **Yes**.

BlackICE adds the event to the list of ignored events on the **Detection** tab in the **BlackICE Settings** window.

Ignore a future event

To ignore a future event:

1. Click **Tools**→**Edit BlackICE Settings**.
 2. Select the **Intrusion Detection** tab.
 3. Click **Add**.
- The Exclude from Reporting window appears.
4. Do one of the following:
 - To ignore future events of a specific type, go to Step 5.
 - To ignore future events from a specific intruder, go to Step 6.
 5. Select **All** in the **Addresses to Trust** area, and then go to Step 8.
 6. Type the IP address of the intruder in the **IP** box.

- Use standard 000.000.000.000 notation.

- If you ignore events from a range of IP addresses, place a dash between them. For example, 192.168.10.23–192.168.10.32.

7. In the **Events to Ignore** area, clear the **All** check box.

The system enables the **Name** and **ID** boxes, and disables the **Add Firewall Entry** check box.

8. Select the event type in the **Name** box, or select the event number in the **ID** box.
9. Click **Add**.
10. Click **OK**.

Additional firewall customization

BlackICE allows you to customize additional firewall settings, such as:

- blocking a port
- blocking a specific IP address
- accepting a specific IP address
- accepting a specific port
- trusting a specific address

For more information about customizing these settings, see the *BlackICE Server Protection User Guide*.

Setting Up Application Protection

Introduction

BlackICE Server Protection protects your server from the potentially harmful activity of unauthorized applications by monitoring the applications on your server. Application Protection consists of two main features:

- **Application control:** enables you to control which applications may launch. This can prevent unknown and possibly destructive applications from damaging your server.
- **Communications control:** enables you to control which applications have access to a local network or the Internet. This can prevent unauthorized applications communicating on the Internet and can even prevent intruders from using your server to launch attacks against other systems.

Application Protection

Important: BlackICE protects your computer from unknown applications and from applications connecting to a network, such as the Internet. **Tools → Edit BlackICE Settings**, and select either the Application Control tab or the Communications Control tab. Then clear the Enable Protection check box. BlackICE cannot protect you from applications that were installed or modified before you installed BlackICE Server Protection. If you create a baseline record that includes malicious applications, those applications will still be able to launch and connect to a network.

Application control default setting

The default behavior of BlackICE Server Protection depends on the choices you made during installation:

- If you installed BlackICE Server Protection in Attended mode, BlackICE asks you what to do when it detects an unknown or a modified application trying to launch.
- If you installed BlackICE in Unattended mode, BlackICE automatically terminates any unknown application that tries to launch or contact a network.

BlackICE also is configured to protect its own program files, so that BlackICE configuration files cannot be altered without your authorization.

Changing the Application Control settings on your server

To control which applications can run on your server:

1. Click **Tools** → **Edit BlackICE Settings**.
2. Select the **Application Control** tab.
3. In the **When an unknown application launches** section, select one of the following:
 - **Ask me what to do:** BlackICE prompts you to specify whether you want unknown applications to launch. This setting is selected by default if you installed BlackICE in Attended mode.
 - **Always terminate the application:** BlackICE terminates any unknown applications that attempt to launch. This setting is selected by default if you installed BlackICE in Unattended mode.
4. In the **When a modified application launches** section, select one of the following:
 - **Ask me what to do:** BlackICE prompts you to specify whether you want modified applications to launch. This setting is selected by default if you installed BlackICE in Attended mode.
 - **Always terminate the application:** BlackICE terminates any modified applications that attempt to launch. This setting is selected by default if you installed BlackICE in Unattended mode.
5. Select the **Protect Agent Files** check box if you want to prevent changes being made to the BlackICE configuration files. This box is selected by default.
6. Click **OK**.

Communications control

You can configure BlackICE Server Protection to notify you whenever an application tries to connect to a network. BlackICE detects outbound transmissions and asks you what you want to do. You can allow your server to connect, or you can tell BlackICE to block the transmission. In either case, you can make your choice permanent or for this occurrence only.

Communications control default setting

BlackICE communications control is configured to automatically block applications from contacting a network. To change this behavior, change the settings on the Communications Control tab.

Changing the communications control settings

To control outbound communications:

1. Click **Tools**→**Edit BlackICE Settings**.
2. Select the **Communications Control** tab.
3. Select one of the following:
 - **Always terminate the application:** BlackICE automatically shuts down the application attempting to connect to the network. This setting is selected by default if you installed BlackICE in Unattended mode.
 - **Prompt before terminating the application:** BlackICE asks you if you want to terminate the application attempting to connect to the network. This setting is selected by default if you installed BlackICE in Attended mode.
 - **Always block network access for the application:** BlackICE blocks the application from connecting to the network but does not terminate the application.
 - **Prompt before blocking network access for the application:** BlackICE asks you if you want to block the application from connecting to the network but does not terminate the application.
4. Click **OK**.

Disabling Application Protection

To disable Application Protection:

1. Click **Tools**→**Edit BlackICE Settings**.
2. Select the **Application Control** tab or the **Communications Control** tab.
3. Clear **Enable Advanced Application Protection**.
Note: When you disable Application Protection, you disable both application control and communications control.
4. Click **OK**.

Responding to BlackICE Alerts

Introduction

BlackICE Server Protection indicates the severity of an event by placing an icon beside each event listed on the Events tab. BlackICE Server Protection indicates the action taken in response to the event by placing a mark on the severity level icon.

Severity levels

BlackICE indicates the seriousness of an intrusion by displaying an icon and a number on the Events tab. This table shows the icon and range of numbers for each severity level:





Icon	Rank	Description
	7-10	Critical event: A deliberate attack on your system.
	4-6	Serious event: A deliberate attempt to access information on your system without directly damaging anything.
	1-3	Suspicious event: Network activity that is not immediately threatening, but may indicate that someone is trying to locate security vulnerabilities in your system.
	0	Informational event: A network event that is not threatening, but is worth noting.

Table 2: Security level icons and what they mean

Response levels

BlackICE indicates how it responded to an event by overlaying a mark on the event's severity level icon. The following table shows the response level overlays:



Mark	Effect
	Attack Blocked: (Black line overlay) BlackICE successfully stopped the intrusion. BlackICE may also have blocked the intruding computer. To see if BlackICE is blocking the intruder, double-click the event.
	Attack Unsuccessful: (Gray line overlay) Other defenses successfully stopped the intrusion, so BlackICE did not need to block it. The event did not compromise the system.

Table 3: Response overlays and what they mean



Mark	Effect
(None)	Attack Status Unknown: (No overlay) BlackICE took protection measures, but some packets may have made it through to your server. It is unlikely that the event compromised the system.
	Attack Possible: (Orange overlay) BlackICE triggered protection measures, but some attacking packets were able to get through to your server. The event may have compromised the system.
	Attack Successful: (Red overlay) BlackICE detected but could not block the intrusion. The event has compromised the system.

Table 3: *Response overlays and what they mean (Continued)*

Index

a

- accepting a specific IP 28
- accessing the online Help 17
- alert
 - audible 25
 - visual 25
- alert preference
 - setting 25
- application control 2, 30
 - default setting 29
 - limitations 29
- application protection 29
 - application control 29
 - communication control 29
 - disabling 31
 - restarting 10
 - stopping 8
- Attack Blocked overlay 32
- Attack Possible overlay 33
- Attack Status Unknown overlay 33
- Attack Successful overlay 33
- Attack Unsuccessful overlay 32
- audible alert 25
 - wav file 25
- automatically checking for updates 12

b

- baseline record
 - installation prerequisites for 5
- biremove utility 15

BlackICE

- controlling applications 2
 - controlling network access 1
 - firewall capabilities 1
 - intrusion detection 1
 - restarting 10
 - stopping 8
 - uninstalling 15
- BlackICE Help 17
- blocking
 - intruders 26
 - port 28
 - specific IP 28

C

- Cautious 20
- changing
 - protection level 21
 - wav file 25
- checking for updates 12
- choosing
 - protection level 20
- clear events list 23
- communications control 1, 30–31
 - default setting 30
- contacting support 4, 17
- controlling
 - applications 30
 - communications 31
- Critical event icon 32
- customizing
 - protection level 21

d

- default 31
- default setting
 - application control 29
 - communications control 30
 - protection level 20
- disabling
 - application protection 31
- downloading 4
- downloading updates 12

e

- events
 - clear, list 23
 - filter, list 22
 - freeze list 22
 - ignoring 27

f

- FAQ 17
- filter events list 22
- freeze events list 22
- frequently asked questions 17

g

- getting help 17
- getting support 17

h

- help 17
 - product documentation 17
 - technical support 17
 - with BlackICE 17

i

- icon
 - Critical event 32
 - Informational event 32
 - Serious event 32
 - Suspicious event 32
- ignoring events 27
- Informational event icon 32
- installation
 - default location 6
 - updating existing 12
- installation instructions 5
- installation prerequisites 5
- installing 5
 - prerequisites 5
- intruders
 - blocking 26
- intrusion
 - severity levels 32

l

- license key
 - needed for installation 5
 - recording 15
 - replacing 4
- limitations of application control 29

m

- manually checking for updates 12
- monitoring
 - restarting 10
 - stopping 8

n

- Nervous 20

O

- online resources
 - advICE library 17
 - help 17
 - knowledge base 17
 - product documentation 17
- outbound communications 31
- overlay
 - Attack Blocked 32
 - Attack Possible 33
 - Attack Status Unknown 33
 - Attack Successful 33
 - Attack Unsuccessful 32

P

- Paranoid 20
- port
 - blocking 28
- prerequisites
 - installation 5
- product documentation 17
- product updates 17
- protection level
 - Cautious 20
 - changing 21
 - choosing 20
 - customizing 21
 - default setting 20
 - Nervous 20
 - Paranoid 20
 - Trusting 20

R

- restarting
 - application protection 10
 - BlackICE 10
 - monitoring 10

- restarting BlackICE
 - by restarting your system 11
 - from the control panel 11
 - from the desktop 10

S

- Serious event icon 32
- setting
 - alert preference 25
- severity levels 32
- software updates 12
- specific IP
 - blocking 28
 - trusting 28
- specific IP, accepting 28
- stop monitoring 8
- stopping application protection 8
- stopping BlackICE 8
 - from the console 8
 - from the desktop 8
 - Windows 2000 control panel 9
 - Windows NT control panel 9
- support 4, 17
- Suspicious event icon 32

T

- technical support 17
 - email address 4, 17
- Trusting 20
- trusting
 - specific IP 28

U

- unable to uninstall 15
- uninstalling
 - biremove utility 15
 - BlackICE 15

updates 12
 checking for automatically 12
 checking for manually 12
 downloading 12
updating
 existing installation 12
 updating an application 29
 upgrade information 17

V

visual alert 25

W

wav file 25

**END-USER SOFTWARE LICENSE AGREEMENT FOR INTERNET SECURITY SYSTEMS(TM) BLACKICE(TM) SOFTWARE
(Intrusion Countermeasure Enhancements Products)**

This **BLACKICE End-User Software License Agreement ("EUSLA")** is a legal agreement between you, either an individual or a single entity, ("Licensee") and Internet Security Systems, Inc., a Georgia corporation with offices at 6303 Barfield Road, Atlanta, Georgia 30328 ("ISS") for the ISS **BLACKICE software products ("PRODUCT")**. By installing, copying, or otherwise using **PRODUCT**, the Licensee agrees to be bound by the terms of this EUSLA. If the Licensee does not agree to the terms of this EUSLA, do not install or use the **PRODUCT**; the Licensee may, however, return the **PRODUCT** to the place of purchase for a refund.

1. DEFINITIONS.

- a. **PRODUCT** means all components of BlackICE Server Protection supplied by ISS including, but not limited to, the License Key, computer software, online electronic documentation, HTML files, help text, and PDF files, and may include associated media or printed materials.
- b. **LICENSE** means the rights to use the **PRODUCT** on a single computer running one of the following operating systems, Windows XP Home, Windows XP Pro, Windows 2000 Pro, Windows Me, Windows NT 4.0 Workstation or Windows 98 as set forth in Section 2(b) below.
- c. **LICENSE KEY** means a sequence of ASCII characters that uniquely identifies the Licensee and is entered into the **PRODUCT** to define and enable the **PRODUCT**'s features for a period of time.
- d. **EFFECTIVE DATE** means the date that the **PRODUCT** was delivered to the Licensee, where the delivery consists of a **LICENSE KEY** and **WEB link (URL)** from which the Licensee may download the **PRODUCT**.
- e. **TERM** means the period of time ISS grants the **LICENSE** to the Licensee under the terms and conditions of this EUSLA and is defined by the Perpetual type **LICENSE**.
- f. **PERPETUAL LICENSE** has an unlimited **LICENSE TERM**, unless the EUSLA has been terminated earlier.
- g. **MAINTENANCE** means the Licensee's right to receive product and security updates, patches, product upgrades and technical support.
- h. **ANNUAL MAINTENANCE FEE** means the fee paid by the Licensee to ISS for the right to receive one (1) year of **MAINTENANCE**.

2. RIGHTS AND LIMITATIONS.

- a. Subject to the terms and condition of this EUSLA, ISS grants the Licensee a non-exclusive, non-assignable **LICENSE** to use the **PRODUCT** from the **EFFECTIVE DATE** and for the duration of the **TERM**.
- b. The **PRODUCT** may only be installed on computers that are used solely for the Licensee's own personal or internal business. This EUSLA does not grant any rights to use or install the **PRODUCT** on computers used primarily to service or to benefit persons not having either an employment or contractual business relationship with the Licensee, such as a **WEB server** servicing the public.
- c. Notwithstanding anything else contained in this EUSLA, ISS retains all title to, and, except as expressly and unambiguously licensed herein, all rights to (i) the **PRODUCT**, and all related documentation and materials, (ii) all of their service marks, trademarks, trade names or any other designations and (iii) all copyrights, patent rights, trade secret rights and other proprietary rights in the **PRODUCT**.
- d. The initial purchase of a **PERPETUAL LICENSE** includes **MAINTENANCE** until the first (1st) year anniversary from the **EFFECTIVE DATE**. Thereafter, the Licensee must pay the then **CURRENT ANNUAL MAINTENANCE FEE** for continuation of **PRODUCT MAINTENANCE**.
- e. The Licensee does not have any rights to use the **PRODUCT** on any operating system other than those explicitly sited in Section 1 (b).

3. LICENSEE'S OBLIGATIONS.

Except as expressly and unambiguously provided herein and as conditions of the Licensee's **LICENSE** hereunder, the Licensee represents, warrants and agrees:

- a. Not to reverse assemble, de-compile, or otherwise attempt to derive source code (or the underlying ideas, algorithms, structure or organization) from the **PRODUCT** or from any other information, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation.
- b. To keep all copies of the **PRODUCT** in the possession of the Licensee.
- c. Not to sell, give, lend, give access to, or otherwise transfer the **PRODUCT**, or copies of the **PRODUCT** to anyone that is not an employee or consultant of the Licensee, or to anyone that is not bound to all of the terms and conditions of this EUSLA.
- d. Not to use the **PRODUCT** for timesharing, outsourcing, hosting, or service bureau purposes or otherwise allow others, or third parties benefit from the use of the **PRODUCT**.
- e. Not to remove from any copies of the **PRODUCT** any product identification, copyright or other notices.
- f. Not to modify, incorporate into or with other software, or create a derivative work of any part of the **PRODUCT**.
- g. Not to disseminate performance information or analysis (including, without limitation, benchmarks) from any source relating to the **PRODUCT**.

4. TERMINATION.

- a. Without prejudice to any other rights, ISS may immediately terminate the **LICENSE** if the Licensee fails to comply with all of the terms and conditions of this EUSLA. In such an event, the Licensee must destroy all copies of the **PRODUCT** and all of its component parts.
- b. All of the terms and conditions of this EUSLA shall survive termination with the exception of the **LICENSE** as defined in Sections 1 (b) and Sections 2(a) and 2(d). Termination is not an exclusive remedy and all other remedies will be available to Licensor whether or not the **LICENSE** is terminated.

5. GOVERNING LAW.

This EUSLA shall be deemed to have been made in, and shall be construed pursuant to the laws of the State of Georgia and the United States, without regard to conflicts of laws provisions thereof. This EUSLA will not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded. The prevailing party in any action to enforce this EUSLA shall be entitled to recover reasonable costs and expenses, including, without limitation, reasonable attorneys' fees. If any part of this License is found void or unenforceable, it will not affect the validity of the balance of the License, which shall remain valid and enforceable according to its terms.

6. EXPORT AND IMPORT CONTROLS; USE RESTRICTIONS.

The Licensee will not transfer, export, or reexport the **PRODUCT**, any related technology, or any direct product of either except in full compliance with the export controls administered by the United States and other countries and any applicable import and use restrictions. The Licensee agrees that it will not export or reexport such items to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Commerce Department's Denied Persons List or Entity List, or to any country to which the United States has embargoed goods, or for use with chemical or biological weapons, sensitive nuclear end-uses, or missiles. The Licensee represents and warrants that it is not located in, under control of, or a national or resident of any such country or on any such list. Many ISS Products include encryption and export outside of the United States or Canada is strictly controlled by U.S. laws and regulations. Please contact ISS' Customer Operations for export classification information relating to the **PRODUCT** (customer_ops@iss.net). The Licensee understands that the foregoing obligations are U.S. legal requirements and agrees that they shall survive any term or termination of this License. The **PRODUCT** is a "commercial item," "commercial computer software," and/or "commercial computer software documentation" as defined under U.S. law in FAR section 2.101, DFAR section 252.227-7014(a)(1) and DFAR section 252.227-7014(a)(1), or otherwise. Consistent with DFAR section 227.7202 and FAR Section 12.212, any use, modification, reproduction, release, performance, display, disclosure or distribution of the **PRODUCT** by the

U.S. government shall be governed solely by the terms of this EUSLA and shall be prohibited except to the extent expressly permitted in this EUSLA.

7. LIMITED WARRANTY AND DISCLAIMER.

ISS WARRANTS THAT FOR A PERIOD OF THIRTY (30) DAYS FOLLOWING THE EFFECTIVE DATE THE PRODUCT WILL MATERIALLY CONFORM TO ISS' THEN CURRENT OPERATIONAL SPECIFICATIONS. THE FOREGOING WARRANTIES COVER ONLY PROBLEMS REPORTED TO ISS DURING THE WARRANTY PERIOD. ANY LIABILITY OF ISS WITH RESPECT TO THE SOFTWARE OR THE PERFORMANCE THEREOF OR DEFECTS THEREIN UNDER ANY WARRANTY, NEGLIGENCE, STRICT LIABILITY OR OTHER THEORY WILL BE LIMITED EXCLUSIVELY TO PRODUCT REPLACEMENT OR, IF ISS DETERMINES, IN ITS SOLE DISCRETION, THAT REPLACEMENT IS INADEQUATE AS A REMEDY OR IMPRACTICAL, TO REFUND OF THE LICENSE FEES PAID BY THE LICENSEE AND TERMINATION OF THE LICENSE. EXCEPT FOR THE FOREGOING, THE PRODUCT AND ISS PROPRIETARY MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. FURTHER, ISS DOES NOT WARRANT, GUARANTEE, OR MAKE ANY REPRESENTATIONS THAT THE SOFTWARE WILL BE FREE FROM BUGS, THAT ITS USE WILL BE UNINTERRUPTED, OR REGARDING THE USE, OR THE RESULTS OF THE USE, OF THE SOFTWARE OR OTHER ISS PROPRIETARY MATERIALS IN TERMS OF CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE. THE LICENSEE UNDERSTANDS THAT ISS IS NOT RESPONSIBLE, AND WILL HAVE NO LIABILITY, FOR HARDWARE, SOFTWARE, OR OTHER ITEMS OR ANY SERVICES PROVIDED BY ANY PERSON OTHER THAN ISS.

8. NO WARRANTIES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, ISS, ITS SUPPLIERS, DISTRIBUTORS AND RESELLERS DISCLAIM ALL OTHER WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH REGARD TO THE PRODUCT.

9. NO LIABILITY FOR CONSEQUENTIAL DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL ISS OR ITS SUPPLIERS, DISTRIBUTORS AND RESELLERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OF OR INABILITY TO USE THE PRODUCT, EVEN IF ISS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES AND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO THE LICENSEE.

10. CUSTOMER REMEDIES.

ISS' ENTIRE LIABILITY AND THE LICENSEE'S EXCLUSIVE REMEDY SHALL NOT EXCEED THE LICENSE FEES PAID FOR THE PRODUCT.

Revised January 8, 2002