INTERNET SECURITY SYSTEMS™

REALSECURE®

Desktop Protector User Guide

Version 3.5

Internet Security Systems, Inc.
6303 Barfield Road
Atlanta, Georgia 30328-4233
United States
(404) 236-2600
http://www.iss.net

June 2002

Contents

Preface

Overview

Introduction

This guide is designed to help you use RealSecure Desktop Protector to protect your local system and your network from unwanted intrusions.

Scope

This guide describes the features of RealSecure Desktop Protector and shows you how to use them.

- Chapter 1 explains how Desktop Protector protects your local system from attacks and unwanted intrusions.
- Chapter 2 provides information about using Desktop Protector to help ICEcap Manager manage network-wide security.
- Chapter 3 provides instructions for installing and configuring Desktop Protector on your computer.
- Chapter 4 provides detailed procedures for configuring Desktop Protector for your particular circumstances.
- Appendixes A through E describe the screens and dialog boxes you can use to control RealSecure Desktop Protector.

Audience

This guide is intended for network administrators responsible for installing and maintaining software on corporate systems.

What's new in this guide

This guide replaces the BlackICE Agent 3.0 User Guide. This guide includes information about a new layer of safety for your desktop, called Application Protection. Application Protection consists of two features:

- **Application Control.** Desktop Protector prevents unauthorized applications from running on your local system. This helps to keep potentially harmful software from compromising your security, even the software has been successfully installed on your computer.
- **Communications Control.** Desktop Protector blocks applications from contacting the Internet without your authorization. This prevents harmful Trojans from working even if they have been successfully installed on your local system.

Using this guide

Use this guide to help you configure and work with RealSecure Desktop Protector. To get the most effective protection possible, you can follow the steps provided in Chapter 3 to configure Desktop Protector. The instructions are designed to be followed in the order given, but you can skip any step without endangering your system.

Related publications

The following documents are available for download from the Internet Security Systems Web site at www.iss.net.

- For information about working with RealSecure Desktop Protector on a corporate network, see the *RealSecure ICEcap Manager User Guide.*
- For answers to questions about Desktop Protector, see *RealSecure Desktop Protector Frequently Asked Questions*.
- For system requirements for Desktop Protector, see *System Requirements.*
- For general information about Desktop Protector's features, see the *Product Spec Sheet*.

Conventions Used in this Guide

Introduction

This topic explains the typographic conventions used in this guide to make information in procedures and commands easier to recognize.

In procedures

The typographic conventions used in procedures are shown in the following table:

Convention	What it Indicates	Examples
Bold	An element on the graphical user interface.	Type the computer's address in the **IP Address** box. Select the **Print** check box. Click **OK**.
SMALL CAPS	A key on the keyboard.	Press ENTER. Press the PLUS SIGN (+).
`Constant width`	A file name, folder name, path name, or other information that you must type exactly as shown.	Save the `User.txt` file in the `Addresses` folder. Type `IUSR__SMA` in the **Username** box.
`Constant width italic`	A file name, folder name, path name, or other information that you must supply.	Type `Version` *`number`* in the **Identification information** box.
→	A sequence of commands from the taskbar or menu bar.	From the taskbar, select **Start→Run**. On the **File** menu, select **Utilities→Compare Documents.**

Table 1: *Typographic conventions for procedures*

Command conventions

The typographic conventions used for command lines are shown in the following table:

Convention	What it Indicates	Examples
`Constant width bold`	Information to type in exactly as shown.	**`md ISS`**
`Italic`	Information that varies according to your circumstances.	**`md`** *`your_folder_name`*
[ ]	Optional information.	**`dir`** [*`drive:`*] [*`path`*] [*`filename`*] [**`/P`**] [**`/W`**] [**`/D`**]
|	Two mutually exclusive choices.	**`verify`** [**`ON`**|**`OFF`**]
{ }	A set of choices from which you must choose one.	**`% chmod`** {**`u g o a`**}=[**`r`**] [**`w`**] [**`x`**] *`file`*

Table 2: *Typographic conventions for commands*

Getting Technical Support

Introduction

ISS provides technical support through its Web site and by email or telephone.

The ISS Web site

The Internet Security Systems (ISS) Resource Center Web site (http://www.iss.net/support/) provides direct access to much of the information you need. You can find frequently asked questions (FAQs), white papers, online documentation, current versions listings, detailed product literature, and the Technical Support Knowledgebase (http://www.iss.net/support/knowledgebase/).

Hours of support

The following table provides hours for Technical Support at the Americas and other locations:

Location	Hours
Americas	24 hours a day
All other locations	Monday through Friday, 9:00 A.M. to 6:00 P.M. during their local time, excluding ISS published holidays **Note:** If your local support office is located outside the Americas, you may call or email the Americas office for help during off-hours.

Table 3: *Hours for technical support*

Contact information

The following table provides email addresses and telephone numbers for technical support requests:

Regional Office	Email Address	Telephone Number
North America and Latin America	support@iss.net	(1) (888) 447-4861 (toll free) (1) (404) 236-2700
Europe, Middle East, and Africa	support@iss.net	(44) (118) 959-3900
Asia-Pacific and Philippines	asia-support@iss.net	(63) (2) 886-6014
Japan	support@isskk.co.jp	Domestic: (81) (3) 5740-4065 Overseas (APAC): (81) (3) 5740-4066

Table 4: *Contact information for technical support*

Chapter 1

Introduction to RealSecure Desktop Protector

Overview

Introduction

RealSecure Desktop Protector is a comprehensive security solution that helps you protect your system and your network from the following:

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

This chapter describes the basic concepts of RealSecure Desktop Protector.

In this chapter

This chapter contains the following topics:

ICEcap integration

RealSecure Desktop Protector integrates with ICEcap Manager management and reporting console. Desktop Protector forwards information about the events it detects to a server running ICEcap Manager for enterprise-wide security reporting and analysis. ICEcap Manager can in turn install and update Desktop Protector remotely.

Firewall capabilities

RealSecure Desktop Protector provides powerful firewall capabilities, and provides much more than traditional firewall functionality. The Desktop Protector firewall inspects all

inbound and outbound traffic on your system for suspicious activity. Desktop Protector blocks unauthorized activity without affecting normal traffic.

Intrusion detection

RealSecure Desktop Protector contains an intrusion detection system that alerts you to attacks and blocks threats to your system. Desktop Protector captures information about the attacker and logs suspicious activity, which preserves evidence of the attack.

Application protection

RealSecure Desktop Protector prevents unauthorized applications from harming your system or other computers on a network. Application protection consists of two features:

- **Application Control**: Helps you prevent unknown and possibly destructive applications from damaging your system. When you suspect an application may have been modified, Application Control lets you decide whether to let it start. RealSecure Desktop Protector goes beyond the capabilities of other products by preventing unauthorized applications from starting other applications or services.
- **Communications Control**: Helps you prevent unauthorized applications from communicating on the Internet. This can even prevent intruders from using your system to start attacks against other systems. It does this by letting you control which applications have access to a local network or the Internet.

Protection Levels

Introduction

Protection levels are pre-designed sets of security settings developed for different types of Web use. You can choose to have Desktop Protector block all communications with your system, some communications with your system, or no communications with your system. You can change protection levels at any time.

How protection levels work

Protection levels modify your firewall by closing some of the software links, or *ports*, that your system uses to receive communications from other computers. The more restrictive the protection level, the more ports are blocked.

Protection level definitions

Paranoid: Desktop Protector blocks all unsolicited inbound traffic. Very restrictive, but useful if your system faces frequent or repeated attacks. This setting may restrict some Web browsing and interactive content.

Nervous: Desktop Protector 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). Preferable if you are experiencing frequent intrusions.

Cautious: Desktop Protector blocks unsolicited network traffic that accesses operating system and networking services. Good for regular use of the Internet.

Trusting: All ports are open and unblocked and all inbound traffic is allowed. Acceptable if you have a minimal threat of intrusions. This is the default protection level setting. If your local agent is not centrally controlled by ICEcap Manager, you should consider customizing your protection level immediately after installing Desktop Protector.

How protection levels affect applications

This table shows how the protection levels affect some representative applications:

Level	Blocked	Configurable	Not Blocked
Paranoid	IRC file transfer (DCC) NetMeeting PC Anywhere ICQ	Quake (II/III) Internet Phone Net2Phone	FTP file transfers Sending/receiving email Real Audio IRC Chat
Nervous	IRC file transfer (DCC) NetMeeting	ICQ Internet Phone Net2Phone	All of the above, plus PC Anywhere, Quake (II,III)
Cautious	Unsolicited traffic that accesses operating system and networking services	None	All of the above, plus IRC file transfer (DCC) NetMeeting
Trusting	None	None	All inbound traffic

Note: To use an application that is blocked under a selected protection level, use the Advanced Firewall Settings feature to open the ports the application uses. For more information on opening ports, see "Blocking Intrusions" on page 37.

Adaptive Protection

Introduction

Adaptive Protection automatically adapts each agent's security level according to the type of network connection it is using. For example, you can set Adaptive Protection to use a more restrictive security level when users are logged on over a VPN, and a less restrictive security level when users are logged directly onto the network.

When to use adaptive protection

You may need to connect to your corporate network from inside your corporate headquarters, from your home office, or from the floor of a trade show. For example:

- Inside your corporate office, your firewall is automatically set to the Trusting protection level.
- At your home office, your firewall is set to Cautious for most communications. It switches to Trusting when you connect to your corporate network over a VPN, and switches back to Cautious when the VPN connection closes.
- At a trade show, your firewall automatically switches to Paranoid when you plug into the conference network. It switches to Trusting when you connect to your corporate VPN, and then switches back to Paranoid when the VPN connection closes.

Note: Adaptive protection settings are usually sent down to a local agent from ICEcap Manager. Use these instructions on your local agent only if your ICEcap administrator recommends it. Your ICEcap administrator may also provide you with the correct IP addresses to use.

For information about configuring Desktop Protector to switch protection levels dynamically, see “Using Adaptive Protection” on page 35.

For detailed information about setting your protection preferences, see “The Firewall Tab” on page 70.

The Desktop Protector Firewall

Introduction

Desktop Protector automatically stops most intrusions according to the protection level you have chosen, but you still may notice activity that isn't explicitly blocked. You can configure the Desktop Protector firewall to increase your protection. You can block intrusions from a particular address, or you can block intrusions that use a particular protocol.

Protocol analysis

The Desktop Protector firewall works by recognizing the special languages computers use to communicate. For example, your browser receives messages encoded in Hypertext Transfer Protocol (HTTP) from the Web. These information packets are usually received through port 80. When Desktop Protector detects traffic coming in through port 80 that is not correctly encoded in HTTP packets, there may be cause for suspicion.

Dynamic Firewall

Your firewall uses information from the BlackICE intrusion detection engine to reconfigure itself in response to intrusions. The intrusion detection component analyzes unusual packets and, if they are dangerous, instantly configures the firewall to block them before they can have any effect on your system.

Blocking an intruder

You can block any intruder listed on your events list by adding an IP address to your firewall. When you do this, no traffic from that intruder's IP address can enter your system. For information about blocking IP addresses, see “Blocking an IP address” on page 37.

Blocking a port

If you don't have an intruder in mind but you are concerned about intrusion attempts using a specific internet protocol, you can block the port (or ports) that protocol uses. Adding a port entry to your firewall ensures that no traffic from any IP address can enter your system using that port. For information about blocking ports, see “Ignoring Events” on page 40.

Ignoring events

To help reduce the amount of information you have to deal with, you can choose to ignore events that don't pose any threat to your system. For example, your company’s Information Services department may carry out routine port scans for network management purposes. When such a scan appears on your events list, you can right-click the event and select Ignore. For information about ignoring events, see “Ignoring Events” on page 40.

Trusting an address

When you know a particular IP address is safe, you can choose to ignore all events from that address. This is called *trusting* an address. For example, when another computer on your internal network accesses files on your system, it can appear as an intrusion on your events list. You can right-click these events and select **Trust** and **Accept** to tell Desktop Protector not to record any events from that computer. For information about trusting and accepting, see “Trusting Intruders” on page 39.

Application Protection

Introduction

BlackICE protects your computer from unknown applications and from applications connecting to a network, such as the Internet.

How the baseline works

First, BlackICE creates a baseline record (also known as a checksum) of the applications installed on your computer. Then it compares that baseline with any application that attempts to launch or to communicate with a network. If the application does not match the baseline, then BlackICE asks you if you want to stop the application or let it continue.

Note: You must update the baseline whenever you make changes to your system, such as upgrading an application or installing a new application.

Turning off Application Protection

To turn off the Application Protection component:

1. Click **Tools→ Edit BlackICE Settings.**
2. Select either the Application Control tab or the Communications Control tab.
3. Clear the **Enable Application Protectio**n check box.

Adding new or upgraded applications to your computer

Whenever you upgrade an application or install a new application on your computer, the application does not match the Application Protection baseline, so BlackICE regards it as an unknown application. This protects you from someone maliciously updating applications with or replacing them with other files that may be harmful.

Avoiding alert messages when you install software

You can avoid warning messages during upgrade or installation by clicking **Install Mode Options → Enable Install Mode** on the first message you see. This temporarily disables Application Protection. Click **Continue** on the periodic messages until the upgrade or installation ends. Be sure to disable install mode when you are finished.

Note: After you install or upgrade an application, you must add it to the baseline. For information about updating your baseline to include your new or upgraded software, see "Managing your authorized applications" on page 44.

Application Control

Introduction

RealSecure Desktop Protector lets you control which applications and related processes can run on your system. Sometimes a program may be installed on your system without your knowledge. Many of these programs are useful or harmless. However, some of these programs can present security risks. They may allow an intruder to locate password information, make the system more vulnerable to future entry, or destroy programs or data on the hard disk.

How Application Control works

When Application Protection is enabled on your system, it creates a list of currently installed applications.Whenever the computer begins to start an application, Desktop Protector checks that the application is one of these known applications. You can control this default behavior by changing the settings on the Application Control tab.

Example: spyware

For example, some installation programs install a separate application on your system to track your Web site visits (commonly known as spyware). Desktop Protector detects the application when it starts, and checks to see if you have authorized the application to run. If not, Desktop Protector can close the program automatically or alert you, depending on the Application Control options you have set.

Application control is not virus detection

Application control is not the same as virus detection. Desktop Protector does not search your system for harmful applications. Instead, Desktop Protector watches for new applications that may have been installed on your system since the last time Application Protection searched for new or altered applications, and alerts you when they start. For example, if you install Desktop Protector after a Trojan application has been installed on your computer, Desktop Protector assumes the application is known to you and does not block it from starting or contacting a network.

Important: To get the full benefit of Application control, scan your system for viruses with an anti-virus program to make sure it is free of dangerous applications before you install Desktop Protector or have Desktop Protector search for new or modified applications. It is a good idea to run your anti-virus scan in both normal and safe mode.

More information

For instructions, see “Working with the Application Protection Baseline” on page 42.

Communications Control

Introduction

To reduce security risks from potential "Trojan horse" applications on your system, RealSecure Desktop Protector lets you choose which applications or processes can access a network, such as the Internet or a local area network.

How Communications Control works

Desktop Protector tracks all the applications (and related processes) that you authorize to access a network from your system. If any software installed on your system attempts to access a network without your authorization, Desktop Protector detects its outbound transmissions and asks you what to do:

- If you recognize the application, you can allow it to continue or you can block it.
- If you block it, you can have Desktop Protector automatically block the application in the future.

Example: auto-update

For example, some applications include a feature that automatically checks the application provider's Web site for software updates. The first time a newly installed or modified program tries to do this, Desktop Protector asks if you want this application to access the network. You can control this behavior by altering the settings on the Communications Control tab.

More information

For instructions, see "Configuring Communications Control" on page 46.

Desktop Protector Alerts

Introduction

Your dynamic firewall handles most alerts for you, but you can take additional steps to make its responses even more effective. The information in this topic may help you determine which events merit your attention.

Severity levels

Some network events are more dangerous than others. Desktop Protector assigns each event a numerical rank that reflects the event's potential risk level, and reports that rank with an icon on the Events tab. The following table lists the severity levels Desktop Protector uses:

Icon	Rank	Description
	7-10	**Critical**. These are deliberate attacks on your system for the purpose of damaging data, extracting data, or crashing the system. Critical events always trigger protection measures.
	4-6	**Serious**. These are deliberate attempts to access information on your system without directly damaging anything. Some serious events trigger protection measures.
	1-3	**Suspicious**. These are network activities that are not immediately threatening, but may indicate that someone is attempting to locate security vulnerabilities in your system. For example, intruders may scan the available ports or services on a system before attacking it. Suspicious events do not trigger protection measures.
	0	**Informational**. These are network events that are not threatening but worth noting. Informational events do not trigger protection measures.

Table 5: *Desktop Protector severity icons*

Response levels

Desktop Protector reports how it responded to each event by showing a symbol. The symbol for a response can appear two ways:

- as an icon beside the event
- as a mark over the severity level icon

This table describes Desktop Protector response level icons and overlays:

Icon	Overlay	Description
		**Attack Blocked**: Desktop Protector successfully blocked the attack. Depending on the severity of the event, Desktop Protector may also have blocked the attacking system. To see if Desktop Protector is currently blocking the intruder, double-click the event.
		**Attack Unsuccessful**: Other defenses of your system, such as the operating system, successfully blocked the intrusion. Therefore, Desktop Protector did not need to block the event. The event did not compromise the system.
		**Attack Status Unknown**: Desktop Protector triggered protection measures as soon as it identified the attack, but some attacking packets may have made it through to the computer. It is unlikely that the event compromised the system.
		**Attack Possible**: Desktop Protector triggered protection measures as soon as it identified the intrusion. However, some attacking packets were able to get into the computer. The event may have compromised the system.
		**Attack Successful**: Desktop Protector detected abnormal traffic entering or exiting the system as a result of the intrusion. However, the Desktop Protector protection measures could not block the intrusion. The event has compromised the system.

Table 6: *Desktop Protector response icons and overlays and what they mean*

Collecting Information

Introduction

When an intruder attempts to break into your system, RealSecure Desktop Protector can track the intruder's activities. You can use this information to determine what an intruder did to your computer. This section explains how to gather and use this information.

Back Tracing

Desktop Protector can back trace each intrusion to determine where it originated. You can tell Desktop Protector to seek information from the originating computer itself or from points the packets passed through on the way to your computer.

When Desktop Protector back traces an intruder, it attempts to gather the IP address, DNS name, NetBIOS name, Node, Group name, and MAC address. Skilled intruders will often block Desktop Protector from acquiring this information.

To set up back tracing, see "Introduction" on page 50 and "The Back Trace Tab" on page 76.

Evidence files

RealSecure Desktop Protector can capture network traffic attributed to an intrusion and place that information into an evidence file. Desktop Protector captures and decodes each packet coming into the system, so it can generate files that contain detailed information about the intruder's network traffic.

To an experienced network engineer, evidence files show exactly what the intruder did or attempted to do. Because evidence files provide proof of the attacker's activities, this can be very useful to law enforcement or legal counsel in tracking criminal intruders.

For information about setting up evidence gathering, see "Collecting Evidence Files" on page 52.

Packet log files

Packet logging records all the packets that enter your system. This can be useful if you need more detailed information than evidence logs contain. Packet logs can become very large and use considerable hard disk space. However, if you are experiencing repeated intrusions on a system, packet logging can help gather additional information about activity on the system.

For information about setting up packet logging, see "Collecting Packet Logs" on page 54.

Filtering Information

Introduction

You probably won't need to inspect all the information RealSecure Desktop Protector gathers about the Internet traffic that reaches your system. You can use the configuration tabs to control how much information appears on the information tabs and how often Desktop Protector alerts you to potential risks.

You can instruct Desktop Protector to show only events that present risks over a given level. For example, Desktop Protector determines port scans from your ISP to be of only informational interest. You can omit those events from the Events tab. For information on how to do this, see "Filtering the Events List" on page 48.

Severity levels

Desktop Protector assigns a severity level to every event, to indicate how dangerous the event may be to your system. The severity level appears as an icon beside the event on the Events tab.

Freezing events

Sometimes events are recorded so quickly that it can be difficult to keep 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. For information on freezing the Events list, see "Freezing the Events list" on page 49.

Deleting events

Even if you are filtering out events that are not very risky, your events list can grow very long. You can delete individual events from the Events tab, or you can delete the whole events list. For information about deleting events, see "Clearing the Events list" on page 48.

Event alerts

Desktop Protector can alert you to events by making a sound or by showing an alert icon in your system tray. The alert icons are coded to match the seriousness of the event. You can tell Desktop Protector to alert you only to events of a particular severity. For information about setting your alarm preferences, see "Setting alarm preferences" on page 48.

Customizing event and intruder information

You can configure the Events and Intruders tabs to show only the columns that contain the information you are most interested in. For example, if you find that multiple attacks on your system use the same protocol, you can include the Protocol column in the Events tab. For information on choosing columns to view, see "Showing and hiding columns" on page 49.

Chapter 2

Using RealSecure Desktop Protector with ICEcap Manager

Overview

Introduction

RealSecure Desktop Protector interacts with the ICEcap management and reporting console to provide enterprise-wide security monitoring and management. This chapter provides the background knowledge required for setting up connections between Desktop Protector and ICEcap Manager from your system.

For more detailed information about using RealSecure Desktop Protector with ICEcap Manager, see the *RealSecure ICEcap Manager User Guide*.

In this chapter

This chapter contains the following topics:

How ICEcap Manager Works With RealSecure Desktop Protector

Introduction

ICEcap Manager interacts with agents in two ways:

- **Collecting and managing information.** As each RealSecure agent detects events, it forwards information about those events to the ICEcap server. ICEcap Manager stores and logs the events for enterprise-wide security reporting and analysis.
- **Installing, updating and controlling remote agents.** ICEcap administrators can use ICEcap Manager to control the configuration of all RealSecure agents on the network. This provides a central platform for standardizing security settings across the enterprise.

Independent operation

ICEcap Manager and RealSecure Desktop Protector work independently from one another. If either the agent or ICEcap Manager is offline or unavailable, the other system continues working without interruption. RealSecure Desktop Protector and ICEcap Manager interact only when an event or a configuration issue occurs.

This table identifies the possible interactions between RealSecure Desktop Protector and ICEcap Manager:

Interaction	Description	Initiated by:
Event Reporting	When configured to report to an ICEcap Manager, Desktop Protector reports information about each event.	Desktop Protector
Configuration Updates	ICEcap Manager issues instructions to Desktop Protector to update security settings. **Note**: Only ICEcap Manager can issue configuration updates. While end-users may be able to configure their local installation of Desktop Protector, this configuration information is stored locally. It is not transmitted to ICEcap Manager.	ICEcap Manager
Software Updates	ICEcap Manager installs files on the remote agent to add RealSecure functionality. **Note**: Only ICEcap Manager can distribute software updates. Local RealSecure agents cannot update other systems.	ICEcap Manager

Table 7: *Interactions between ICEcap Manager and the agent*

Control levels

By default, ICEcap Manager has total control over all agents, allowing modification only to display and event notification preferences. However, ICEcap administrators can configure groups to allow agents partial local control or almost complete local control.

The control level can be set only from ICEcap Manager, as part of a policy applied to an ICEcap group and pushed to the remote agents in the group. An end user cannot choose a control level from the local Desktop Protector interface.

Note: RealSecure agents that include the Local Console can have any level of configuration sharing, whether they are remotely installed from ICEcap Manager or

locally installed. Silent Desktop Protector installations are always completely ICEcap-controlled. For more information about silent agent installations, see the *RealSecure ICEcap Manager User Guide*.

This table summarizes the levels of control ICEcap Manager can exert over an agent.

Control Level	Result
Total ICEcap Control	ICEcap Manager has complete control over these agents. If the local host has the Local Console installed, the end user can modify the display and alarm preferences but not the blackice.ini or firewall.ini files. Configuration settings are disabled.
Shared ICEcap Control	The local system has partial control over configuration settings, and can alter any parameters that ICEcap Manager has not explicitly set. For example, the user can trust an address that ICEcap Manager does not trust. However, the user cannot unblock an ICEcap-blocked address or change the protection level ICEcap Manager enforces.
Shared Local Control	The local system has control over all configuration settings. Although ICEcap Manager distributes configuration settings to all agents in the group, the end user can override any of those configuration settings.

Table 8: *Levels of local or remote control of the local agent*

What level of control is in effect?

The ICEcap control level determines what you can do with the firewall and Application Protection components of Desktop Protector on your computer.

To see what level of control ICEcap Manager has over Desktop Protector on your computer:

1. From the Main Menu, select **Tools → Edit BlackICE Settings.**
2. Is the **Enable local configuration editing** checkbox visible?
   - If *yes*, you have some degree of control over Desktop Protector on your system.
   - If *no*, ICEcap Manager has total control of the agent on your system.
3. Which option is selected under Configuration Priority?
   - **Remote**: the local agent is under shared ICEcap Control. You can alter any parameters that ICEcap Manager has not explicitly set.
   - **Local**: the agent is under shared local control. You can override any parameters ICEcap Manager has set.

How ICEcap Manager Handles Information

Introduction

To help organize information, ICEcap Manager categorizes agents and the events they report into *accounts* and *groups*. To report an event, a RealSecure agent must be assigned to a group within an ICEcap account.

Accounts

Accounts represent significant divisions or organizational elements within the company. For example:

- A manufacturing company's sales division might constitute one account while its factory operations might constitute another.
- A European corporation might establish one account for its facilities in France and another for its British operations.
- A financial services company might create one account for its trading floor and a separate account for its back-office processing operations.

For more information about creating and using accounts, see the *RealSecure ICEcap Manager User Guide*.

Groups

Groups are logical collections of systems (also known as hosts) organized for modular reporting and configuration. Each account consists of one or more groups. For example, a single account might include a group for all the servers on a network and a group for all the end-user workstations. Each group belongs to only one account. An agent can report into only one group.

Assigning an agent to a group

ICEcap Manager is solely responsible for assigning agents to groups. Although agents can report a group name, ICEcap Manager must authorize that name and make the appropriate assignment.

The first time an agent reports an event, ICEcap Manager assigns the agent to a group by *IP address assignment* or by *group name assignment*. For more information about this authorization process, see the *RealSecure ICEcap Manager User Guide*.

Changing groups

Agents cannot alter their group assignment.You can change the group name on the ICEcap tab in the BlackICE Settings, but the change takes effect only if ICEcap Manager authorizes the change. This prevents intruders from reassigning an agent to a group with less restrictive settings. Consult the *RealSecure ICEcap Manager User Guide* for more information about change agent group assignments.

Working with VPN and dial-up users

VPN and dial-up users present unique challenges for managing remote agent software.

- Some VPN users cannot be reliably grouped by IP address because they have dynamic IP addresses. Desktop Protector may report the remote user's ISP- assigned IP address and not the local network address.
- Mobile computers that are connected to the internal network while in the office, but dial into the network while on the road, can have many different IP addresses.

To handle this situation, it is a good idea to create a group exclusively for dial-up or VPN users in the appropriate account, using group name precedence. For information on how to create a remote users' group, see the *RealSecure ICEcap Manager User Guide*.

Transmitting Data to ICEcap Manager

Introduction

Desktop Protector must be able to transmit data across your network to the ICEcap server. Agents can report to the ICEcap server by one of three methods:

- over the Internet
- over a Virtual Private Network
- through a proxy server

Reporting over the Internet

Reporting over the Internet is safe, but not without risks. Communications from RealSecure agents are encrypted, and ICEcap Manager requires an account name and password to submit data.

Reporting over a VPN

VPN connections using the point-to-point tunneling protocol encrypt packets sent over the Internet, adding an additional layer of security between remote systems and ICEcap Manager.

Reporting through a proxy server

RealSecure agents can also be configured to report events through a proxy server.

Installing Desktop Protector Remotely

Introduction

In addition to managing event information, ICEcap Manager can install Desktop Protector software on remote systems. This can include systems with the Local Console or "silent" installations that include only the monitoring and protection engine.

Remote installations of Desktop Protector must be carried out from ICEcap Manager. For additional information about setting up and executing remote installations, see the *RealSecure ICEcap Manager User Guide*.

Note: If a Desktop Protector version already exists on a target system, ICEcap Manager does not reinstall Desktop Protector when a remote installation is executed. To reinstall Desktop Protector, the software must be manually or remotely removed first and then reinstalled.

Using ICEcap Manager to Control RealSecure Agents

Introduction

ICEcap Manager manages agents by applying policies to groups of agents. Any configuration change made to a group is distributed to all the members of that group. This reduces the effort required to support remotely installed systems.

Pushing to agents

To modify the configuration of agents on the network, you can make the changes on the ICEcap server and have ICEcap Manager push those changes to all agents in one or more groups. This ensures that all members of a group share the same configuration.

How ICEcap Manager communicates with agents

ICEcap Manager and Desktop Protector communicate with each other using encrypted HTTP packets. Both Desktop Protector and ICEcap Manager can transmit these packets through a proxy server.

Although ICEcap Manager initiates configuration updates and software updates, the local agents actually download the files from ICEcap Manager. This prevents intruders from "pushing" unauthorized security settings to agents.

Note: ICEcap Manager does not maintain a link to all the agents on the network. Each individual system reports events to the ICEcap server.

Criteria for ICEcap control

For ICEcap Manager to assume total or partial control of an agent, the agent must meet these criteria:

- The remote system must belong to one ICEcap group.
- A policy must be associated with that group.

If a system belongs to a group, but that group does not have a policy associated with it, ICEcap Manager cannot make any configuration changes on the remote system. Software updates are distributed to the agents, but configuration settings are not.

Important: ISS recommends that each group have a properly configured policy. This ensures that configuration settings are standardized on ICEcap Manager.

Chapter 3

Setting Up RealSecure Desktop Protector

Overview

Introduction

This chapter provides instructions for installing and configuring RealSecure Desktop Protector locally. For information about installing Desktop Protector from ICEcap Manager, see the *RealSecure ICEcap Manager User Guide*.

In this chapter

This chapter contains the following topics:

Installing RealSecure Desktop Protector

Introduction

This topic gives instructions for installing Desktop Protector.

Local or remote installation

You can install RealSecure Desktop Protector locally at your agent computer or remotely from RealSecure ICEcap Manager. In most cases, you should distribute Desktop Protector to network systems from ICEcap Manager. This allows centralized control of configuration. However, in some cases it may be quicker to install an agent manually.

For information about installing remotely with RealSecure ICEcap Manager, see the *RealSecure ICEcap Manager User Guide*.

Manual ICEcap configuration

When Desktop Protector is installed directly on an agent computer, you must manually configure the ICEcap settings. When Desktop Protector reports to ICEcap Manager, any configuration and protection settings attributed to the agent's account and group are distributed to the agent.

Note: Manual installations of RealSecure Desktop Protector always include the local user interface. Only ICEcap Manager can create and distribute agents without the local user interface, known as "silent" agents. For information about installing silent agents, see the *RealSecure ICEcap Manager User Guide*.

Prerequisites

Before you install RealSecure Desktop Protector, you must do the following:

- Scan your system for viruses.
- Disable the real-time scanning function of any anti-virus detection software on your system to avoid unwanted interactions during the installation.

Procedure

To install RealSecure Desktop Protector, follow these steps:

4. Are you installing Desktop Protector from the CD?
   - If *yes*, go to Step 5.
   - If *no*, locate the directory to which you downloaded Desktop Protector, and then go to Step 6.

   If you have lost your original copy of the software, you can download a new copy from the Internet Security Systems Web site at `www.iss.net`.
5. Insert the CD in the CD-ROM drive.
6. Double-click `RSDPSetup.exe`.
7. In the Install Wizard, click **Next**.

   If the setup program detects an existing version of Desktop Protector, the program prompts you to uninstall or upgrade the existing version.
   - To update Desktop Protector, click **Next**.
   - To remove Desktop Protector from your hard drive, follow the instructions in "Uninstalling Desktop Protector" on page 28.

8. Read the End User License Agreement.
   - If you accept the End User License Agreement, click **I Accept**, and then go to Step 9.
   - If you do not accept the End User License Agreement, click **I Decline**.

   The setup program exits.
9. Enter the license key provided by your ICEcap administrator.

   Each agent must have a license key installed. Depending on your ICEcap Manager purchase agreement, you may need to update this key to ensure that the software continues to run.

   Note: For information about handling license keys from ICEcap Manager, see the *RealSecure ICEcap Manager User Guide*.
10. Click **Next**.
11. In the Select Program Folder window, select a location for the Desktop Protector shortcuts folder on the Windows Start menu.

    Important: The setup application places a shortcut in the Startup folder automatically. Do not place Desktop Protector shortcuts in the Startup folder yourself.
12. Click **Next**.
13. Will this computer report events to an ICEcap Manager?
    - If *yes*, select **Enable ICEcap Reporting,** and then enter the applicable information.
    - If *no*, go to Step 19.
14. Enter the fully qualified URL for the ICEcap server. Include the port number.

    The default event reporting port is 8082. For example, if ICEcap Manager is on a server at the address 192.168.0.101 using event port 8082, enter `http://192.168.0.101:8082`.

    Important: You can enter the machine name of the ICEcap server, but it is preferable to use its IP address.
15. Enter ICEcap Manager Account this computer is assigned to.
16. Enter the account password.
17. Enter the name of the Group this computer is assigned to.

    Note: ICEcap Manager must authorize this group name assignment. See the *RealSecure ICEcap Manager User Guide* for more information about group assignments.
18. If there is a proxy server between this computer and the ICEcap server, enter the URL or IP address in the **Proxy URL** field. Leave the default, auto, if you are unsure or there is no proxy server.
19. Click **Next**.
20. Do you want to read the Release Notes?
    - If *yes*, go to Step 21.
    - If *no*, clear the **I would like to view the README file** checkbox.

    Note: If you are installing this version of RealSecure Desktop Protector for the first time, ISS recommends that you read the Release Notes.
21. Click **Finish**.

    The Desktop Protector service starts.

Stopping Desktop Protector

Introduction

When you quit the Desktop Protector application, Desktop Protector does not stop monitoring your system. To stop Desktop Protector from monitoring for intrusions and to stop protecting your system against unknown or modified applications, you must stop the BlackICE intrusion detection and application protection features.

Note: Stopping Desktop Protector is not the same as removing it. For information about removing RealSecure Desktop Protector, see "Uninstalling Desktop Protector" on page 28.

Stopping Desktop Protector from the console

To stop Desktop Protector from the Desktop Protector window:

1. From the Main Menu, click **Tools→ Stop BlackICE Engine**.

   Desktop Protector stops monitoring incoming traffic and a red line appears over the Desktop Protector icon. 
2. From the Main Menu, click **Tools→ Stop BlackICE Application Protection**.

   Desktop Protector stops monitoring your system for unauthorized applications and outgoing transmissions.

Stopping Desktop Protector from the desktop

To stop Desktop Protector from the desktop:

1. Right-click the Desktop Protector icon. 
2. Select **Stop BlackICE Engine**.

   Desktop Protector stops monitoring incoming traffic and a red line appears over the Desktop Protector icon. 
3. Right-click the Desktop Protector icon.
4. Select **Stop BlackICE Application Protection**.

   Desktop Protector stops monitoring your system for unauthorized applications and outgoing transmissions.

Stopping Desktop Protector from the control panel (Windows NT)

To stop Desktop Protector 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**.

   Desktop Protector stops monitoring incoming traffic and a red line appears over the Desktop Protector icon. 
4. Select **RapApp**, and then click **Stop**.

   Desktop Protector stops monitoring your system for unauthorized applications and outgoing transmissions.

Stopping Desktop Protector from the control panel (Windows 2000)

To stop Desktop Protector 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**.

   Desktop Protector stops monitoring incoming traffic and a red line appears over the Desktop Protector icon. 
5. In the right pane, right-click **RapApp**, and then select **Stop**.

   Desktop Protector stops monitoring your system for unauthorized applications and outgoing transmissions.

Stopping Desktop Protector from the control panel (Windows XP)

To stop Desktop Protector from the Windows XP control panel:

1. Click **Start→ Settings →Control Panel**.
2. Double-click **Performance and Maintenance**.
3. Double-click **Administrative Tools**.
4. Double-click **Services**.

   The Services window appears.
5. In the right pane, right-click **BlackICE**, and then select **Action→ Stop**.

   Desktop Protector stops monitoring incoming traffic and a red line appears over the RealSecure Desktop Protector icon. 
6. In the right pane, right-click **RapApp**, and then select **Action→ Stop**.

   Desktop Protector stops monitoring your system for unauthorized applications and outgoing transmissions.

Restarting Desktop Protector

Introduction

You can restart RealSecure Desktop Protector after you have stopped it, or you can let Desktop Protector restart automatically when you restart your computer.

Note: Opening the Desktop Protector window does not make Desktop Protector resume monitoring your system. To restart intrusion protection after stopping it manually, you must follow one of the following procedures or restart your computer.

Restarting Desktop Protector from the main window

To restart Desktop Protector from the Desktop Protector window:

1. From the Main Menu, click **Tools→ Start BlackICE Engine**.

   Desktop Protector resumes monitoring incoming traffic. The red line disappears from the Desktop Protector icon.
2. From the Main Menu, click **Tools→ Start BlackICE Application Protection**.

   Desktop Protector resumes monitoring your system for unauthorized applications and outgoing transmissions.

Restarting Desktop Protector from the desktop

To restart Desktop Protector from the desktop:

1. Right-click the Desktop Protector icon.
2. In the pop-up menu, select **Start BlackICE Engine**.

   Desktop Protector resumes monitoring incoming traffic. The red line disappears from the Desktop Protector icon.
3. Right-click the Desktop Protector icon.
4. In the pop-up menu, select **Start BlackICE Application Protection**.

   Desktop Protector resumes monitoring your system for unauthorized applications and outgoing transmissions.

Restarting Desktop Protector from the control panel (Windows NT)

To restart Desktop Protector 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**.

   Desktop Protector resumes monitoring incoming traffic. The red line disappears from the Desktop Protector icon.
4. Select **RapApp**, and then click **Start**.

   Desktop Protector resumes monitoring your system for unauthorized applications and outgoing transmissions.

Restarting Desktop Protector from the control panel (Windows 2000)

To restart Desktop Protector 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**.

   Desktop Protector resumes monitoring incoming traffic. The red line disappears from the Desktop Protector icon. 

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

   Desktop Protector resumes monitoring your system for unauthorized applications and outgoing transmissions.

Restarting Desktop Protector from the control panel (Windows XP)

To restart Desktop Protector from the Windows XP control panel:

1. Click **Start→ Settings→ Control Panel**.
2. Double-click **Performance and Maintenance**.
3. Double-click **Administrative Tools**.
4. Double-click **Services**.

   The Services window appears.

5. In the right pane, right-click **BlackICE**, and then select **Action→ Start**.

   Desktop Protector resumes monitoring incoming traffic. The red line disappears from the Desktop Protector icon. 

6. In the right pane, right-click **RapApp**, and then select **Action→ Start**.

   Desktop Protector resumes monitoring your system for unauthorized applications and outgoing transmissions.

Restarting Desktop Protector by restarting your system

When you restart your system, Desktop Protector automatically resumes monitoring your system, unless you have disabled Application Protection. For information about disabling Application Protection, see "Disabling Application Protection" on page 45.

Uninstalling Desktop Protector

Introduction

You can remove Desktop Protector from your computer using the Windows Add/Remove Programs Utility or the BlackICE Agentremove utility.

Important: Use the `agentremove.exe` utility only if you are unable to remove Desktop Protector through the Windows Add/Remove utility. This utility removes the user interface component (`blackice.exe`), the application protection component (`rapapp.exe`), and the intrusion detection engine (`blackd.exe`).

Note: When you uninstall Desktop Protector, the local system is no longer protected from intrusions.

Record your license key

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

Uninstalling Desktop Protector from the Windows control panel

To uninstall Desktop Protector in Windows:

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**.

   The uninstall program asks you if you want to delete the configuration settings that control RealSecure Desktop Protector on this computer.
5. Do you intend to reinstall Desktop Protector?
   - If *yes*, keep the files that contain settings you will continue to use. To keep a file, leave its checkbox selected.
   - If *no*, clear all the checkboxes.

   You can decide to delete or keep the following files:
   - `firewall.ini`: This file contains any firewall entries you have added to protect against specific events or intruders. If you have customized your local firewall settings, you may want to keep this file for later use.
   - `blackice.ini`: This file contains the settings that determine how your local Desktop Protector user interface behaves. If you have configured Desktop Protector alerts or visual or sound feedback and would like to use the same settings when you reinstall Desktop Protector, you may want to keep this file.
   - `sigs.ini`: This file contains information about intrusion types for the BlackICE intrusion detection component to watch for. If you have added any signatures to the default signature database, you may want to keep this file for later use.
   - `protect.ini`: This file contains the instructions that determine how Desktop Protector handles unknown applications and unauthorized network access. If you have customized these settings, you may want to keep this file.
6. Click **Next**.

7. Do you want to remove the remaining intrusion files and delete the directory?
   - If *yes*, click **Yes**.
   - If *no*, click **No**.
8. Click **Finish**.

   The system removes Desktop Protector from your system.

Uninstalling Desktop Protector using the agentremove.exe utility

To remove Desktop Protector using the `agentremove` utility:

1. Locate the `agentremove.exe` file on the ISS CD or in the BlackICE folder on your system drive.
2. Double-click `agentremove.exe`.

   The system starts the `agentremove.exe` utility.
3. Delete the BlackICE directory from your system.

Chapter 4

Configuring RealSecure Desktop Protector

Overview

Introduction

This chapter provides the procedures to configure RealSecure Desktop Protector for your specific conditions. These procedures are designed to be performed in sequence.

In this chapter

This chapter includes the following topics:

Connecting to ICEcap Manager

Introduction

RealSecure Desktop Protector interacts with ICEcap Manager management and reporting console to provide enterprise-wide security monitoring and management. If ICEcap Manager application has granted local control, you can use the ICEcap tab to manually configure how Desktop Protector reports intrusion information to an ICEcap server.

Procedure

To configure the local Desktop Protector agent to report to ICEcap Manager and receive updates from ICEcap Manager:

1. On the Main Menu, select **Tools → Edit BlackICE Settings.**
2. Select the ICEcap tab.
3. Is **Enable local configuration editing** selected?
   - If *yes*, go to Step 4.
   - If *no*, you cannot change any settings from the local agent. Contact your ICEcap administrator.
4. Select **Reporting enabled**.
5. In the **URL** text box, enter the fully qualified URL of the ICEcap server in the format `http://<ICEcap server name>:<HTTP event port number>`. For example, if ICEcap Manager is on a server named ICECAP using event port 8082 (the default), enter `http://ICECAP:8082`. You can use the ICEcap server's IP address or DNS name.
6. In the **Account Name** text box, enter ICEcap Manager account name to use when uploading data. Refer to your ICEcap Manager documentation for more information about account names. The default account name is iceman.
7. In the **Password** text box, enter the current ICEcap Manager event password. This is the password that Desktop Protector uses to authenticate itself when it reports events to the ICEcap server.
8. In the **Group Name** text box, specify ICEcap Manager group to which this Desktop Protector installation is assigned.

   Note: This group must be created beforehand in ICEcap Manager and must have the correct configuration settings to report properly. See the *RealSecure ICEcap Manager User Guide* for more information about groups and group name precedence settings.
9. In the **Proxy URL** text box, enter the fully qualified URL for the proxy server, if any. If you are not using a proxy server, leave this field blank.
10. Click **OK**.

Testing your ICEcap connection

To see if your local agent can communicate with the ICEcap server:

1. On the Main Menu, select **Tools → Edit BlackICE Settings.**
2. Select the ICEcap tab.
3. Click **Test**.

   Desktop Protector sends a proactive heartbeat to the ICEcap server and ICEcap Manager updates the local agent's settings.
4. One of four messages appears in the **Last Status** text box:

- **OK:** The local RealSecure agent is successfully exchanging information with ICEcap Manager.
- **Authentication Failure:** The agent may have an incorrect account name or password. Re-enter the account, group, and password values and test again. If this error persists, check with your ICEcap administrator that you are using the correct account name, password, and group.
- **Abort:** The last attempt to communicate was cut off before it was complete. This is may be due to an interruption in network access between ICEcap Manager and the local RealSecure agent. Contact your ICEcap administrator.
- **Connection Failure:** The local agent was unable to connect to ICEcap Manager. You may have an improperly installed or configured network interface, or the local Desktop Protector system is in an area of the network that cannot access the ICEcap server. Contact your ICEcap administrator.

Local or remote precedence?

ICEcap Manager determines whether the settings on the local computer take precedence over settings received from ICEcap Manager. To find out your current precedence:

1. On the Main Menu, select **Tools → Edit BlackICE Settings.**
2. Select the ICEcap tab.
3. Click **Test**.

   Desktop Protector sends a proactive heartbeat to the ICEcap server and ICEcap Manager updates the local agent's settings.
4. Is **Enable local configuration editing** selected?
   - If *yes*, go to Step 5.
   - If *no*, you cannot change any intrusion detection settings from this computer. To change the local ICEcap configuration settings, contact your ICEcap administrator.
5. Under Configuration Priority, is the **Local** or **Remote** option button selected?
   - If the **Local** option button is selected, directions from ICEcap Manager are applied only to settings that you have not explicitly configured from the Local Console.
   - If the **Remote** option button is selected, ICEcap Manager can override any settings you enter on this computer.

Setting Your Protection Level

Introduction

Protection levels are predesigned sets of security settings developed for different types of Web use. You can choose to have Desktop Protector block all communications with your system, some communications with your system, or no communications with your system. This topic shows how to:

- set your protection level
- configure Desktop Protector to switch protection levels dynamically

Note: If your system is set up to report to ICEcap Manager and ICEcap Manager has configuration priority, you cannot set the protection level from the local agent. To change any firewall settings, you must contact your ICEcap administrator.

Setting your protection level

To set your protection level:

1. From the Main Menu, select **Tools→ Edit BlackICE Settings→ Firewall**.
2. Select a protection level:
   - To block *all* unsolicited inbound traffic, select **Paranoid**.
   - To block all unsolicited inbound traffic except for some interactive content on Web sites (such as streaming media), select **Nervous.**
   - To block only unsolicited network traffic that accesses operating system and networking services, select **Cautious**.
   - To allow all inbound traffic, select **Trusting**.
3. Do you want to enable auto-blocking?
   - If *yes*, select **Enable Auto-Blocking**.
   - If *no*, clear **Enable Auto-Blocking**.
4. Do you want to enable resource sharing?
   - 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?
   - If *yes*, select **Allow NetBIOS Neighborhood**.
   - If *no*, clear **Allow NetBIOS Neighborhood**.

For more information about protection levels, see “The Firewall Tab” on page 70.

Using Adaptive Protection

You can set up your firewall to switch protection levels automatically when it detects a connection with a remote computer. To do this, choose one of the procedures in this topic.

Setting adaptive protection from inside the corporate network

To switch to the Trusting protection level when your computer connects from inside your corporate network:

1. Click **Tools→ Advanced Firewall Settings**.

   The Advanced Firewall Settings window appears.
2. Select the Remote Adaptive Protection tab.
3. Under **Trusting**, enter up to five IP addresses in your corporate network.
4. Select the Local Adaptive Protection tab.
5. Under **Trusting**, enter up to five IP addresses included in your corporate network in the **Trusting** text box.
6. Click **OK**.

   Your firewall is configured to switch to Cautious when you make a connection inside your corporate network.

Setting adaptive protection from a home office

To work at the Cautious protection level from your home office and switch to Trusting when your computer connects with your corporate network:

1. Click **Tools→ Advanced Firewall Settings**.

   The Advanced Firewall Settings window appears.
2. Select the Remote Adaptive Protection tab.
3. Under **Trusting**, enter up to five IP addresses included in your corporate network.
4. Select the Local Adaptive Protection tab.
5. Under **Cautious**, enter up to five IP addresses that your computer may use when connecting to the Internet from your home.

   Note: These can be static IP addresses or a range of addresses that your ISP provides.
6. Click **OK**.

   Your firewall is configured to switch to Trusting when you connect to your corporate network from your home office.

Setting adaptive protection from a remote location

To work at the Paranoid level from a remote location such as a trade show or hotel and switch to Cautious when you connect with your corporate network:

1. Click **Tools→ Advanced Firewall Settings**.

   The Advanced Firewall Settings window appears.
2. Select the Remote Adaptive Protection tab.
3. Under **Cautious**, enter up to five IP addresses included in your corporate network.
4. Select the Local Adaptive Protection tab.
5. Under **Paranoid**, enter the IP address that your computer will use when connecting from the conference location.

Note: This can be a single static IP address or a set of addresses that the conference host provides.

6. Click **OK**.

   Your firewall is configured to switch to Cautious when you connect to your corporate network from your remote location.

Blocking Intrusions

Introduction

Desktop Protector identifies and stops most intrusions according to your preset protection level, but you may still notice activity that isn't explicitly blocked. This topic explains how to handle intrusions from a particular address or intrusions that use a particular protocol.

Caution: Do not block port scans from your own internal network. This may interfere with normal network management procedures.

Blocking an event or an intruder

You can block any intruder listed on your events list. When you do, Desktop Protector creates an IP address entry in your firewall that prevents all traffic from that IP address from entering your system. To block an intruder or an event:

1. Do one of the following:
   - On the Intruders tab, right-click the name of the intruder.
   - On the Events tab, right-click the name of the event.
2. On the submenu, select the duration of the block.

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

Blocking an IP address

To block an IP address:

1. From the Tools menu, select **Advanced Firewall Settings**.

   The Advanced Firewall Properties window appears.
2. Click **Add**.

   The Add Firewall Entry window appears.
3. Type a name for the IP address filter.

   Note: This should be the name of the system to block, if you know it. For example, if you are creating a filter to block all port scans from a known intruder, use the intruder's computer name for the name of this address filter. For information about how to learn about intruders, see "Back Tracing" on page 50.
4. Type the IP address or range of addresses for the system to block.
   - Use standard `000.000.000.000` notation.
   - If you are specifying a range of IP addresses, place a dash between them. For example, `192.168.10.23–192.168.10.32`.
   - To block transmissions from all IP addresses through a specific port, select **All Addresses.**

   Note: You cannot block all transmissions from all IP addresses in this window. To block all unsolicited inbound traffic, select the "Paranoid" protection level on the Firewall tab.
5. In the **Mode** area, select **Reject**.
6. In the **Duration of Rule** area, select the length of the block.
7. Click **Add**.

   Desktop Protector adds the entry to the list in the Advanced Firewall Settings window.

Blocking a Port

If you don't have a specific intruder in mind but you are concerned about intrusion attempts using a particular internet protocol, you can block the port that protocol uses. Adding a port entry to your firewall ensures that no traffic from any IP address can enter your system using that port.

To block a port:

1. From the Tools menu, select **Advanced Firewall Settings**.
2. Click **Add**.

   The Add Firewall Entry window appears.
3. Type a name for the port in the **Name** field.

   Note: You can use any name. For convenience, try using the name of the protocol or the software that uses the port, such as "Quake" or "SMTP."
4. Type the port number in the **Port** field.
   - Use a whole number between 1 and 65535.
   - To enter a range of ports, use the format 9-999.
   - To close all ports on your computer to communications from a specific IP address, select **All Ports**, then go to "Blocking an IP address" on page 37.

   Note: You cannot use Add Firewall Entry to block or accept all transmissions from all IP addresses through all ports. To instruct Desktop Protector to block all unsolicited inbound traffic, select the "Paranoid" protection level on the Firewall tab. To accept all traffic, select the "Trusting" protection level. For more information, see "Setting Your Protection Level" on page 34.
5. Select the port type in the **Type** field.

   Note: To create an entry for both port types, you must create two separate port filters.
6. In the **Mode** area, select **Reject**.

   The Desktop Protector application closes the port.
7. In the **Length of Block** area, select the length of time to block the port.
8. Click **Add**.

   Desktop Protector adds the entry to the list in the Advanced Firewall Settings window.

Trusting Intruders

Introduction

When an address is trusted, Desktop Protector assumes all communication from that address is authorized and excludes the address from any intrusion detection. Trusting ensures that Desktop Protector does not block systems whose intrusions may be useful to you. You can choose to trust a system that has already intruded on your computer, or you can identify a potential intruder to trust ahead of time.

Important: Trust only those systems that you are certain are safe, or are legitimately executing network scans, such as servers from an ISP. Keep in mind that intruders can fake the IP addresses of internal systems. It is possible, though very unlikely, for an intruder to fake a trusted address and avoid detection from Desktop Protector.

Trusting an existing intruder

To trust an intruder that Desktop Protector has detected:

1. Do one of the following:
   - On the Intruders tab, right-click the intruder.
   - On the Events tab, right-click the event/intruder combination that includes the intruder you want to trust.
2. On the shortcut menu, select **Trust Intruder**.
3. From the submenu, select one of the following:
   - **Trust and Accept**: The BlackICE intrusion detection component ignores all attacks from the intruder and the firewall accepts all communications from the intruder's IP address. The intruder is not subjected to any Desktop Protector detection or protection.
   - **Trust Only**: The BlackICE intrusion detection component ignores all attacks from the intruder.

   Important: Use caution when trusting a system. Intruders often mask their identity with forged IP addresses, so an intruder could use your trusted addresses as a mechanism against you. We recommend only trusting those systems that are authorized, trustworthy and secure.
4. Click **Yes**.

   Desktop Protector immediately starts trusting the intruder, and adds the intruder address to the list of trusted IP addresses on the Desktop Protector Settings Detection tab.

Trusting an intruder in advance

To trust an intruder that Desktop Protector has not yet detected:.

1. From the Main Menu, select **Tools→ Edit BlackICE Settings**.
2. Select the Intrusion Detection tab.
3. Click **Add**.

   The Exclude from Reporting window appears.
4. Type the IP address in the **IP** box, or select **All**.
   - Use standard `000.000.000.000` notation.
   - If you are specifying a range of IP addresses, place a dash between them. For example, `192.168.10.23-192.168.10.32`.
5. Click **OK**.

Ignoring Events

You can configure RealSecure Desktop Protector to ignore events that are not a threat to your system.

Note: *Ignoring* an event is different from *trusting* an intruder. Ignoring disregards certain kinds of events. When an event type is ignored, Desktop Protector does not log any information about events of that type. Trusting excludes an address from intrusion detection. Intrusions from that address are not shown on the Events tab.

Ignoring an existing event type

To ignore an event type:

1. On the Events tab, right-click the event/intruder combination.
2. On the shortcut menu, select **Ignore Event**.
3. From the submenu, select one of the following:
   - **This Event**: The BlackICE intrusion detection component ignores all future instances of the event.
   - **This Event by this Intruder**: The BlackICE intrusion detection component ignores all future instances of this event by the referenced intruder.
4. Click **Yes**.

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

Ignore an event type in advance

When you know of a potential event but haven't seen that type of event yet, and you want Desktop Protector to allow the event, you can preemptively ignore the event type. For example, you may want to ignore future HTTP port scans from your Internet Service Provider. Follow these steps:

1. From the Main Menu, select **Tools→ Edit BlackICE Settings.**
2. Select **Intrusion Detection**.
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 are specifying a range of IP addresses, place a dash between them. For example, `192.168.10.23–192.168.10.32`.
7. In the **Attacks 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**.

For more information, see “The Prompts Tab” on page 83.

Working with the Application Protection Baseline

Introduction

When you install RealSecure Desktop Protector, it creates a baseline record (also known as a checksum) of the applications installed on your computer. Desktop Protector uses this information to prevent any unauthorized applications from running. When Desktop Protector alerts you that an unknown application is starting, you can stop the application or let it run. If you let it run, Desktop Protector can remember your choice or require new authorization every time the application starts.

Updating the baseline

After you install or update software, you must add each new or upgraded application to the baseline so that BlackICE recognizes that it is an approved application. There are two ways to add an application to the baseline:

- create a new baseline
- start the new or upgraded application and tell Desktop Protector to include it in the existing baseline

Important: To get the full benefit of Application Protection, scan your system for viruses with an anti-virus program to make sure it is free of dangerous applications before you update your system's baseline. It is a good idea to run your anti-virus scan in both normal and safe mode.

Creating a new baseline

To create a new baseline:

1. On the Tools menu, select **Advanced Application Protection Settings**.

   The Advanced Application Protection Settings window appears.
2. Click the **Baseline** tab.
3. Expand the folder tree.
4. Select the folders to include in your baseline by checking the box next to the folder name. If you select a folder that contains subfolders, Desktop Protector inspects all the subfolders in that folder.

   Tip: To include the whole drive in the baseline, check the box next to the drive letter at the top of the tree.
5. Click **Save Changes**.

   Desktop Protector begins creating a baseline of the application files that are installed in the folders you chose.

   Note: This process can take several minutes, depending on the size of the folders.
6. To check the list of applications Desktop Protector created, click **Known Applications**.

Adding an application to your baseline

To add an application to your baseline after you have installed or upgraded the application:

1. Start the application.

   Desktop Protector alerts you that an unknown or modified application is trying to start.
2. In the warning message window, select **Allow the application to launch** and **Don't ask me again**.

3. Repeat for every warning message that appears. The number of messages you see depends on how many files the application runs. BlackICE will not display the warning messages again unless the application changes.

Building your baseline over time

Desktop Protector can learn your application protection preferences as you work. You can have Desktop Protector ask you for a decision on each program as it launches.

To update your baseline as you work:

1. On the Tools menu, select **Edit BlackICE Settings**, then select the Application Control tab.
2. Select an option under **When an unknown application launches**.
   - To have Desktop Protector check with you when it detects an application you have not explicitly allowed to run, select **Ask me what to do**. This is the default.
   - To have Desktop Protector automatically shut down any application you have not allowed to run, select **Always terminate the application**.

Application Protection alerts

If you have enabled the Application Protection component and selected **Ask me what to do**, Desktop Protector alerts you when an unknown application starts. For information about how to respond to these alerts, see "Responding to Application Protection Alerts" on page 56.

Note: To avoid false positives, update your application protection baseline every time you install new software. Installing a new application can change some helper files, such as DLLs, that are already in your baseline. Desktop Protector may flag these as "modified files" until you update your baseline.

Application file types

Desktop Protector determines which files are included in the baseline from the file name extensions. Desktop Protector currently checks for these application file types:

Extension	File Type
dll	Dynamic link library, a collection of resources that enable a program file to do its job
drv	Driver, a small program that enables a device or service to work
exe	Executable file, containing program instructions
ocx	Special-purpose program for functions such as scroll bar movement and window resizing in Windows applications
scr	Screensaver program
sys	Files that control basic operating system functions
vxd	"Virtual device" that enables other software to work

Adding file types to the baseline

If you know of application files on your system that have different extensions, you can add those extensions before creating your baseline.

To search for additional file types:

1. On the Desktop Protector Tools menu, select **Advanced Application Protection Settings**.
2. On the Advanced Application Protection Settings window Tools menu, select **Checksum Extensions**.

   The Checksum Extensions window appears.
3. Enter the extension in the **Extensions** text box.
4. Click **Add**.
5. Repeat steps 3 and 4 until all the file types have been added.
6. Click **OK**.

   Desktop Protector adds the new file type extensions to the list.

Application Protection alerts

If you have enabled Application Protection and selected **Ask me what to do**, Desktop Protector alerts you when an unknown application starts. For information about how to respond to these alerts, see "Responding to Application Protection Alerts" on page 56.

Managing your authorized applications

After you have created your baseline, you can change the authorizations of any file in it. You can allow it to run, or you can prevent it from running. If you allow it to run, you can block it from accessing a network or allow it to access the network.

Changing application permissions

To manage your authorized application files:

1. On the Tools menu, select **Advanced Application Protection Settings**.
2. Click the **Known Applications** tab.

   Desktop Protector displays the list of applications it has detected on your system.
3. In the **Filename** column, find the name of the application file whose authorization you want to change.
   - To prevent the application from running, select **Terminate** in the **Application Control** column. Desktop Protector adds the application to the list of programs that are not allowed to run on this computer.
   - To allow the application to run, leave the selection in the **Application Control** column blank. Desktop Protector regards this as an authorized application.
4. Click **Save Changes**.

Stopping Application Protection temporarily

To stop Desktop Protector from monitoring your system for unauthorized applications:

- On the Tools menu, click **Stop BlackICE Application Protection**.

  A red slash appears across the Desktop Protector icon in your system tray to indicate that Application Protection is turned off.

Caution: When you stop the Application Protection component, your system is no longer protected from running unauthorized applications, such as Trojans. However, Desktop Protector intrusion detection monitoring is still in effect.

Disabling Application Protection

To permanently prevent Desktop Protector from monitoring your system for unauthorized applications, follow this procedure:

1. On the Tools menu, select **Edit BlackICE Settings**, and then select the Application Control tab.
2. Clear **Enable Application Protection**.

   Desktop Protector disables the Application Protection feature. You must manually enable Application Protection to resume the service.

Note: Stopping the Application Protection component is not the same as disabling it. When you stop the Application Protection component, it resumes protecting your system when you restart your system. If you disable the component, it does not restart when you restart your computer. To make it available again, you must re-enable it.

More information

For more information about using your Application Protection settings, see "Advanced Application Protection Settings" on page 99 and "The Application Control Tab" on page 84.

Configuring Communications Control

Introduction

When you set your communications control preferences, you establish a rule for RealSecure Desktop Protector to follow whenever an application tries to access a network without your approval. You have the option of terminating the application or letting it run. If you choose to let it run, you can block its network access or allow it to reach the network.

How to set your communications preferences

To set your communications control preferences:

1. From the Main Menu, select **Tools→ Edit BlackICE Settings**, and then select the Communications Control tab.
2. To watch for outbound communications from this computer, select **Enable Application Protection**.

   Note: If ICEcap Manager has disabled Communication Control on this agent, the **Enable Application Protection** option is dimmed and you cannot change the settings on the Communications Control tab.

   For information about using this option, see "Disabling Application Protection" on page 45.
3. Choose one of these options:
   - To automatically close down any unauthorized application that tries to access a network from your system, select **Always terminate the application**. If you installed Desktop Protector in Unattended mode, this option is selected by default.
   - To have Desktop Protector give you the choice of running or terminating the unauthorized process whenever it tries to contact a network, select **Prompt before terminating the application**. This option is selected by default.
   - To allow unauthorized processes to run but automatically block them from connecting to a network, select **Always block network access for the application**.
   - To have Desktop Protector ask you whether an unauthorized processes can connect to a network, select **Prompt before blocking network access for the application**.

Managing your applications' communications

You can change the authorizations of any application in your baseline. You can allow it to communicate with a network or prevent it from communicating.

To change authorizations:

1. On the Tools menu, select **Advanced Application Protection Settings**.
2. Click the **Known Applications** button.

   The application files on your system are displayed.
3. To automatically close down an application when it attempts to connect to a network, select **Terminate** in the **Communications Control** column.
4. To prevent an application from communicating with a network, select **Block** in the **Communications Control** column.
5. To explicitly allow an application to communicate with a network, leave the **Communications Control** column blank.
6. Click **Save Changes**.

For more information about setting your Communications Control preferences, see "The Communications Control Tab" on page 86.

Controlling Event Notification

Introduction

You may find that you want regular access to more or less information than RealSecure Desktop Protector shows by default. You can use the Desktop Protector configuration tabs to control the following:

- how much information appears on the Desktop Protector information tabs
- how frequently Desktop Protector alerts you to potential risks

Filtering the Events List

To filter events:

1. On the View menu, select **Filter by Event Severity**.
2. From the submenu, select the least severe events to display.

   For example, 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 attacks. For example, if the list is filtered to show only serious and critical attacks, the Suspicious and Informational icons do not appear.

Clearing the Events list

To clear the Events list:

1. From the Main Menu, select **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. For more information about what you are deleting, see "The Events Tab" on page 62.
   - Select **Evidence logs** to delete all evidence log data. For information about what is included in evidence data, see "Collecting Evidence Files" on page 52.
   - Select **Packet logs** to delete all packet log data. For information about what packet log data consists of, see "Collecting Packet Logs" on page 54.
3. Click **OK**.

Note: Clearing the event list does not stop Desktop Protector from trusting, blocking, or ignoring events or intruders.

Setting alarm preferences

To set Desktop Protector alarm preferences:

1. From the Main Menu, select **Tools→ 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 (`bialarm.wav`). To change the `.wav` file used in audible notification, click the folder icon and locate the desired file.

4. Click **OK**.

For more information about setting your notification preferences, see "The Notifications Tab" on page 81.

Freezing the Events list

Freezing the Events list stops Desktop Protector from refreshing the tab information until you unfreeze it. However, freezing does not stop the monitoring, detection, and protection features of Desktop Protector.

Note: Remember to unfreeze the application after viewing the list so that Desktop Protector can display new attacks. When you restart the computer, Desktop Protector resets to an unfrozen state.

To freeze the Events list:

- From the Main Menu, select **View→Freeze**.

Showing and hiding columns

You can configure the columns that the Events and Intruders tabs display.

Note: Removing a column from the window does not remove the information from that column in Desktop Protector.

To select columns to view:

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

   The Columns window opens.
2. Follow the instructions on the Columns window.
3. Click **OK**.

Back Tracing

Introduction

RealSecure Desktop Protector can track an intruder's activities to help you determine what an intruder did to your computer. This topic explains how to gather and use this information.

How does back tracing work?

Back tracing is the process of tracing a network connection to its origin. When somebody connects to your system over 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. RealSecure Desktop Protector can read information from these packets and identify each router the intruder's packets had to travel through. Desktop Protector can often identify the intruder's system in this way.

Back tracing information

When Desktop Protector back traces an intruder, it attempts to gather the IP address, DNS name, NetBIOS name, Node, Group name, and MAC address. Skilled intruders will often try to block Desktop Protector from acquiring this information.

Procedure

To set up back tracing:

1. From the Main Menu, select **Tools→ Edit BlackICE Settings**.
2. Select the **Back Trace** tab.
3. Type the severity level for an indirect trace in the **Indirect Trace Threshold** box.

   Note: The default threshold for an indirect trace is 3. With this setting, any event with a severity of 3 or above triggers an indirect back trace.
4. Do you want Desktop Protector to query Domain Name Service servers for information about the intruder?
   - If *yes*, select **DNS lookup**.
   - If *no*, clear **DNS lookup**.
5. Type the severity level for a direct trace in the **Direct Trace Threshold** box.

   Note: The default threshold for the direct trace is 6. With this setting, any event with a severity of 6 or above triggers a direct back trace.
6. Do you want Desktop Protector to determine the computer address of the intruder's computer?
   - If *yes*, select **NetBIOS nodestatus**.
   - If *no*, clear **NetBIOS nodestatus**.

Direct and indirect tracing

Desktop Protector can trace intruders *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. Indirect back tracing does not make contact with the intruder's system, and therefore does not acquire much information. Indirect traces are best suited for lower-severity attacks.
- A direct trace goes all the way back to the intruder's system to collect information. Direct back tracing makes contact with the intruder's system and therefore can acquire a lot of information. Direct back traces are best for high-severity attacks, when you

want as much information about the intruder as possible. However, intruders can detect and block a direct trace.

Where is the back tracing information?

Back tracing information appears in two places:

- in the information pane of the Intruder tab
- in standard text files in the Hosts folder in the directory where Desktop Protector is installed. Each file is prefixed with the intruder's IP address.

Note: The severity of the incoming event, not the identity of the intruder, triggers the back trace.

For more information about setting your back tracing preferences, see "The Back Trace Tab" on page 76.

Collecting Evidence Files

Introduction

RealSecure Desktop Protector can capture network traffic attributed to an intrusion and place that information into an evidence file. Desktop Protector captures and decodes each packet coming into the system, so it can generate files that contain detailed information about the intruder's network traffic.

Where are my evidence files?

Desktop Protector evidence files are stored in the installation directory folder. For example, if you install Desktop Protector in the `Program Files` directory on the `C:` drive, the evidence files are located in `C:\Program Files\ISS\BlackICE`. Each file has an `*.enc` extension.

Note: If you upgraded to RealSecure Desktop Protector 3.5 from a previous version of BlackICE, your evidence log files are still stored in `C:\Program Files\Network ICE\BlackICE`.

Evidence file format

The evidence and packet log files are trace files. You must have a trace file decoding application to view the contents of these files. Many networking and security product companies produce such decoders. Some shareware decoders are also available on the Internet. If you are using Windows NT or Windows 2000 Server, you can install the Network Monitoring service, which includes Network Monitor, a decoding application. See the Windows NT or Windows 2000 documentation for more information.

Procedure

To collect evidence files:

1. From the Main Menu, select **Tools→ Edit BlackICE Settings**.
2. Select the **Evidence Log** tab.
3. Select **Logging Enabled**.
4. In the **File prefix** box, specify the prefix for the evidence file names.
   - To place a date stamp (format YYYYMMDD) and number (NN) in the file name, enter `%d` after the prefix. For example, if you enter `evd%d`, the file names will look like this: `evdYYYYMMDD-NN.enc`. The time is in 24-hour format in Greenwich Mean Time (GMT).
5. In the **Maximum Size** box, specify how large each evidence file can get.

   Note: For best results, keep this value smaller than 2048 kilobytes (2 MB).
6. In the **Maximum Number of Files** box, choose how many files Desktop Protector can generate in the specified collection time period.

   Note: For example, if the maximum number of files is 32 (the default value), Desktop Protector does not generate more than 32 evidence files in any 24-hour period.

Clearing evidence logs

To delete evidence logs:

Note: Clearing evidence log data does not affect the Desktop Protector intrusion detection and firewall functions.

1. From the Main Menu, click **Tools→ Clear Files**.

   The Files to Delete window appears.
2. Select **Evidence logs**.

3. Click **OK**.

For more information about setting your evidence logging preferences, see "The Evidence Log Tab" on page 74.

Collecting Packet Logs

Introduction

Packet logging records all the packets that enter your system. This can be useful if you need more detailed information than evidence logs contain.

Where are my packet log files?

Desktop Protector packet log files are stored in the installation directory folder. For example, if you install Desktop Protector in the `Program Files` directory on the `C:` drive, the packet log files are located in `C:\Program Files\ISS\BlackICE`. Each file has an `*.enc` extension.

Note: If you upgraded to RealSecure Desktop Protector 3.5 from a previous version of BlackICE, your packet log files are still stored in `C:\Program Files\Network ICE\BlackICE`.

Packet log file format

The packet log files are trace files. You must have a trace file decoding application to view the contents of these files. Many networking and security product companies produce such decoders. Some shareware decoders are also available on the Internet. If you are using Windows NT or Windows 2000 Server, you can install the Network Monitoring service, which includes Network Monitor, a decoding application. See the Windows NT or Windows 2000 documentation for more information.

Procedure

To collect packet logs:

1. From the Main Menu, click **Tools→ Edit BlackICE Settings**.
2. Select the **Packet Log** tab.
3. Select **Logging Enabled**.
4. In the **File prefix** box, specify the prefix for the packet log file names.
   - Desktop Protector automatically places an incremental counter in the filename. For example, if you enter `ABC`, the file names will be `ABC0001.enc`, `ABC0002.enc`, and so on.
5. In the **Maximum Size** box, specify how large each log file can get.

   Note: For best results, keep this value under 2048 kilobytes (2 MB).
6. In the **Maximum Number of Files** box, specify how many log files to generate.

   Note: The default is 10.

   Packet log files are generated until the maximum number of files are used. Once the maximum number of files are used, Desktop Protector starts replacing the first log file with a new file, and so on.

Clearing packet logs

To delete packet logs:

1. From the Main Menu, select **Tools→ Clear Files**.

   The Files to Delete window appears.
2. Select **Packet logs**.
3. Click **OK**.

Note: Clearing packet log data does not affect the Desktop Protector intrusion detection and firewall functions.

For more information about choosing your packet logging settings, see "The Packet Log Tab" on page 72.

Responding to Application Protection Alerts

Introduction

Programs can start without your knowledge. The Application Protection component may be triggered when you start a new program through the **Start** menu or by clicking a shortcut, but it may also be triggered by a program that starts without giving any on-screen indication. If you have enabled Application Protection and selected **Ask me what to do**, Desktop Protector alerts you when an unknown application starts.

Procedure

To respond to the Application Protection dialog:

1. Are you installing new software on your computer?
   - If *yes*, click **Install Mode Options**, and then click **Enable Install Mode.**

     Desktop Protector temporarily stops Application Protection so that the new software can start the applications required for its installation. Desktop Protector will remind you every three minutes to enable Application Protection again.

     Note: Some installation programs require you to restart your system. Desktop Protector Application Control stays in Install Mode even if you restart. This may be necessary for some software installations or updates that continue to install after system reboot. When the installation is finished, update your system baseline and then disable Install Mode.
   - If *no*, go to Step 2.
2. Are you certain that this is an application you have authorized?
   - If *yes*, click **Continue**.

     Desktop Protector allows the application to start.

     Tip: To have Desktop Protector assume this application is authorized every time it runs, select **Don't ask me again,** then click **Continue**. Desktop Protector adds the application to your list of authorized applications and does not warn you about it again.
   - If *no*, go to Step 3.
3. Click **More Info...**

   A popup dialog box appears with the name and path of the application file that triggered Application Protection.
4. Is this file an authorized application?
   - If *yes*, click **OK**, and then click **Continue**.

     Desktop Protector allows the application to start.
   - If *no*, go to Step 5.
5. Do you want to enable the application to run even though it may be a dangerous program?
   - If *yes*, click **OK**, and then click **Continue**.

     Desktop Protector allows the application to start.
   - If *no*, click **OK**, and then click **Terminate**.

   Desktop Protector adds the application to your list of prohibited applications.

Exporting Desktop Protector Data

Introduction

You may want to export RealSecure Desktop Protector data into a spreadsheet program or word processor to look at the intrusion activity on your system.

Procedure

To export data:

1. Copy or cut the selected information to place it on the clipboard.
2. Paste the information into any application that accepts text input.

INTERNET SECURITY SYSTEMS™

Appendixes

Appendix A

Operating Tabs

Overview

Introduction

This appendix describes the operating tabs. RealSecure Desktop Protector gathers information and presents it on the Events tab, the Intruders tab and the History tab.

In this appendix

This appendix contains the following topics:

The Events Tab

Introduction

The Events tab summarizes all intrusion and system events on your computer. The tab columns show the time, type, and severity of an event; the intruder's name and IP address; how Desktop Protector has responded to the event, and other information.

Customizing information

To customize the information on the Events tab, right-click a column header and select **Columns**. A window appears in which you can add, hide, show, resize, or rearrange columns. By default, the information on the Events tab is sorted first by severity, then by time.

Sorting

Click a column header to sort the list by that column. Click the column header again to reverse the sort order.

AdvICE button

When you select an event in the Events tab, a brief description of the attack appears at the bottom of the tab. For more information about the event, or to see suggested remedies for the attack, click **advICE** to connect to the ISS Web site for the latest information about that event.

Note: For more information about filtering the information shown on the Events tab, see"Filtering the Events List" on page 48.

Default Events tab columns

This table describes the default columns on the Event tab. For information about adding optional columns, see "Showing and hiding columns" on page 49:

This column...	Contains this information...
Severity	The severity icon is a visual representation of the severity of an event and the response from RealSecure Desktop Protector. For more information, see "Severity levels" on page 12.
Time	The date and time the event occurred, in 24-hour format.
Event	The name of the event type. A description of the event is displayed at the bottom of the window.
Intruder	The NetBIOS or DNS name of the attacking system. When Desktop Protector cannot determine a name, it displays the intruder's IP address.
Count	If an intruder executes the same attack several times, the Events tab shows the collected occurrences as one event. This column displays the number of occurrences that made up that event. The Time column shows the time the most recent event occurred.

Table 9: *Events tab default columns*

Optional columns on the Events tab

This table describes optional columns that you can add to the Events tab. To add an optional column, right-click any column heading and select **Columns...**

This column...	Contains this information...
TCP Flags	Data in the packet header specifying the intended treatment of the packet, such as `R` (reset), `P` (push), or `U` (urgent).
Parameter(s)	When an intruder is scanning a particular port, this column displays the port numbers scanned. To consult the ISS Web site for details about what the scan may indicate, click the advICE button. The Parameter(s) column cannot be used to sort the Events list.
Protocol ID	The network protocol (such as HTTP, FTP or NetBIOS) applicable to the intruder's communications. For example, if the intruder was sending malicious Web site commands, the protocol would likely be HTTP.
Destination Port	The TCP/UDP port on the local system that was the target of the attempted intrusion.
Source Port	The TCP/UDP port on the intruder's system where the event originated.
Target	The NetBIOS (WINS) name or DNS name of the attacked system (the target). In most cases, this is the local system. If Desktop Protector cannot determine a name, it shows the target's IP address.
Target IP	The IP address of the attacked system. This is usually the IP address of the local system.
Intruder IP	The IP address of the attacking system.
Event ID	Internal reference number for each unique event signature.
Response Level	A visual representation of the protection Desktop Protector provided against the intrusion. Each event is indicated with one of five response levels. For information on how Desktop Protector responds to events, see page Response Levels on page 15.
Severity (numeric)	A numeric representation of the severity of the event. For more information, see "Desktop Protector Alerts" on page 9.

Table 10: *Events tab optional columns*

Shortcut commands on the Events tab

This table describes the commands available by right-clicking an item on the Event tab:

This command...	Has this effect...
Ignore Event	To ignore an event, right-click an event/intruder combination, and then select **Ignore Event**. Ignoring event types is a useful way to stop Desktop Protector from reporting routine scans from ISPs and network probes.
Select Most Recent	To highlight the most recent event, right-click an event, and then select **Select Most Recent**.
Block Intruder	To block an intruder, right-click an event/intruder combination, and then select **Block Intruder**.
Trust Intruder	To trust an intruder, right-click an event/intruder combination, and then select **Trust Intruder**. On the submenu, select **Trust and Accept** or **Trust Only**.
Cut	To remove an event/intruder combination from the list, right-click the event/intruder combination, and then select **Cut**.
Copy	To copy an event/intruder combination to your system's clipboard, right-click the event/intruder combination, and then select **Copy**.
Delete	To remove an event/intruder combination from the list, right-click the event/intruder combination, and then select **Delete**.
Select All	To select all the events in the list, right-click an event/intruder combination, and then select **Select All**.
Find	To search for a record in the list, right-click an event/intruder combination, and then select **Find**.
Clear Events List	To remove all events from the list, right-click anywhere in the list, and then select **Clear Events List**.
Print	To print the entire contents of the Events list, right-click an event/intruder combination, and then select **Print**.

Table 11: *Events tab shortcut commands*

Buttons on the Events tab

This table describes the buttons that appear on the Intruders tab:

This button...	Has this effect...
Close	Closes the main Desktop Protector window. The detection and protection engine remains active.
Help	Displays the online Help for this tab.

Table 12: *Events tab buttons*

The Intruders Tab

Introduction

The Intruders tab displays all the information RealSecure Desktop Protector has collected about all the intruders who have initiated events on your system. This information helps you determine the severity and location of each intruder.

Sorting

By default, the intruder list is sorted first in alphabetical order by intruder and then in descending order of severity. Click a column header to sort the list by that column. Click the column header again to reverse the sort order.

Details pane

When you select an intruder from the Intruder list, the information RealSecure Desktop Protector has gathered about the intruder appears in the Details pane.

Default columns on the Intruders tab

This table describes the columns that appear by default on the Intruders tab:

This column...	Contains this information...
Severity icon	The severity icon is a visual representation of the severity of an event and the response from Desktop Protector. For more information, see “Severity levels” on page 12.
Blocked State icon	The blocked state icon indicates that Desktop Protector is blocking all network traffic from this intruder. For information about blocking an intruder, see “Blocking Intrusions” on page 37.
Intruder	The NetBIOS or DNS name of the attacking system. When Desktop Protector cannot determine a name, it displays the intruder’s IP address.

Table 13: *Intruders tab default columns*

Shortcut commands on the Intruders tab

This table describes the commands available by right-clicking information on the Intruders tab:

This command...	Has this effect...
Block Intruder	To block an intruder, right-click the intruder, then select **Block Intruder**.
Trust Intruder	To trust an intruder, right-click the intruder, then select **Trust Intruder**. On the submenu, select **Trust and Accept** or **Trust Only**.
Cut	To remove an intruder from the list, right-click the intruder, then select **Cut**.
Copy	To copy an intruder to your system clipboard, right-click the intruder, and then select **Copy**.
Delete	To remove an intruder from the list, right-click the intruder, then select **Delete**.
Select All	To select all the intruders in the list, right-click any intruder, then select **Select All**.

Table 14: *Intruders tab right-click commands*

This command...	Has this effect...
Find	To search for an intruder in the list, right-click any intruder, and then select **Find**.
Print	To print the entire contents of the Intruders list, right-click any intruder, and then select **Print**.

Table 14: *Intruders tab right-click commands*

Optional columns on the Intruders tab

This table describes the optional columns you can add to the Intruders tab. For information about adding optional columns to the display, see "Showing and hiding columns" on page 49.

This column...	Contains this information...
Intruder IP	The IP address of the attacking system.
Severity (numeric)	The highest severity rating attributed to this intruder.

Table 15: *Intruders tab optional columns*

Buttons on the Intruders tab

This table describes the buttons that appear on the Intruders tab:

This button...	Has this effect...
Close	Closes the main Desktop Protector window. The detection and protection engine remains active.
Help	Displays the online Help for this tab.

Table 16: *Intruders tab buttons*

The History Tab

Introduction

The History tab graphs network and intrusion activity on your system.

Note: For detailed information about activity on the Events graph, click the graph near the marker that shows the time you are interested in. The Events tab appears, with the intrusion closest to that time highlighted.

History tab options

This table describes the options available on the History tab:

This option...	Has this effect...
Interval	Selects the interval for displaying activity on both graphs, as follows: • **Min** displays activity over the last 90 minutes. • **Hour** displays activity over the last 90 hours. • **Day** displays activity over the last 90 days.

Table 17: *History tab options*

Information on the History tab

This table describes the features on the History tab that provide information about intrusions:

This feature...	Has this effect...
Interval	Selects the interval for displaying activity on both graphs, as follows: • **Min** displays activity over the last 90 minutes. • **Hour** displays activity over the last 90 hours. • **Day** displays activity over the last 90 days.
Total in 90 Hours (Days, Minutes)	Displays summary statistics for the selected interval, as follows: • **Critical** displays the number of events rated critical. This event type is tracked with a red line on the Events graph. • **Suspicious** displays the number of events rated serious and suspicious. These event types are tracked with a yellow line on the Events graph. • **Traffic** displays the amount of network traffic, measured in number of packets. Traffic is tracked with a green line on the Network Traffic graph.
Events Graph	Displays the number of critical and suspicious events detected per second during the specified period. The maximum number of events per second appears in the upper left corner of the Events graph.
Network Traffic Graph	Tracks the number of packets your system sends and receives during the period shown. The maximum number of events per second appears in the upper left corner of the Events graph.

Table 18: *History tab information features*

History tab buttons

This table describes the buttons on the History tab:

This button...	Has this effect...
Close	Closes the main Desktop Protector window. The detection and protection engine remains active.
Help	Displays the Help.

Table 19: *History tab buttons*

Appendix B

Configuration Tabs

Overview

Introduction

You can control some aspects of the way RealSecure Desktop Protector works by changing the settings on the configuration tabs.

In this Appendix

This appendix contains the following topics:

The Firewall Tab

Introduction

Use the Firewall tab to choose how tightly Desktop Protector controls access to your system.

Note: If your computer is reporting intrusion events to ICEcap Manager and local configuration editing has been disabled, you cannot set any options on the Firewall tab from the local system.

Protection level settings

You can choose one of these four protection levels:

Level	Description
Paranoid	All ports are blocked to incoming traffic.
Nervous	All system ports are blocked, and TCP application ports 1024 through 6635 are blocked.
Cautious	All system ports are blocked, but all application ports that you have not explicitly blocked are open.
Trusting	Keeps all ports open and unblocked, allowing all inbound traffic. This is the default setting.

Table 20: *Protection levels*

For information about how to choose your protection level, see "Setting Your Protection Level" on page 34.

Current Protection Level

If you are using adaptive protection to automatically switch protection levels based on network traffic, this field identifies the protection level your computer is currently using. This is not always the same as the protection level you selected manually. For more information, see "Using Adaptive Protection" on page 35.

Enable Auto-Blocking

When this option is selected, Desktop Protector automatically blocks intruders when they attempt to break into your system. To stop auto-blocking, clear this option. Attacks are still reported and logged, but not automatically blocked.

If Auto-Blocking is not selected, you must manually block intruders to protect your system.

Allow Internet File Sharing

Internet or Windows file sharing allows you to share files with others across the Internet or over a LAN. For example, you can connect to your system the Internet and upload or download files.

Clear this check box to do the following:

- prevent systems from connecting to your system and accessing your shares over the Internet or network
- make your system unavailable to all systems on a local network, so if you are on a network, you should select this option unless you do not share files among systems.

Note: This option modifies the firewall setting for TCP port 139. If you select this option, Desktop Protector accepts communications on port 139; if you disable this option,

Desktop Protector rejects or blocks communications on port 139. On Windows 2000, this setting also affects port 445.

Allow NetBIOS Neighborhood

Select this option to allow your system to appear in the Network Neighborhood of other computers.

Clear this option to hide a computer from the Network Neighborhood. Hiding your system does not disable file sharing, but users must locate the computer manually using its IP address.

Note: This option modifies the firewall setting for UDP ports 137 and 138. If you select this option, Desktop Protector accepts communications on these ports; if you disable this option, Desktop Protector rejects or blocks communications on these ports.

Firewall tab buttons

This table describes the buttons that appear on the Firewall tab.

This button...	Has this effect...
OK	Click to save your changes and return to the main Desktop Protector window.
Cancel	Click to discard your changes and return to the Desktop Protector window.
Apply	Click to save your changes and keep the current tab open.
Help	Displays the online Help for this tab.

The Packet Log Tab

Introduction

The Packet Log tab allows you to configure the RealSecure Desktop Protector packet logging features. When packet logging is enabled, Desktop Protector records all the network traffic that passes through your system.

Packet logs or evidence logs?

Because they contain a record of all network traffic, packet logs can grow very large and occupy a lot of disk space. If you do not need to record every packet, evidence logging may be a better choice. See "Collecting Evidence Files" on page 52.

Reading packet logs

Packet logs are stored in the Desktop Protector installation directory. If you installed Desktop Protector in the default location, you can find the packet log files at `C:/Program Files/ISS/BlackICE`. Use a trace file decoding application such as Network Monitor to view the information in these files.

Note: If you upgraded to 3.5 from a previous version of BlackICE, your evidence log files are still stored in `C:\Program Files\Network ICE\BlackICE`.

Packet log files are encoded as trace files. You must have decoding application. See the Windows NT or Windows 2000 documentation for more information.

Packet Log settings

This table describes the settings on the Packet Log tab:

This setting...	Has this effect...
Logging Enabled	When selected, Desktop Protector captures packet logs. Packet logging is disabled by default.
File Prefix	Specifies the prefix for the packet log file names. Desktop Protector automatically places an incremental counter in the filename. For example, if you enter `ABC`, the file names will be `ABC0001.enc`, `ABC0002.enc`, etc. The default file prefix is `log`.
Maximum Size (kilobytes)	Specifies the maximum size, in kilobytes, for each log file. The default value is 2048 kilobytes.
Maximum Number of Files	Specifies the maximum number of log files to generate. The default value for the maximum number of files to log is 10.

Table 21: *Packet Log tab settings*

For more information about setting your packet logging preferences, see "Collecting Packet Logs" on page 54.

Packet Log tab buttons

This table describes the buttons that appear on the Packet Log tab.

This button...	Has this effect...
OK	Click to save your changes and return to the main Desktop Protector window.
Cancel	Click to discard your changes and return to the Desktop Protector window.
Apply	Click to save your changes and keep the current tab open.
Help	Displays the online Help for this tab.

The Evidence Log Tab

Introduction

When your system is attacked, RealSecure Desktop Protector can capture evidence files that record network traffic from the intruding system. Evidence files record the specific packet that set off a protection response. This can be a good way to investigate intrusions without using a lot of disk space for records.

Evidence files

Evidence files are located in the installation directory folder. For example, if you installed Desktop Protector in the Program Files directory on the `C:` drive, the evidence files are in `C:\Program Files\ISS\BlackICE`. The file extension for all evidence log files is `*.enc`.

Note: If you upgraded to RealSecure Desktop Protector 3.5 from BlackICE Agent, your evidence log files are still stored in `C:\Program Files\Network ICE\BlackICE`.

Evidence files are encoded as trace files. To view the contents of these files, you must have a decoding application, such as Network Monitor (included with the Windows NT Server and Windows 2000).

The Evidence Log tab controls the size and grouping of each evidence file set. For more information about tracking evidence of intrusions, see "Collecting Evidence Files" on page 52.

Note: Evidence files are not the same as packet logs. Packet logs are a capture of all inbound and outbound traffic on the system. An evidence file focuses on the traffic associated with specific attacks.

Evidence Log settings

This table describes the available log file settings:

This setting...	Has this effect...
Logging enabled	Instructs Desktop Protector to collect evidence files for suspicious events. If Desktop Protector is remotely installed from ICEcap, this option is disabled by default. If Desktop Protector is installed manually, this setting is enabled by default.
File prefix	Specifies the prefix for the evidence file names. To place a date stamp (format YYYYMMDD) and number (NN) in the file name, enter `%d` after the selected prefix. For example, if you enter `evd` (the default file prefix), the file names will look like this: `evdYYYYMMDD-NN.enc`. The time is in 24-hour format in Greenwich Mean Time (GMT).
Maximum size (in kilobytes)	Controls how big each evidence file can get. For best results, keep this value under 2048 kilobytes (2 MB). To ensure that the file fits on a floppy disk, consider using a maximum size of 1400 kilobytes (the default).
Maximum number of files	Limits the number of files Desktop Protector generates in the specified collection time period. For example, if the maximum number of files is 32 (the default value), Desktop Protector does not generate more than 32 evidence files in any 24-hour period.

Table 22: *Evidence log tab settings*

Evidence Log tab buttons

This table describes the buttons that appear on the Evidence Log tab.

This button...	Has this effect...
OK	Click to save your changes and return to the main Desktop Protector window.
Cancel	Click to discard your changes and return to the Desktop Protector window.
Apply	Click to save your changes and keep the current tab open.
Help	Displays the online Help for this tab.

The Back Trace Tab

Introduction

Back tracing is the process of tracing a network connection to its origin. When somebody connects to your system over 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. RealSecure Desktop Protector can read information from these packets and identify each router the intruder's packets had to travel through. Desktop Protector can often identify the intruder's system in this way.

For more information about setting your back tracing preferences, see "Introduction" on page 50.

Threshold

The threshold setting indicates the event severity level that will trigger a trace of the attack. Severity refers to the numeric level of each event.

- The default event severity for the indirect trace threshold is 3.
- The default event severity for the direct trace threshold is 6.

DNS lookup

When this option is selected, RealSecure Desktop Protector queries available DNS (Domain Name Service) servers for information about the intruder.

Note: DNS Lookup is enabled by default.

NetBIOS nodestatus

When this option is selected, Desktop Protector performs a NetBIOS lookup on the intruder's system.

Note: NetBIOS Node Status is enabled by default.

Back Trace Tab buttons

This table describes the buttons that appear on the Back Trace tab.

This button...	Has this effect...
OK	Click to save your changes and return to the main Desktop Protector window.
Cancel	Click to discard your changes and return to the Desktop Protector window.
Apply	Click to save your changes and keep the current tab open.
Help	Displays the online Help for this tab.

The Intrusion Detection Tab

Introduction

The Intrusion Detection tab allows you to control the IP addresses or intrusions the Desktop Protector engine trusts or ignores.

For information about trusting and ignoring, see "Trusting Intruders" on page 39 and "Ignoring Events" on page 40.

Intrusion Detection tab columns

This table describes the information that appears in the columns on the Intrusion Detection tab.

This column...	Contains this information...
Intruder IP	The IP address of the system you want to trust.
Intruder	The machine name of the system you want to trust.
Event name	The name of the event type you want to ignore.
Event ID	The standard numerical designation for the event type you want to ignore. You can look up the numerical Event ID in the **ID:** field of the Exclude from Reporting dialog.

Table 23: *Intrusion Detection tab columns*

Intrusion Detection tab buttons

This table describes the buttons that appear on the Intrusion Detection tab.

This button...	Has this effect...
Add	Click to open the Exclude from Reporting dialog. For information about using the Exclude from Reporting dialog to trust addresses or ignore events, see "Blocking Intrusions" on page 37.
Delete	Click to remove the Trust or Ignore instruction associated with the highlighted record.
Modify	Click to open the Exclude from Reporting dialog to make changes to the highlighted Trust or Ignore record.
OK	Click to save your changes and return to the main Desktop Protector window.
Cancel	Click to discard your changes and return to the Desktop Protector window.
Apply	Click to save your changes and keep the current tab open.
Help	Displays the online Help for this tab.

Table 24: *Intrusion Detection tab buttons*

The ICEcap Tab

Introduction

The ICEcap tab allows you to manually control how RealSecure Desktop Protector reports intrusion information to an ICEcap server. When ICEcap reporting is enabled, all events are reported to an ICEcap server for enterprise-wide reporting and analysis. For more information, see "Connecting to ICEcap Manager" on page 32.

ICEcap tab features

This table describes the settings you can configure on the ICEcap tab.

This setting...	Has this effect...
Reporting Enabled	Select this box to enable ICEcap reporting. Clear this box to turn off ICEcap reporting. **Caution**: Clearing **Reporting Enabled** on the ICEcap tab disconnects Desktop Protector from the ICEcap server. This stops all event reporting to ICEcap. It also prevents ICEcap from downloading any configuration, security or software updates to the local Desktop Protector installation.
URL	The fully qualified URL for the ICEcap server, in the format `http://<ICEcap server name>:<HTTP event port number>`. For example, if ICEcap is on a server named ICECAP using event port 8082, then the entry would be `http://ICECAP:8082` (the default). You can use the ICEcap server's IP address or DNS name.
Account Name	The ICEcap account name to use when Desktop Protector uploads data. Refer to your ICEcap documentation for more information about account names. The default account name is iceman.
Event Password	Enter the current ICEcap event password. This is the password that Desktop Protector uses to report events to the ICEcap server.
Group Name	The ICEcap group of which the local system is a member, for event reporting purposes. This group must exist in ICEcap and possess the correct configuration settings to report properly. See the *RealSecure ICEcap Manager User Guide* for more information about Groups and group name precedence settings.
Proxy URL	If there is a proxy server between the local system and the ICEcap server, enter the fully qualified URL for the proxy server. If you are not using a proxy server, leave this field blank.
Configuration Priority	Displays the current status of configuration sharing with ICEcap. It is for informational purposes only and is always disabled.
Enable Local Configuration Editing	If this box is selected, the local system has some control or total control over the local configuration settings. If ICEcap reporting is enabled, ICEcap Manager controls this setting and it cannot be changed from the local computer. For more information on shared configuration, see "How ICEcap Manager Works With RealSecure Desktop Protector" on page 14.
Configuration Priority	If **Enable Local Configuration Editing** is selected, one of these option buttons is selected: • **Local**: The agent has complete control over all the local configuration settings. • **Remote**: The agent can only add configuration settings that ICEcap has not already explicitly set.

Table 25: *ICEcap tab settings*

This setting...	Has this effect...
Last Status	Shows the result of RealSecure Desktop Protector's last attempt to check in with the ICEcap server, at the time displayed in the **Time** field. One of these results appears: • **OK**: Your computer is communicating normally with ICEcap Manager. • **Authentication Failure**: The agent was unable to prove its authenticity with the ICEcap server. • **Abort**: The last attempt to communicate was cut off before it was complete. • **Connection Failure**: The local agent was unable to connect to ICEcap Manager.

Table 25: *ICEcap tab settings*

ICEcap tab buttons

This table describes the buttons that appear on the ICEcap tab.

This button...	Has this effect...
OK	Click to save your changes and return to the main Desktop Protector window.
Cancel	Click to discard your changes and return to the Desktop Protector window.
Apply	Click to save your changes and keep the current tab open.
Help	Displays the online Help for this tab.

The Notifications Tab

Introduction

The Notifications tab allows you to control some interface and notification functions.

Notification settings

This table describes the settings you can configure on the Notifications tab:

This setting...	Has this effect...
Event Notification	Desktop Protector alarm preferences control how and when the application notifies you of an event
Visible Indicator	Enables the Desktop Protector System Tray icon to flash when an event is reported.The visible indicator is triggered only if Desktop Protector is closed or hidden. Select the option button that includes the types of events you want the system to trigger an alert for.
Audible Indicator	Enables Desktop Protector to play a `.wav` file when an event is reported. The audible alarm is triggered whether the Desktop Protector window is open or closed. Select the option button that includes the types of events you want the system to trigger an alarm for.
WAV File	If the Audible Indicator option is selected, use this field to define the `.wav` file. Click the folder icon to select a `.wav` file.
Preview	Click to listen to the selected alert `.wav` file. This feature is only enabled if the Audible Indicator option is selected.must have a sound card and speakers to play the audible alarm.

Table 26: *Notifications tab settings*

For more information about choosing your notification settings, see "Controlling Event Notification" on page 48.

Notifications tab buttons

This table describes the buttons that appear on the Notifications tab.

This button...	Has this effect...
OK	Click to save your changes and return to the main Desktop Protector window.
Cancel	Click to discard your changes and return to the Desktop Protector window.
Apply	Click to save your changes and keep the current tab open.
Help	Displays the online Help for this tab.

The Prompts Tab

Introduction

The Prompts tab enables you to choose the level of feedback you want from the RealSecure Desktop Protector user interface.

Prompts tab settings

This table describes the settings on the Prompts tab:

This setting...	Has this effect...
Show Confirm Dialogs	Select this option to have Desktop Protector prompt for confirmation when you delete items, clear the event list, and make other significant changes to Desktop Protector. Clear to turn off such confirmations. By default, this check box is enabled.
Tooltips	A Tooltip is the descriptive text that appears when the mouse cursor hovers over a user interface item. Select the option that will give you the level of information you need. To show information appropriate to a new user, click **Beginner**. To show information useful for a user who is familiar with computers, click **Intermediate**. To hide these Tooltips, click **None**. By default, **Beginner** is selected.
Show Prompt When Service Stopped	Select this option to have Desktop Protector remind you when the BlackICE intrusion detection engine is stopped and your computer is unprotected. When you restart your system after you have stopped the BlackICE service, Desktop Protector asks if you want to restart the service. Click **Yes** to restart Desktop Protector. To instruct Desktop Protector not to remind you when the service is stopped, select **Don't ask me again**.

Table 27: *Prompts tab settings*

The Application Control Tab

Introduction

Use the Application Control tab to prevent unauthorized applications from starting on your system.

Enable Application Protection

When **Enable Application Protection** is selected, Desktop Protector monitors your system for unauthorized applications. This option is cleared by default.

Note: Enabling or disabling this feature also enables or disables the Communications Control feature. See "The Communications Control Tab" on page 86.

For information on how to manage your Application Protection settings, see "Working with the Application Protection Baseline" on page 42.

ICEcap control

If the **Enable Application Protection** option is dimmed, ICEcap Manager to which this Desktop Protector installation reports has blocked the local user from starting or stopping Application Control from the local system. Application Control can be started or stopped only by a remote command from ICEcap.

Application Control settings

This table describes the settings you can configure on the Application Control tab.

This setting...	Has this effect...
When an unknown application starts:	
Ask me what to do	When an application that is not in your system baseline attempts to start, Desktop Protector asks you if you want to shut it down.
Always terminate the application	When an application that is not in your baseline attempts to start, Desktop Protector shuts it down.
When a modified application starts:	
Ask me what to do	An application is in your baseline but has been modified since the last time you created or updated your baseline. When the application attempts to start, Desktop Protector asks you if you want to shut it down.
Always terminate the application	An application is in your baseline but has been modified since the last time you created or updated your baseline. When the application attempts to start, Desktop Protector shuts it down.

Protect Agent Files

When **Protect Agent Files** is selected, RealSecure Desktop Protector locks the BlackICE program files and the files that contain your known applications list and communications control settings. Only Desktop Protector can write to these files.

More information

For more information on how to choose your Application Control options, see "Working with the Application Protection Baseline" on page 42 and "Advanced Application Protection Settings" on page 99.

Application Control tab buttons

This table describes the buttons that appear on the Application Control tab.

This button...	Has this effect...
OK	Click to save your changes and return to the main Desktop Protector window.
Cancel	Click to discard your changes and return to the Desktop Protector window.
Apply	Click to save your changes and keep the current tab open.
Help	Displays the online Help for this tab.

The Communications Control Tab

Introduction

Use the Communications Control tab to prevent programs on your system from contacting a network without your knowledge.

Enable Application Protection

When **Enable Application Protection** is selected, the RealSecure Desktop Protector Application Protection component is running. This option is cleared by default.

Note: Enabling or disabling this feature also enables or disables the Application Control feature. See "The Application Control Tab" on page 84.

Communications Control Enabled

If **Communications Control Enabled** is checked, RealSecure Desktop Protector blocks outbound transmissions according to your instructions or those of ICEcap Manager to which this agent reports.

ICEcap control

If the **Communications Control Enabled** checkbox is dimmed, ICEcap Manager to which this Desktop Protector installation reports has blocked the local user from starting or stopping communications control from the local system. Communications control can be started or stopped only by a remote command from ICEcap.

Communications Control Settings

Your selection of an option on the Communications Control tab determines what Desktop Protector does about all future relevant events. You have these choices:

This setting...	Has this effect...
When an unauthorized application attempts to access the network:	
Always terminate the application	When any application you have not previously authorized to contact a network tries to send a transmission, Desktop Protector shuts down the application.
Prompt before terminating the application	When an unauthorized application tries to send a transmission, Desktop Protector asks you if you want to shut down the application.
Always block network access for the application	When an unauthorized application tries to send a transmission, Desktop Protector prevents the transmission.
Prompt before blocking network access for the application	When an unauthorized application tries to send a transmission, Desktop Protector asks you if you want to prevent the transmission.

For information about how to choose an option, see "Configuring Communications Control" on page 46.

Communications Control List buttons

This table describes the buttons that appear on the Communications Control tab.

This button...	Has this effect...
OK	Click to save your changes and return to the main Desktop Protector window.

This button...	Has this effect...
Cancel	Click to discard your changes and return to the Desktop Protector window.
Apply	Click to save your changes and keep the current tab open.
Help	Displays the online Help for this tab.

Appendix C

Advanced Firewall Settings

Overview

Introduction

You can use the Advanced Firewall Settings window to block intruders or ports or to configure Desktop Protector to dynamically switch protection levels.

- When you block an intruder, RealSecure Desktop Protector creates an IP address entry in your firewall that prevents all traffic from that IP address from entering your system.
- When you block a port, Desktop Protector creates a port entry in your firewall that prevents any traffic from entering through that port.
- When you set up adaptive protection, Desktop Protector automatically switches protection levels according to the risks associated with the network environment you are in.

In this Appendix

This chapter contains the following topics:

The Firewall Rules Tab

Introduction

Use the IP Address tab to create, modify and delete firewall settings for IP addresses and ports. Add and remove addresses or ports from the firewall list as necessary to modify and protect your system.

Caution: This firewall editor is intended only for users with advanced computer networking experience.

Sorting

Click a column header to sort the list by that column. Click the column header again to reverse the sort order.

Column descriptions

The following table describes the columns on the Advanced Firewall Settings window:

This column...	Contains this information...
Icon	A visual representation of the firewall setting. Green indicates that all communication is accepted from the address. A slash through the icon indicates that the IP address is blocked and all network traffic from that system is rejected.
Owner	Shows who created the firewall entry. Entries generated through the Desktop Protector automatic blocking feature display auto. Entries created manually from the Desktop Protector user interface show “BIgui.”
Address	The IP address of the accepted or blocked system. If the firewall entry is for a port, the word ALL appears.
Port	The accepted or rejected port number. If the firewall entry is for an IP address, the word ALL appears.
Type	The type of port: UDP or TCP.
Start Time	The date and time the setting was created, in MM/DD/YY hh:mm:ss format. Times are in 24-hour format.
End Time	The termination time and date for the setting in MM/DD/YY hh:mm:ss format. Times are in 24-hour format. Permanent settings show the text PERPETUAL.
Name	The best name Desktop Protector has for the IP address. This may be a DNS or NetBIOS (WINS) name. **Note**: If the setting was configured from the Advanced Firewall Settings screen, this column is empty.

Table 28: *Advanced Firewall Settings window columns*

Buttons

The following table describes the buttons on the IP Address tab:

This button...	Has this effect...
Options	To be notified when Desktop Protector is about to stop blocking an IP address, select Warn Before Block Expires.
Add	To manually add a new IP address filter or a new port configuration, click Add. The Add Firewall Entry window appears. For information on managing individual IP addresses, “Blocking Intrusions” on page 37.
Delete	To delete a firewall setting, select the setting and click Delete. Click Yes to remove the IP address from the Desktop Protector firewall.
Modify	Select a firewall setting to change and click Modify. A Modify Firewall Entry window appears.

Table 29: *Advanced Firewall Settings window buttons*

Shortcut menu

These commands are available when you right-click an item in the firewall list:

Note: The Accept and Reject settings produce different shortcut options.

This command...	Has this effect...
Unblock Only	Removes a blocked address from the firewall.
Unblock and Accept	Changes the blocked addresses' firewall setting from Reject to Accept.
Unblock, Accept and Trust	Changes the entry's firewall setting from Reject to Accept, and then trusts the address or port. When trusting the entry, the Desktop Protector intrusion detection engine ignores attacks from the address.
Modify	Opens a window that allows you to change the firewall setting.
Delete	Removes the accepted address from the firewall.
Cut	Removes the address from the list and copies the information to your system’s clipboard. You can paste the information into any application that accepts text input, such as a word processing or spreadsheet program.
Copy	Copies the selected address to your system’s clipboard. You can paste the information into any application that accepts text input, such as a word processing or spreadsheet program
Find	Searches the address list for information that you specify
Print	Sends the contents of the Advanced Firewall Settings window to the default printer in comma-separated text format.

Table 30: *Advanced Firewall Settings window shortcut commands*

The Local Adaptive Protection Tab

Use this tab to configure your firewall to switch protection levels dynamically. When your firewall detects a connection, and your computer is using one of the IP addresses specified on this tab, your firewall automatically switches to the appropriate protection level.

Options

This table describes the options available on the Adaptive Protection tab:

Group	Description
Paranoid	When your computer identifies itself with an IP address in any of these fields to connect to a remote system, the firewall switches to the Paranoid protection level.
Nervous	When your computer identifies itself with an IP address in any of these fields to connect to a remote system, the firewall switches to Nervous.
Cautious	When your computer identifies itself with an IP address in any of these fields to connect to a remote system, the firewall switches to Cautious.
Trusting	When your computer identifies itself with an IP address in any of these fields to connect to a remote system, the firewall switches to Trusting.

Buttons

This table describes the functionality of the buttons on the Adaptive Protection tab:

This button...	Has this effect...
OK	Saves the settings and closes the Advanced Firewall Settings window.
Cancel	Closes the Advanced Firewall Settings window without saving any changes.
Apply	Saves any changes but does not close the Advanced Firewall Settings window.
Help	Opens the Help for this window.

The Remote Adaptive Protection Tab

When your firewall detects a connection with a remote system that is using one of the IP addresses specified on this tab, your firewall automatically switches to the appropriate protection level.

Options

This table describes the options available on the Adaptive Protection tab:

Group	Description
Paranoid	A connection with a remote system at an IP address in any of these fields triggers the firewall to switch to the Paranoid protection level.
Nervous	A connection with a remote system at an IP address in any of these fields triggers the firewall to switch to Nervous.
Cautious	A connection with a remote system at an IP address in any of these fields triggers the firewall to switch to Cautious.
Trusting	A connection with a remote system at an IP address in any of these fields triggers the firewall to switch to Trusting.

Buttons

This table describes the functionality of the buttons on the Adaptive Protection tab:

This button...	Has this effect...
OK	Saves the settings and closes the Advanced Firewall Settings window.
Cancel	Closes the Advanced Firewall Settings window without saving any changes.
Apply	Saves any changes but does not close the Advanced Firewall Settings window.
Help	Opens the Help for this window.

The Add Firewall Entry Dialog

Introduction

Use this dialog to create or change firewall settings that block or accept IP addresses.

Add Firewall Entry dialog settings

The Add Firewall Entry dialog features these fields:

This field...	Contains...
Name	The descriptive name for the filter. It is a good idea to use the name of the potential intruder or of the protocol or software using the port, such as “SMTP” or “Quake.”
IP Address	The IP Address to block or accept. You can enter IP address ranges. Use the format `0.0.0.0-1.1.1.1` to enter a range.
All Addresses	When selected, blocks all IP addresses from communicating with your computer through a specified port.
Port	The port to block or accept. This must be a whole value between `1` and `65535`.
All Ports	When selected, closes off all ports on your computer to communications from a specific IP address.
Type	The type of address or port. If you need to create an entry for multiple types, you must create a separate filter for each type. Choose from: • IP • TCP • UDP
Mode	The type of firewall setting. Choose from: • Accept • Reject
Add Trusted Address Entry	When checked, trusts the specified address. Trusted addresses are completely free from any intrusion monitoring. Leaving the address untrusted allows Desktop Protector to report events from the address. **Note**: Only available when **Accept** is selected.
Duration of Rule	The duration of the firewall block. Choose from: • Hour • Day • Month • Forever All limited durations begin at the time the firewall entry is created.

Table 31: *Add Firewall Settings dialog features*

Add Firewall Entry dialog buttons

The Add Firewall Entry dialog has these buttons:

This button...	Has this effect...
Add	Click to create the firewall entry.
Cancel	Closes the window without saving the setting.

Table 32: *Add Firewall Settings dialog buttons*

The Modify Firewall Entry Dialog

Introduction

Use this dialog to change a firewall setting that you have set up previously.

Modify Firewall Entry dialog settings

The Modify Firewall Entry dialog features these fields:

This field...	Contains...
Name	The descriptive name for the filter. It is a good idea to use the name of the potential intruder or of the protocol or software using the port, such as “SMTP” or “Quake.”
IP Address	The IP Address to block or accept. You can enter IP address ranges. Use the format 0.0.0.0-1.1.1.1 to enter a range.
All Addresses	When checked, blocks all IP addresses from communicating with your computer through a specified port.
Port	The port to block or accept. This must be a whole value between 1 and 65536.
All Ports	When selected, closes off all ports on your computer to communications from a specific IP address.
Type	The type of address or port. If you need to create an entry for multiple types, you must create a separate filter for each type. Choose from: • IP • TCP • UDP
Mode	The type of firewall setting. Choose from: • Accept • Reject
Add Trusted Address Entry	When checked, trusts the specified address. Trusted addresses are completely free from any intrusion monitoring. Leaving the address untrusted allows Desktop Protector to report events from the address. **Note**: Only available when Accept is selected.
Duration of Rule	The duration of the firewall block. Choose from: • Hour • Day • Month • Forever All limited durations begin at the time the firewall entry is created.

Table 33: *Modify Firewall Settings dialog features*

Modify Firewall Entry dialog buttons

The Modify Firewall Entry dialog has these buttons:

This button...	Has this effect...
Add	Click to create the firewall entry.
Cancel	Closes the window without saving the setting.

Table 34: *Modify Firewall Settings dialog buttons*

Appendix D

Advanced Application Protection Settings

Overview

Introduction

The Advanced Application Settings window lets you control which applications can start on your system and which applications can connect to a network, such as the Internet.

- For information about controlling applications on your system, see "Working with the Application Protection Baseline" on page 42 and "The Application Control Tab" on page 84.
- For information about controlling network access from your system, see "Configuring Communications Control" on page 46 and "The Communications Control Tab" on page 86.

In this Appendix

This Appendix contains the following topics:

Advanced Application Settings window buttons

.The Advanced Application Settings window has these buttons:

This button...	Has this effect...
Save Changes	Click to save the settings you chose on the Known Applications tab.
Run Baseline	Click to have Desktop Protector inspect your computer according to the instructions you set on the Baseline tab.
Help	Click to open the online help for this screen.

Table 35: *Advanced Application Protection Settings window buttons*

Advanced Application Settings window menu commands

The Advanced Application Protection Settings window features these menus:

This command...	Has this effect...
File menu	
Run Baseline	Executes the choices you have made on the Baseline tab.
Save Changes	Records the settings you have made Known Applications tab.
Exit	Closes the Advanced Application Protection Settings window without saving any changes.
Tools menu	
Checksum extensions	Opens the Checksum Extensions dialog. You can use this dialog to control what kinds of application files Desktop Protector detects. For information about how to do this, see “Adding file types to the baseline” on page 44.
Find	Searches the Filenames column for the text you specify.
Help menu	
BlackICE Help Topics	Displays the Desktop Protector online Help.
Online Support	Starts your Web browser and points it to a collection of frequently asked questions (FAQ) about Desktop Protector on the ISS Web site.
WWW.ISS.NET	Starts your browser and points it to the ISS Web site, www.iss.net, which contains the latest information about RealSecure Desktop Protector.
About Protection Settings	Displays information about this version of the Desktop Protector application protection module.

Table 36: *Advanced Application Settings window menu commands*

The Known Applications Tab

Introduction

The Known Applications tab shows the application files Desktop Protector has detected on your system. If an application not on this list attempts to start, Desktop Protector alerts you or automatically closes the application, depending on the options you selected on the Application Control tab. For more information, see "Working with the Application Protection Baseline" on page 42 and "The Application Control Tab" on page 84

Known Applications tab columns

The information in the file pane appears in the following columns:

This column...	Contains this information...
Filename	The name of the application file. Click the Filename column header to sort the display by this column.
Path	The location of the application file on your system.
Application Control	To automatically close down the application when it attempts to start, select **Terminate**. To let the application run, leave the option blank.
Communications Control	To prevent this application from accessing a network, set the option to **Block**. To shut down this application when it attempts to contact a network, set the option to **Terminate**. To allow this application to access a network, leave the option blank.
Company	The vendor of the application file.
Product	The name of the application.
Number of Versions	Number of times the file has been replaced or upgraded.

Table 37: *Advanced Application Settings window file pane columns*

The Baseline Tab

Introduction

The Baseline tab allows you to control how RealSecure Desktop Protector inspects your system for application files.

The system tree pane

The system tree pane shows the drives and directories RealSecure Desktop Protector has found on your system. To see the application files in a directory, check the box next to the directory name. To view all the application files on a drive, check the box next to the drive name.

The file pane

The file pane shows all the application files Desktop Protector has detected on your system. To have Desktop Protector search a drive or directory, check the box next to the drive or directory name.

The Checksum Extensions Dialog

Introduction

The Checksum Extensions dialog enables you to customize the application file types that RealSecure Desktop Protector lists when it inspects your system. Desktop Protector determines which files are included in the baseline from the file name's extension (the three characters after the period).

Checksum Extensions dialog fields

The information in the file pane appears in this field:

Field	Information
Extensions	In the text box, enter the three-character extension for an application type you want Desktop Protector to track. The box below contains the extensions for the application types that Desktop Protector already looks for. By default, Desktop Protector records these application types: • **dll**: dynamic link library, a collection of resources that enable a program file to do its job • **drv**: driver, a small program that enables a device or service to work • **exe**: executable file, containing program instructions • **ocx**: special-purpose program for functions such as scroll bar movement and window resizing in Windows applications • **scr**: screensaver program • **sys**: files that control basic operating system functions • **vxd**: “virtual device” that enables other software to work

Table 38: *Information fields on the Checksum Extensions dialog*

Checksum Extensions dialog buttons

The Checksum Extensions dialog includes these buttons:

This button...	Has this effect...
Add	To add a file type to your system baseline, enter an extension in the Extensions: text box and click **Add**.
Delete	To have Desktop Protector ignore a file type when it creates your baseline, highlight the file type and click **Enter**.
OK	Saves your settings and closes the Checksum Extensions dialog.
Cancel	Closes the Checksum Extensions dialog without saving any changes.
Help	Opens this online help system.

Table 39: *Buttons on the Checksum Extensions dialog*

Appendix E

The Main Menu

Overview

Introduction

The Main Menu appears above the information tabs. This Appendix explains how to use the menu options to control the appearance and operation of Desktop Protector features.

In this Appendix

This Appendix contains the following topics:

The File Menu

Introduction

Use the File menu to control the essential operations of RealSecure Desktop Protector.

Print...

Print sends information from Desktop Protector to your default printer. To print information about an event or intruder:

1. On the Events or Intruders tab, select an event or intruder.
2. Click **Print**.
3. In the Print window, choose a printer and the desired number of copies, and then click **OK**.

For more information about things you can do with Desktop Protector data, see "Back Tracing" on page 50.

Exit

Exit closes the Desktop Protector user interface. The Desktop Protector icon is removed from the task bar when you close the interface, but Desktop Protector continues to monitor for intrusions.

The Edit Menu

Introduction

Use the Edit menu to manipulate the intrusion records that RealSecure Desktop Protector gathers. For more information about ways you can use Desktop Protector data, see "Back Tracing" on page 50.

Cut

To cut an event or intruder:

- On the Events or Intruders tab, click an event or intruder, and then select **Cut** from the Edit menu.
  - Desktop Protector removes the entry from the list.
  - Desktop Protector copies the entry to your system's clipboard in comma-delimited text format.

Copy

To copy an event or intruder:

- On the Events or Intruders tab, click an event or intruder, and then select **Copy** from the Edit menu.

  Desktop Protector copies the information to your system's clipboard in comma-delimited text format.

Delete

To delete an event or intruder:

- On the Events or Intruders tab, click an event or intruder and select **Delete** from the Edit menu.

  Desktop Protector removes the entry from the list.

Select All

To select all events or intruders:

- On the Events or Intruders tab, click an event or intruder and choose **Select All** from the Edit menu.

  Desktop Protector highlights all the events you have viewed during this session.

Find…

To find events or intruders:

1. On the Events or Intruders tab, click an event or intruder and select **Find** from the Edit menu.
2. In the Find window, select **Match Whole Word Only** or **Match Case** to narrow your search terms.
   - To search only records above the highlighted record, click **Up**.
   - To search records below the highlighted record, click **Down**.

The View Menu

Introduction

Use the View menu to choose what items are displayed, and how, on the Events and Intruders lists.

Freeze

Stops Desktop Protector from refreshing the tab information. For more information, see "Freezing the Events list" on page 49.

Filter by Event Severity

Filters the types of attacks that are displayed.

To filter the types of attacks that are displayed:

1. On the Events or Intruders tab, select **Filter by Event Severity** from the View menu.
2. Choose the minimum severity level to see reported. For information about severity levels, see "Severity levels" on page 12.

For more information about filtering Desktop Protector data, see "Filtering the Events List" on page 48.

The Tools Menu

Introduction

The Tools menu enables you to configure the application by editing the settings; edit the Advanced Firewall settings; start or stop the BlackICE engine; clear the event list; or change other preferences.

Edit BlackICE Settings...

Displays the configuration tabs that control the operation of the Desktop Protector engine. For more information, see "Configuration Tabs" on page 69.

Stop BlackICE Engine

Turns off the Desktop Protector intrusion detection engine. If the intrusion detection engine is already stopped, this item is replaced with **Start BlackICE Engine**.

Note: If the **Stop BlackICE Engine** menu item is dimmed, the ICEcap Manager to which this Desktop Protector installation reports has blocked the local user from starting or stopping intrusion detection. The service can be started or stopped only by a remote command from ICEcap.

Stop BlackICE Application Protection

Turns off the Application Protection and Communications Control features. If Application Protection is already turned off, this command is replaced with **Start BlackICE Application Protection**. For more information, see "Working with the Application Protection Baseline" on page 42.

Note: If this menu item is dimmed, ICEcap Manager to which this agent reports has blocked the local user from starting or stopping the Application Protection service. Application Protection can be started or stopped only by a remote command from ICEcap.

Clear Files...

Deletes intrusion information by removing your list of intrusions, evidence logs or packet logs. For more information, see "Clearing the Events list" on page 48.

Advanced Firewall Settings

Displays the Advanced Firewall Settings window, which enables you to control which IP addresses or TCP/UDP port numbers Desktop Protector blocks or accepts. For more information, see "Blocking Intrusions" on page 37.

Advanced Application Protection Settings

Displays the Advanced Application Protection Settings window, with which you can control which applications can run on your system and which applications can access a network. For more information, see "Working with the Application Protection Baseline" on page 42.

The Help Menu

Introduction	The Help menu offers links to the Help, the ISS Web site, and information about Desktop Protector.
BlackICE Help Topics	Displays the Desktop Protector online Help.
Online Support	Starts your Web browser and points it to a collection of frequently asked questions (FAQ) about Desktop Protector on the ISS Web site.
WWW.ISS.NET	Starts your Web browser and points it to the ISS Web site, www.iss.net, which contains the latest information about RealSecure Desktop Protector and other ISS products.
About BlackICE	Displays your Desktop Protector license key and more information about your Desktop Protector version.
Support Knowledge Base	Starts your browser and points it to the advICE library, a collection of online security information at www.iss.net.

The System Tray Menu

Introduction

The system tray menu provides a quick way to access some key Desktop Protector functions. You can see this menu by right-clicking the Desktop Protector icon in the lower right corner of your screen.

View BlackICE Events

Opens the Desktop Protector user interface to the Events list, which displays information about recent intrusions. For more information, see "The Events Tab" on page 62.

Edit BlackICE Settings...

Opens the RealSecure Desktop Protector user interface to the settings dialog, from which you can select one of the configuration tabs. For information about any of the configuration tabs, see "Configuration Tabs" on page 69.

Advanced Firewall Settings

Opens the Desktop Protector user interface to the Advanced Firewall Settings window, which enables you to customize the IP addresses and ports that Desktop Protector blocks or accepts. For more information, see "Blocking Intrusions" on page 37.

Advanced Application Protection Settings

Opens the Advanced Application Protection settings window, where you can control which applications can run on your system or access a network. For more information, see "Working with the Application Protection Baseline" on page 42 or "Configuring Communications Control" on page 46.

Stop BlackICE Engine

Turns off the Desktop Protector intrusion detection functions. No incoming traffic is analyzed or blocked. If the intrusion detection engine is already stopped, this item is replaced with **Start BlackICE Engine**. For more information, see "Stopping Desktop Protector" on page 24.

Note: If the **Stop BlackICE Engine** menu item is dimmed, ICEcap Manager to which this Desktop Protector installation reports has blocked the local user from starting or stopping intrusion detection. The service can be started or stopped only by a remote command from ICEcap.

Stop BlackICE Application Protection

Turns off the Desktop Protector Application Protection feature. Desktop Protector does not warn you when unauthorized applications start, and no outbound traffic is analyzed or blocked. For more information, see "Working with the Application Protection Baseline" on page 42. If Application Protection is already turned off, this command is replaced with **Start BlackICE Application Protection**.

Note: If the **Stop Application Protection** menu item is dimmed, ICEcap Manager to which this Desktop Protector installation reports has blocked the local user from starting or stopping the Application Protection service. Application Protection can be started or stopped only by a remote command from ICEcap.

WWW.ISS.NET

Starts your browser and points it to the Internet Security Systems web site.

Exit

Closes the Desktop Protector user interface. This command does not stop the BlackICE intrusion detection engine or application control features. For more information, see "Stopping Desktop Protector" on page 24.

Index

a

b

c

d

e

f

h

i

m

n

o

p

r

s

t

u

v

w

Internet Security Systems, Inc. Software License Agreement

THIS SOFTWARE IS LICENSED, NOT SOLD. BY INSTALLING THIS SOFTWARE, YOU AGREE TO ALL OF THE PROVISIONS OF THIS SOFTWARE LICENSE AGREEMENT ("LICENSE"). IF YOU ARE NOT WILLING TO BE BOUND BY THIS LICENSE, RETURN ALL COPIES OF THE SOFTWARE AND LICENSE KEYS TO ISS WITHIN FIFTEEN (15) DAYS OF RECEIPT FOR A FULL REFUND OF ANY PAID LICENSE FEE. IF THE SOFTWARE WAS OBTAINED BY DOWNLOAD, YOU MAY CERTIFY DESTRUCTION OF ALL COPIES AND LICENSE KEYS IN LIEU OF RETURN.

1. License - Upon payment of the applicable fees, Internet Security Systems, Inc. ("ISS") grants to you as the only end user ("Licensee") a nonexclusive and nontransferable, limited license for the accompanying ISS software product in machine-readable form and the related documentation ("Software") for use only on the specific network configuration, for the number of devices, and for the time period ("Term") that are specified in Licensee's purchase order, as accepted by ISS, and the invoice and license key furnished by ISS. ISS limits use of Software based upon the number and type of devices upon which it may be installed, used, gather data from, or report on, depending upon the specific Software licensed. A device includes any network addressable device connected to Licensee's network, including remotely, including but not limited to personal computers, workstations, servers, routers, hubs and printers. Licensee may reproduce, install and use the Software on multiple devices, provided that the total number and type are authorized in Licensee's purchase order, as accepted by ISS, and the invoice and license key furnished by ISS. Licensee may make a reasonable number of backup copies of the Software solely for archival and disaster recovery purposes.
2. Covenants - ISS reserves all intellectual property rights in the Software. Licensee agrees: (a) the Software is owned by ISS and/or its licensors, is a valuable trade secret of ISS, and is protected by copyright laws and international treaty provisions; (b) to take all reasonable precautions to protect the Software from unauthorized access, disclosure, copying or use; (c) not to modify, adapt, translate, reverse engineer, decompile, disassemble, or otherwise attempt to discover the source code of the Software; (d) not to use ISS trademarks; (e) to reproduce all of ISS' and its licensors' copyright notices on any copies of the Software; and (f) not to transfer, lease, assign, sublicense, or distribute the Software or make it available for timesharing, service bureau, or on-line use.
3. Support and Maintenance - During the term for which Licensee has paid the applicable support and maintenance fees, ISS will, upon request, provide software maintenance and support services that it makes generally available under its then current Maintenance and Support Policy. Support and maintenance include telephone support and electronic delivery to Licensee of error corrections and updates to the Software (but NOT new releases or products that substantially increase functionality and are marketed separately) and documentation as described in ISS' then current Maintenance & Support Policy.
4. Limited Warranty - The commencement date of this limited warranty is the date on which ISS furnishes to Licensee the license key for the Software. For a period of ninety (90) days after the commencement date or for the Term (whichever is less), ISS warrants that the Licensed Software will conform to material operational specifications described in its then current documentation. However, this limited warranty shall not apply unless (i) the Software is installed, implemented, and operated in accordance with all written instructions and documentation supplied by ISS, (ii) Licensee notifies ISS in writing of any nonconformity within the warranty period, and (iii) Licensee has promptly and properly installed all corrections, new versions, and updates made available by ISS to Licensee. Furthermore, this limited warranty shall not apply to nonconformities arising from any of the following: (i) misuse of the Software, (ii) modification of the Software, (iii) failure by Licensee to utilize compatible computer and networking hardware and software, or (iv) interaction with software or firmware not provided by ISS. If Licensee timely notifies ISS in writing of any such nonconformity, then ISS shall repair or replace the Software or, if ISS determines that repair or replacement is impractical, ISS may terminate the applicable licenses and refund the applicable license fees, as the sole and exclusive remedies of Licensee for such nonconformity. **THIS WARRANTY GIVES LICENSEE SPECIFIC LEGAL RIGHTS, AND LICENSEE MAY ALSO HAVE OTHER RIGHTS THAT VARY FROM JURISDICTION TO JURISDICTION. ISS DOES NOT WARRANT THAT THE SOFTWARE WILL MEET LICENSEE'S REQUIREMENTS, THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT ALL SOFTWARE ERRORS WILL BE CORRECTED. LICENSEE UNDERSTANDS AND AGREES THAT LICENSED SOFTWARE IS NO GUARANTEE AGAINST INTRUSIONS, VIRUSES, TROJAN HORSES, WORMS, TIME BOMBS, CANCELBOTS OR OTHER SIMILAR HARMFUL OR DELETERIOUS PROGRAMMING ROUTINES AFFECTING LICENSEE'S NETWORK, OR THAT ALL SECURITY THREATS AND VULNERABILITIES WILL BE DETECTED OR THAT THE PERFORMANCE OF THE LICENSED SOFTWARE WILL RENDER LICENSEE'S SYSTEMS INVULNERABLE TO SECURITY BREACHES. THE REMEDIES SET OUT IN THIS SECTION 4 ARE THE SOLE AND EXCLUSIVE REMEDIES FOR BREACH OF THIS LIMITED WARRANTY.**
5. Warranty Disclaimer - **EXCEPT FOR THE LIMITED WARRANTY PROVIDED ABOVE, THE SOFTWARE IS PROVIDED "AS IS" AND ISS HEREBY DISCLAIMS ALL WARRANTIES, BOTH EXPRESS AND IMPLIED, INCLUDING IMPLIED WARRANTIES RESPECTING MERCHANTABILITY, TITLE, NONINFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE. SOME JURISDICTIONS DO NOT ALLOW DISCLAIMERS OF IMPLIED WARRANTIES, SO THE ABOVE LIMITATION MAY NOT APPLY TO LICENSEE. LICENSEE EXPRESSLY ACKNOWLEDGES THAT NO REPRESENTATIONS OTHER THAN THOSE CONTAINED IN THIS LICENSE HAVE BEEN MADE REGARDING THE GOODS OR SERVICES TO BE PROVIDED HEREUNDER, AND THAT LICENSEE HAS NOT RELIED ON ANY REPRESENTATION NOT EXPRESSLY SET OUT IN THIS LICENSE.**
6. Proprietary Rights - ISS represents and warrants that ISS has the authority to license the rights to the Software that are granted herein. ISS shall defend and indemnify Licensee from any final award of costs and damages against Licensee for any actions based on infringement of any U.S. copyright, trade secret, or patent as a result of the use or distribution of a current, unmodified version of the Software; but only if ISS is promptly notified in writing of any such suit or claim, and only if Licensee permits ISS to defend, compromise, or settle same, and only if Licensee provides all available information and reasonable assistance. The foregoing is the exclusive remedy of Licensee and states the entire liability of ISS with respect to claims of infringement or misappropriation relating to the Software.
7. Limitation of Liability - Licensee acknowledges that some of the Software is designed to test the security of computer networks and may disclose or create problems in the operation of the systems tested. Licensee accepts the risk of such possibility and hereby waives all rights, remedies, and causes of action against ISS and releases ISS from all liabilities arising therefrom. **ISS' ENTIRE LIABILITY FOR MONETARY DAMAGES ARISING OUT OF THIS LICENSE SHALL BE LIMITED TO THE AMOUNT OF THE LICENSE FEES ACTUALLY PAID BY LICENSEE UNDER THIS LICENSE, PRORATED OVER A THREE-YEAR TERM FROM THE DATE LICENSEE RECEIVED THE SOFTWARE. IN NO EVENT SHALL ISS BE LIABLE TO LICENSEE UNDER ANY THEORY INCLUDING CONTRACT AND TORT (INCLUDING NEGLIGENCE AND STRICT PRODUCTS LIABILITY) FOR ANY SPECIAL, PUNITIVE, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING, BUT NOT LIMITED TO, COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, DAMAGES FOR LOST PROFITS, LOSS OF DATA, LOSS OF USE, OR COMPUTER HARDWARE MALFUNCTION, EVEN IF ISS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.**
8. Termination - Licensee may terminate this License at any time by notifying ISS in writing. All rights granted under this License will terminate immediately, without prior written notice from ISS, at the end of the term of the license, if not perpetual. If Licensee fails to comply with any provisions of this License, ISS may immediately terminate this License if such default has not been cured within ten (10) days following written notice of default to Licensee. Upon termination or expiration of the License, Licensee shall cease all use of the Software and destroy all copies of the Software and associated documentation. Termination of this License shall not relieve Licensee of its obligation to pay all fees incurred prior to such termination and shall not limit either party from pursuing any other remedies available to it.
9. General Provisions - This License, together with the identification of the Software, pricing and payment terms stated in the applicable Licensee purchase order as accepted by ISS and ISS invoice and license key, constitute the entire agreement between the parties respecting its subject matter. Standard and other additional terms or conditions contained in any purchase order or similar document are hereby expressly rejected and shall have no force or effect. This License will be governed by the substantive laws of the State of Georgia, USA, excluding the application of its conflicts of law rules. This License will not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded. 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. This License may only be modified in writing signed by an authorized officer of ISS.
10. Notice to United States Government End Users - Licensee acknowledges that any Software furnished under this License is commercial computer software developed at private expense and is provided with RESTRICTED RIGHTS. Any use, modification, reproduction, display, release, duplication or disclosure of this commercial computer software by the United States Government or its agencies is subject to the terms, conditions and restrictions of this License in accordance with the United States Federal Acquisition Regulations at 48 C.F.R. Section 12.212 and Subsection 227.7202-3 or applicable subsequent regulations. Contractor/manufacturer is Internet Security Systems, Inc., 6303 Barfield Road, Atlanta, GA 30328, USA.
11. Export and Import Controls; Use Restrictions - Licensee will not transfer, export, or reexport the Software, 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. 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. 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 software 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 Software (customer_ops@iss.net). Licensee understands that the foregoing obligations are U.S. legal requirements and agrees that they shall survive any term or termination of this License.
12. Authority - Because the Software is designed to test or monitor the security of computer network systems and may disclose or create problems in the operation of the systems tested, Licensee and the persons acting for Licensee represent and warrant that: (a) they are fully authorized by the Licensee and the owners of the computer network for which the Software is licensed to enter into this License and to obtain and operate the Software in order to test and monitor that computer network; (b) the Licensee and the owners of that computer network understand and accept the risks involved; and (c) the Licensee shall procure and use the Software in accordance with all applicable laws, regulations and rules.

13. No High Risk Use - Licensee acknowledges that the Software is not fault tolerant and is not designed or intended for use in hazardous environments requiring fail-safe operation, including, but not limited to, aircraft navigation, air traffic control systems, weapon systems, life-support systems, nuclear facilities, or any other applications in which the failure of the Licensed Software could lead to death or personal injury, or severe physical or property damage. ISS disclaims any implied warranty of fitness for High Risk Use.

Revised May 14, 2002