# Contents

**Preface** ................................................................. v
  Overview ........................................................................... v
  About Network Sensor Documentation ................................ vi
  Conventions Used in this Guide ......................................... vii
  Getting Technical Support ............................................... viii

**Chapter 1: Introduction to the Network Sensor** ..................... 1
  Overview ........................................................................... 1
  About RealSecure and the Network Sensor ......................... 2
  Features of the Network Sensor ....................................... 5

**Chapter 2: Network Sensor Policies** ................................... 7
  Overview ........................................................................... 7
  About Network Sensor Policies ........................................ 8

**Chapter 3: Configuring Signatures** ..................................... 11
  Overview .......................................................................... 11
  About Signatures .............................................................. 12
  Editing Pre-Defined Signatures ......................................... 13
  Customizing Protocol Ports .............................................. 15
  Customizing Advanced Properties for Event Propagation ..... 16
  Monitoring Connection Events ......................................... 20
  Customizing Signatures for Connection Events .................. 23
  Using Filters ..................................................................... 24
  Using Packet Filters ......................................................... 25
  Using Event Filters .......................................................... 29
  Specifying IP Addresses for Connection Events and Filters ... 32
  Using Network Services ................................................... 33

**Chapter 4: Creating User-Defined Signatures** ....................... 35
  Overview .......................................................................... 35
  Creating User-Defined Signatures ..................................... 36
  Regular Expressions in User-Defined Signatures ................. 38
  Using the Context Box in User-Defined Signatures .............. 41

**Chapter 5: Troubleshooting** ............................................. 43
  Overview .......................................................................... 43
  Policy File Descriptions ................................................... 44
  Isolating Policy Problems ................................................ 46

**Appendix A: Context Descriptions for User-Defined Signatures** 53
  Overview .......................................................................... 53
  DNS_Query Context .......................................................... 55
  Email_Receiver Context .................................................... 56
  Email_Sender Context ....................................................... 57
  Email_Subject Context ...................................................... 58
  File_Name Context ........................................................... 59
  News_Group Context ........................................................ 60
  Password Context ............................................................ 61
Preface

Overview

Introduction
This guide introduces you to network sensor policies, policy files, and signatures. This guide also tells how the network sensor uses policies and signatures to protect your system from attacks and misuse.

Purpose
This policy guide describes how to use the RealSecure network sensor to protect your system from attacks and misuse.

Scope
This policy guide describes features that are specific to the network sensor. General information about RealSecure sensors, such as managing policies, configuring responses, and configuring sensors, is described in the RealSecure Workgroup Manager User Guide and the RealSecure SiteProtector Strategy Guide.

Audience
This guide is intended for current or new users of the RealSecure software.

What's new in this guide
This guide includes updated policy information.
About Network Sensor Documentation

Using this guide Please read this entire guide before configuring policies for the Network Sensor.

Related publications For additional information about network sensor, see the following publications:

- RealSecure Network Sensor and Gigabit Network Sensor Installation Guide
- RealSecure OS Sensor Policy Guide
- RealSecure Server Sensor Policy Guide
- RealSecure Workgroup Manager Installation Guide
- RealSecure Workgroup Manager User Guide
- RealSecure SiteProtector Strategy Guide
- RealSecure Help
- RealSecure SiteProtector Help
- ISS Response, Policy, and Event Collector Help
- Advanced Tuning Parameters Reference Document
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:

<table>
<thead>
<tr>
<th>Convention</th>
<th>What it Indicates</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bold</td>
<td>An element on the graphical user interface.</td>
<td>Type the computer’s address in the IP Address box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select the Print check box. Click OK.</td>
</tr>
<tr>
<td>SMALL CAPS</td>
<td>A key on the keyboard.</td>
<td>Press ENTER.</td>
</tr>
<tr>
<td>Constant width</td>
<td>A file name, folder name, path name, or other information that you must type exactly as shown.</td>
<td>Save the User.txt file in the Addresses folder.</td>
</tr>
<tr>
<td>Constant width</td>
<td>A file name, folder name, path name, or other information that you must supply.</td>
<td>Type Version number in the Identification information box.</td>
</tr>
<tr>
<td>Constant width</td>
<td>A file name, folder name, path name, or other information that you must supply.</td>
<td>Type Version number in the Identification information box.</td>
</tr>
<tr>
<td>Constant width italic</td>
<td>A file name, folder name, path name, or other information that you must supply.</td>
<td>From the taskbar, select Start→ Run.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>On the File menu, select Utilities→ Compare Documents.</td>
</tr>
</tbody>
</table>

Table 1: Typographic conventions for procedures

Command conventions

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

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

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:

<table>
<thead>
<tr>
<th>Location</th>
<th>Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Americas</td>
<td>24 hours a day</td>
</tr>
<tr>
<td>All other locations</td>
<td>Monday through Friday, 9:00 A.M. to 6:00 P.M. during their local time, excluding ISS published holidays</td>
</tr>
</tbody>
</table>

Note: If your local support office is located outside the Americas, you may call or email the Americas office for help during off-hours.

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

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

Table 3: Hours for technical support

Table 4: Contact information for technical support
Chapter 1

Introduction to the Network Sensor

Overview

Introduction This chapter introduces the RealSecure system and the network sensor.

In this chapter The chapter contains the following topics:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About RealSecure and the Network Sensor</td>
<td>2</td>
</tr>
<tr>
<td>Features of the Network Sensor</td>
<td>5</td>
</tr>
</tbody>
</table>
# About RealSecure and the Network Sensor

## Introduction

This section discusses the RealSecure system and the network sensor.

## RealSecure system

The RealSecure system is an automated, real-time intrusion detection and response system that unobtrusively analyzes activity across your computer systems and networks. A RealSecure system includes two major components:

- management
- sensors

## Management components

The management component serves the following purposes:

- visually monitors events (with a console)
- collects data from sensors (with one or more event collectors)
- stores data from sensors (in a database)

You must choose one of the following two types of management software to manage and monitor sensors:

- Workgroup Manager
- SiteProtector

This guide describes how to apply policies, using the Workgroup Manager.

## The Workgroup Manager

The Workgroup Manager consists of a console, asset database, event collector, and enterprise database.

**Reference:** For more information about the Workgroup Manager, see the *RealSecure Workgroup Manager User Guide*. For more information about using policies with SiteProtector, see the *RealSecure SiteProtector Strategy Guide* or the SiteProtector Help.

## RealSecure console

The console is the graphical user interface for the RealSecure system; you use the console to control any sensors the console is managing.

## Command Line Interface

If you do not have access to the console, you can use a command-line utility called the Command Line Interface (CLI) to manage your sensors. The CLI operates in the same way as another session of the RealSecure console.

**Reference:** For more information about using the Command Line Interface, see the *RealSecure Workgroup Manager User Guide*. For more information about installing the Command Line Interface, see the *RealSecure Network and Gigabit Network Sensor Installation Guide*.

## RealSecure sensors

Sensors monitor network and system traffic for attacks and other security-related events. Sensors respond to and notify you about these responses as they occur.

The RealSecure system provides three types of sensors:

- network sensor
- gigabit network sensor
- server sensor

**Network sensors**

Network sensors are specially designed to protect an entire network segment from intrusion. The network sensor monitors network packets and looks for events that could indicate an attack against your network.

**Gigabit network sensors**

The network sensor version 7.0 offers an optional high-performance gigabit packet driver. To enable the driver, you must purchase a gigabit network sensor license. When the driver is enabled, the network sensor uses a gigabit adapter for monitoring network traffic.

**Purchasing a license:** To purchase a license for the gigabit network sensor, contact your local sales representative.

**Server sensors**

For more information about server sensors, see the RealSecure Server Sensor Installation Guide or the RealSecure Server Sensor Policy Guide.

**What is a policy?**

A policy is a file that contains a list of items, called signatures, that determine what the sensor can detect.

**What is a signature?**

A signature is the internal code that the RealSecure system uses to detect an event, or series of events, that might signal an attack on your network or that can provide security-related information.

**Network segment definition**

A network segment, also known as a “collision domain,” is a part of your network that is shared among several devices. Each device on a segment can monitor all of the traffic going to other devices, but devices on other network segments cannot monitor this same traffic.

**Reference:** For information about how many network sensors you can install, see the RealSecure Network Sensor and Gigabit Network Sensor Installation Guide.
The following diagram shows how a set of sensors and a Workgroup Manager could be deployed on a network. Notice how network sensors protect from outside and from inside the firewall as well as on each network segment.

Figure 1: Example of RealSecure deployment
Features of the Network Sensor

Introduction
Like other sensors, the network sensor uses policies that control what the sensor monitors and how it responds to events that it detects. The features of the network sensor are controlled through these policies. You can either use the pre-defined policies that ship with the network sensor, or you can customize the policies.

When you customize policies, you can do the following:

- customize (fine-tune) pre-defined signatures
- determine how the sensor responds to events
- monitor attempted and successful network connections
- have the sensor ignore specific traffic to and from trusted computers
- create custom signatures to monitor specific activity that other signatures do not detect
- administer the network sensor from a command line

Reference: For information about pre-defined policies and the policy editor, see “About Network Sensor Policies” on page 8.

Customizing pre-defined signatures
In a network sensor policy, you can customize pre-defined signatures using two methods:

- control event propagation (Security Events)
- change the port numbers associated with protocol ports (Connection Events)

Event propagation
Event propagation is a method that the network sensor uses to determine if an event is really important or not. Event propagation reduces false positives and prevents the RealSecure console from being flooded with unnecessary events.

By using protocol ports, you can classify a set of port numbers and use this classification when modifying pre-defined or custom signatures.

Reference: For more information about customizing pre-defined signatures, see “Using Network Services” on page 33.

Determining responses
When an intrusion is detected, the RealSecure system can respond in the following ways:

- recording the date, time, source, and target of the event
- recording the content of the event
- notifying the network administrator
- reconfiguring the firewall
- terminating the event automatically

You can also create custom responses for the RealSecure system to use.

Reference: For more information about responses, see the “Working with Responses” chapter in the RealSecure Workgroup Manager User Guide.
### Chapter 1: Introduction to the Network Sensor

| **Monitoring network connections** | You can create custom signatures to monitor network connections. Unlike other signatures, connection event signatures monitor any connection to a particular port, regardless of the type of activity.  

**Reference:** For more information about connection events, see “Monitoring Connection Events” on page 20. |
| **Using filters to ignore specific traffic** | You can use filters to have the network sensor ignore traffic to or from certain systems or on certain port numbers, even if the traffic, under other circumstances, is considered a security risk.  

**Reference:** For more information about filters, see “Using Filters” on page 24, “Using Packet Filters” on page 25, and “Using Event Filters” on page 29. |
| **Creating custom signatures** | If you want to monitor an event that the standard RealSecure signatures cannot detect, you can create your own custom signature.  

**Reference:** For more information about creating custom signatures, see “Creating User-Defined Signatures” on page 36. |
| **Administering from the command line** | You can administer network sensors from the command line to apply changes to large numbers of sensors quickly.  

**Reference:** For more information, see the “Using the Command Line Interface” chapter in the RealSecure Workgroup Manager User Guide. |
| **Installing updates** | You can install RealSecure Updates (X-Press and product updates) to add new signatures or apply service releases, or to upgrade the network sensor to a new version.  

**Reference:** For more information, see the RealSecure Workgroup Manager User Guide. |
Chapter 2

Network Sensor Policies

Overview

Introduction

This chapter describes network sensor policies.

In this chapter

This chapter contains the following topics:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About Network Sensor Policies</td>
<td>8</td>
</tr>
</tbody>
</table>
About Network Sensor Policies

**Introduction**

This topic describes the following:

- the definition of a policy
- how to work with policies
- what signatures do
- the pre-defined RealSecure policies
- the location of policy files
- the names of policy files and troubleshooting

**Policy definition**

A policy is a file that contains a list of items, called signatures, that determine what the sensor can detect. Policies control the following sensor behaviors:

- the kind of security events a sensor detects
- the priority of each event
- how a sensor responds to security events

**How to work with policies**

You can view, create, and edit policies with the RealSecure console. You also use the console to apply new or updated policies to a sensor.

**Reference:** For general information about working with policies through the console, see the “Working with Policies” chapter in the *RealSecure Workgroup Manager User Guide*.

**SiteProtector users:** For information about working with policies in SiteProtector, see the *RealSecure SiteProtector Strategy Guide* or the SiteProtector Help.

**What signatures do**

The sensor uses a signature to detect a specific security event.

**Reference:** For more information about signatures, see “About Signatures” on page 12.

**Pre-defined policies**

When you install the network sensor, it contains several pre-defined policies that are configured for various environments. Table 5 describes these pre-defined policies.

**Note:** The variable X.X in the policy file names represents policy files from the previous version of the RealSecure software. When you upgrade from one version to the next, the upgrade installation renames the previous policy files to reflect the version number associated with those files.
These pre-defined policies are described in the following table:

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attacks And Audits (or Maximum Coverage X.X)</td>
<td>This policy is used for evaluation purposes. It sends all events to the console. Every signature is enabled and every session protocol signature is active. All of the events that the RealSecure system normally supports are also active. This policy can impose serious penalties on the performance of RealSecure network sensors and should be used only in evaluation environments. Attacks And Audits is not a good policy to use in a high traffic environment because all signatures are turned on and logged.</td>
</tr>
<tr>
<td>Attack Detector (or Attack Detector X.X)</td>
<td>A default policy in the RealSecure system. Using this policy, a RealSecure sensor focuses on network attacks only. Sessions are not decoded and connection events are not reported. On a secure network, sensors using this policy generate virtually no traffic. This policy is appropriate for Security Administrators who want to know only about the most severe network events.</td>
</tr>
<tr>
<td>Blank</td>
<td>This policy is a blank template that you can use to create a custom policy. There are no signatures enabled in the Blank policy. Using the Blank policy without enabling signatures provides no security. Use this policy only as a template.</td>
</tr>
<tr>
<td>DMZ Engine (DMZ Engine X.X)</td>
<td>Using this policy, the RealSecure system focuses on activity that occurs outside a firewall in the demilitarized zone (DMZ). This policy monitors for network attacks and attempted exploitation of typical internet protocols, such as HTTP, FTP, SMTP, POP, and DNS. This policy is appropriate for Security Administrators who want to carefully watch events happening outside the corporate firewall.</td>
</tr>
<tr>
<td>Engine Inside Firewall (or Engine Inside Firewall X.X)</td>
<td>Using this policy, a RealSecure sensor focuses on important signatures and protocols most likely to traverse the firewall. This policy is appropriate for Security Administrators who want to carefully watch events happening inside the corporate firewall.</td>
</tr>
<tr>
<td>For Windows Networks (or For Windows Networks X.X)</td>
<td>This policy includes a collection of attack signatures, session signatures, and filter rules that are specific to Windows networking environments. Several of the attacks that the RealSecure system can recognize are specific to Unix systems. If there are no Unix systems, then these signatures are not necessary. This policy includes signatures for networks that include only Windows devices.</td>
</tr>
<tr>
<td>Original X.X</td>
<td>This policy represents the default policy that a sensor originally used just after installation. You can view this policy to see the policy settings at sensor installation time. You can also use this policy to reset the sensor to its installation time policy settings.</td>
</tr>
<tr>
<td>Protocol Analyzer X.X</td>
<td>A default policy in the RealSecure system. This policy is the opposite of the Attack Detector policy. With the Protocol Analyzer policy, only the session decoding is active. Attack detection is inactive. This policy is appropriate for Security Administrators who want to understand how their network is being used. It might be appropriate for sensors installed on backbones or busy segments on networks with other RealSecure sensors that are providing attack-detection services.</td>
</tr>
</tbody>
</table>

Table 5: Pre-defined policy descriptions
Chapter 2: Network Sensor Policies

Location of policies
By default, network sensor policies reside in the following directory on the console computer:

C:\Program Files\ISS\RealSecure 6.5 Console\Network Policies

Important: If you make edits to these policy files using a text editor, ISS Customer Support can not help you recover or correct policy files if you encounter problems.

Names of policy files and troubleshooting
The sensor uses several files that control responses, policies, and other sensor configuration settings like encryption and communication with the Workgroup Manager.

Reference: For more information about these files and how the sensor uses them, see “Policy File Descriptions” on page 44.

### Table 5: Pre-defined policy descriptions (Continued)

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Recorder X.X</td>
<td>A default policy in the RealSecure system. This policy provides sample connection events for recording telnet, FTP, SMTP (e-mail) and NNTP (NetNews) sessions. To record a session, create a connection event for each side of the session. This policy provides functional examples that you can incorporate into customized policies.</td>
</tr>
<tr>
<td>Web Watcher X.X</td>
<td>A default policy in the RealSecure system. Sensors using the Web Watcher policy see all the HTTP traffic traversing the local network segment. Only the HTTP-based attack signatures are enabled with this policy. Other attack signatures are not active. This policy is appropriate for Security Administrators who want to gain a better understanding of the Web traffic on the network. It might also be appropriate for a sensor installed on a segment with Web servers only.</td>
</tr>
</tbody>
</table>
Chapter 3

Configuring Signatures

Overview

Introduction
This chapter describes how to configure pre-defined network sensor signatures, connection event signatures, and filters.

In this chapter
This chapter contains the following topics:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About Signatures</td>
<td>12</td>
</tr>
<tr>
<td>Editing Pre-Defined Signatures</td>
<td>13</td>
</tr>
<tr>
<td>Customizing Protocol Ports</td>
<td>15</td>
</tr>
<tr>
<td>Customizing Advanced Properties for Event Propagation</td>
<td>16</td>
</tr>
<tr>
<td>Monitoring Connection Events</td>
<td>20</td>
</tr>
<tr>
<td>Customizing Signatures for Connection Events</td>
<td>23</td>
</tr>
<tr>
<td>Using Filters</td>
<td>24</td>
</tr>
<tr>
<td>Using Packet Filters</td>
<td>25</td>
</tr>
<tr>
<td>Using Event Filters</td>
<td>29</td>
</tr>
<tr>
<td>Specifying IP Addresses for Connection Events and Filters</td>
<td>32</td>
</tr>
<tr>
<td>Using Network Services</td>
<td>33</td>
</tr>
</tbody>
</table>
Chapter 3: Configuring Signatures

About Signatures

Introduction

Configuring policies involves configuring and creating signatures. This topic describes the different types of signatures that you can configure.

Prerequisites to configuring signatures

You cannot customize signatures or create user-defined signatures for a pre-defined policy. You must derive a policy from a pre-defined policy or use a policy that you have already created.

Reference: To customize a policy, look up “policies, deriving” and “policies, customizing” in the Help index.

Signature organization

In the Workgroup Manager policy editor, the network sensor signatures are organized into five groups:

<table>
<thead>
<tr>
<th>Group</th>
<th>Group Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Events</td>
<td>Network traffic with content that can indicate an attack or other suspicious activity. These events are triggered when the network traffic matches one of the profiles in the active policy.</td>
</tr>
<tr>
<td>Connection Events</td>
<td>Network traffic that connects to the monitored network through a particular port, from a particular address, with a certain network protocol, etc. These connections are noted by the policy in the way they connect to the network, not because of their contents. Connection events do not necessarily constitute an attack or other suspicious activity, but are network occurrences that might be interesting to a Security Administrator.</td>
</tr>
<tr>
<td>User-Defined Events</td>
<td>You can define your own network events based on text pattern matching within specific context.</td>
</tr>
<tr>
<td>Packet Filters</td>
<td>Packet filters determine which packets the IDS (intrusion detection system) processes. The sensor reads a packet from the network and determines if the packet matches a packet filter. If the packet matches a filter, then the IDS does not process the packet.</td>
</tr>
<tr>
<td>Event Filters</td>
<td>Event filters work after the IDS processes packets and detects an event. When the IDS generates an event, the sensor determines if the event matches an event filter. If the event matches a filter, then the sensor disregards the event.</td>
</tr>
</tbody>
</table>

Table 6: Network sensor signature groups

The remainder of this chapter describes the configuration options related to all signatures except for those that are user-defined. For information about user-defined signatures, see Chapter 4, “Creating User-Defined Signatures,” on page 35.

Reference: For information about viewing policies with the RealSecure policy editor, look up “policies, opening” in the Help index.
Editing Pre-Defined Signatures

Introduction
This topic describes the following:

- definition of a pre-defined signature
- attributes of pre-defined signatures that you can customize

Reference: For procedural information about customizing policies, look up “policies, deriving” in the Help index.

Definition: Pre-defined signatures
Pre-defined signatures are contained in the pre-defined policies that are installed with the RealSecure console. The pre-defined network sensor signatures are listed on the Security Events tab in the policy editor.

Attributes you can customize
You can enable or disable pre-defined signatures. You can also customize the following attributes that are explained in detail in Table 7:

- priority events
- responses
- protocol ports
- advanced properties (event propagation)

Field descriptions
The following table describes the items on the Security Events tab:

<table>
<thead>
<tr>
<th>Field or Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Enables or disables the decode/attack signature.</td>
</tr>
<tr>
<td>Event</td>
<td>Specifies the decode/attack signature name.</td>
</tr>
</tbody>
</table>
| Priority        | Indicates the priority level assigned to the signature. This information is used to sort events into high, medium, and low priority and to generate reports.  
  Note: If you change the priority level, it also changes the window in which the event is displayed in the console. |
| Response        | Specifies the responses taken when the selected event occurs.  
  Reference: For more information about responses, see the "Working with Responses” chapter in the RealSecure Workgroup Manager User Guide. |
| Advanced        | Opens the Advanced Properties window. Customizes how often the sensor responds to similar events that occur within a small time frame and other advanced features of the signature.  
  Note: This button appears only after selecting a signature in the Security Events tab.  
  Reference: For more information about configuring advanced properties, see “Customizing Advanced Properties for Event Propagation” on page 16. |

Table 7: Field descriptions: Security Events tab
To configure a pre-defined signature:

1. Open the policy in which you want to modify a pre-defined signature.

   **Reference:** For information about how to open a policy, look up “policies, opening” in the Help.

2. Click the **Security Events** tab.

3. Double-click **Security Events** to open the list.

4. Select the signature that you want to configure.
   
   The properties of the signature appear in the right pane.

5. In the **Priority** box, set the priority of this signature.

6. In the **Responses** box, select the responses that you want the sensor to take when it detects this type of event.

   **Reference:** For information about each response, see the “Working with Responses” chapter in the *RealSecure Workgroup Manager User Guide*.

7. To reduce noise and false positives, click **Advanced Properties** and changes the settings for how responses are created.

   **Reference:** For more information about configuring advanced properties, see “Customizing Advanced Properties for Event Propagation” on page 16.

8. Repeat Steps 4 through 7 for each signature that you are changing.

9. From the **File** menu, click **Save**.
   
   A confirmation message appears.

10. Click **OK**.

11. From the **File** menu, click **Close**.

12. Apply the policy to the sensor(s) that you want to use the signature.

   **Reference:** To apply a policy, look up “policies, applying” in the Help.

---

### Table 7: Field descriptions: Security Events tab (Continued)

<table>
<thead>
<tr>
<th>Field or Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ports</td>
<td>Opens the Protocol Ports window. Used to specify port numbers that you want the sensor to associate with a particular protocol. <em>Reference:</em> For more information about using protocol ports, see the following section, “Customizing Protocol Ports,” on page 15.</td>
</tr>
<tr>
<td>Tuning</td>
<td>Opens the Sensor Tuning window.</td>
</tr>
</tbody>
</table>
# Customizing Protocol Ports

## Introduction
This section explains how to edit protocol ports.

## Definition: protocol ports
Protocol ports classify port numbers by protocol, by signature, or by any other type of classification. The Protocol Ports window enables you to change port numbers associated with these classifications.

## How does the sensor use protocol ports?
The sensor uses protocol ports to determine the ports that pre-defined signatures in each policy use.

## Can settings be shared?
Protocol ports are specific to each policy. The settings are not shared among policies.

## Can protocol ports be associated with signatures?
You cannot associate protocol ports with a user-defined signature or change the protocol port that a particular pre-defined signature uses.

## Procedure: Editing protocol ports
You can change the ports associated with a class of ports; you can make these changes on a policy-by-policy basis.

**Caution:** If you change the value of the ports, it will affect any signature that is using that port classification.

To edit protocol ports:

1. Open the policy in which you want to edit the protocol port.
2. Select the **Security Events** tab, and then click the name of any group in the Security Events folder.
   
   A list of signatures in that group appear in the right pane.
3. Click **Ports**.
   
   The Protocol Ports window appears.
4. Select the type of protocol port that you want to edit, and then click **Edit**.
   
   The Edit Protocol Ports window appears.
5. Type the ports you want to be associated with this protocol in the **Ports** box.
   - Use spaces to separate ports.
   - Use a dash to indicate a range of ports.
6. Click **OK**.
7. Click **OK** again to return to the policy editor.
8. Apply the policy to the sensor(s) that you want to use the signature.

**Reference:** To apply a policy, look up “policies, applying” in the Help.
Chapter 3: Configuring Signatures

Customizing Advanced Properties for Event Propagation

Introduction

This topic describes the following:

- when to customize advanced properties
- how the three types of advanced properties change the way a signature works
- how to customize the advanced properties of a signature
- field descriptions for each component in the Advanced Properties window

When to customize

The network sensor uses default settings to determine how often to respond to events. These settings vary from signature to signature so that you can get the most information with the least amount of redundant, or duplicate, responses. If you want the sensor to respond more frequently or less frequently to a particular signature, you can customize these settings by modifying the advanced properties of a signature.

Advanced property types

A network sensor signature has three types of advanced properties. You can customize all three. These property types appear in the Advanced Properties window:

- Event Propagation section
- Event Filtering section
- Optional Parameters list

Event Propagation section

In the Event Propagation section, you can control how the network sensor defines a duplicate event by selecting the port and address check boxes. The network sensor classifies a series of events between quiet periods as duplicates if they have matching information in the port and address boxes you selected. Quiet periods are the amount of time, in seconds, in which duplicate events no longer occur.

You can limit the number of responses the sensor creates when it detects duplicate events and prevents the network sensor from a denial of service attack with the Flood Protection check box.

Affected responses: All Event Propagation settings (except for Flood Protection) apply to all responses. The Flood Protection setting applies only to LOGDB and VIEWSESSION responses.

Event Filtering section

In the Event Filtering section on the Event Propagation tab, you can customize how frequently the network sensor creates responses when it detects duplicate events (events that contain matching criteria as defined by default in the sensor or customized in the Event Propagation section).

Controlling responses: You can control the frequency of LOGDB and VIEWSESSION responses by limiting the number of total responses created between quiet times in the Ignore duplicate events after box. You can control the frequency of all responses by adjusting the length of time considered to be quiet time in the Ignore duplicate events for box.

Optional Parameters list

The Optional Parameters list shows you all other features of this signature that you can customize. Each optional parameter has two parts:
Customizing Advanced Properties for Event Propagation

- parameter name and current value
- description name and parameter description

The parameter name and value are on the first line in the list. This value sets the parameter in the sensor. The description of how the parameter works is on the second line. This description tells you about the settings available to you in the parameter.

Reference: Additional information about optional parameters is sometimes documented in the Help description for the signature. For more information about optional parameters, click the Help button on the Optional Parameters list.

Field descriptions

The following table describes each field in the Advanced Properties window:

<table>
<thead>
<tr>
<th>Section</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event</td>
<td>Use Defaults</td>
<td>Configures the sensor to use its default settings for defining duplicate events. This default setting varies from event to event and is embedded in the sensor program, not in the policy file. To customize how the network sensor defines duplicate events, clear the check box and customize the settings with the port, address, and Flood Protection check boxes.</td>
</tr>
<tr>
<td></td>
<td>Use Source Address</td>
<td>Configures the sensor to compare the source addresses of multiple events that occur between quiet periods. If the source addresses are the same, then the events are treated as duplicates. If you use this parameter setting with other port and address settings, then all the criteria must be the same before two or more events are treated as duplicates.</td>
</tr>
</tbody>
</table>
|                 | Use Destination Address| Configures the sensor to compare the destination addresses of multiple events that occur between quiet periods. If the destination addresses are the same, then the events are treated as duplicates. If you use this parameter setting with other port and address settings, then all the criteria must be the same before two or more events are treated as duplicates. Include the destination address as a main parameter when you define an event. As in the Use Source Address field, you can use this alone or with the following:  
  - Use Source Address  
  - Use Source Port  
  - Use Destination Port |

Table 8: Field descriptions: Advanced Properties window
Chapter 3: Configuring Signatures

Flood Protection

Requests flood protection for the event. For the LOGDB and VIEWSESSION responses, selecting the Flood Protection box has the same effect as setting the Ignore duplicate events after box to 1.

When you select Flood Protection, the database and session log do not store similar (duplicate) events that happen around the same time, which prevents the database and log from being flooded with the same event.

Selecting Flood Protection also has many benefits that affect the internal response system of the network sensor. The sensor works more efficiently and is not flooded by packets in a denial of service attack.

If you want the database and session log to record more than just one event between quiet times (set by default or customized by you with the Ignore duplicate events for box), use Ignore duplicate events after instead of the Flood Protection. Keep in mind, however, that Ignore duplicate events after only protects LOGDB and VIEWSESSION responses in the network sensor from a denial of service attack, not the internal response system of the network sensor.

Flood protection applies to LOGDB and VIEWSESSION responses and internal responses in the network sensor.

Use Source Port

Configures the sensor to compare the source ports of multiple events that occur between quiet periods. If the source ports are the same, then the events are treated as duplicates.

If you use this parameter setting with other port and address settings, then all the criteria must be the same before two or more events are treated as duplicates.

Use Destination Port

Configures the sensor to compare the destination ports of multiple events that occur between quiet periods. If the destination ports are the same, then the events are treated as duplicates.

If you select this parameter setting with other port and address settings, then all the criteria must be the same before two or more events are treated as duplicates.

Table 8: Field descriptions: Advanced Properties window (Continued)
Customizing Advanced Properties for Event Propagation

**Procedure**

To customize advanced properties:

1. From the Sensor Properties window, select the policy containing the signature to customize.

2. Click **Customize**.
   
   The Policy Editor window appears.

3. Select the **Security Events** tab.

4. In the signature list in the left pane, click the name of the signature you want to modify.

5. Click **Advanced**.

   The Advanced Properties window appears.

6. Change the settings in the Event Propagation, Event Filtering, or Optional Parameters sections to configure how the RealSecure system responds to this event.

   **Reference:** For information about these sections, see “Customizing Advanced Properties for Event Propagation” on page 16.

7. Click **OK**.

<table>
<thead>
<tr>
<th>Section</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Filtering</td>
<td>Ignore duplicate events after</td>
<td>Limits the number of LOGDB and VIEWSESSION responses that the network sensor creates for duplicate events. Duplicate events are events that contain matching criteria as defined by default in the sensor or customized by you in the Event Propagation section. The sensor considers these events duplicates when they occur sequentially without a quiet period. Instead, you can specify that the sensor respond to only the first couple of instances of the event and ignore the rest of the duplicate events until the quiet period (specified by default in the sensor or by you in the <strong>Ignore Duplicate Events for</strong> box) has passed. This setting applies only to LOGDB and VIEWSESSION responses and does not affect any other responses. <strong>Reference:</strong> For more information and examples, refer to the RealSecure Help.</td>
</tr>
<tr>
<td></td>
<td>Ignore duplicate events for</td>
<td>Sets the quiet period that must pass before the sensor generates one or more responses to indicate that this event has occurred. A quiet period is the amount of time, in seconds, in which duplicate events (as defined by default in the sensor or customized by you in the event propagation settings) no longer occur. The sensor’s interval timer times the quiet period. When a duplicate event occurs before the quiet period has passed, the interval timer is reset to the number of seconds you specify. If the sensor has reached its response limit for duplicate events, then the sensor does not create another response to the event unless the event occurs after the quiet time has passed. <strong>Reference:</strong> For more information and examples, refer to the RealSecure Help.</td>
</tr>
</tbody>
</table>

**Table 8:** Field descriptions: Advanced Properties window (Continued)
Chapter 3: Configuring Signatures

Monitoring Connection Events

Introduction

This topic describes the following:

- definition of connection events
- connection event types
- field descriptions of the Connection Events tab
- how to configure connection events in a policy

Definition: connection events

A connection event occurs when one computer opens a connection to or from a port on a particular address. Unlike other events, the sensor notifies the console of a connection event whenever it detects an open connection on a specific port, regardless of the type of activity, type of network packets, or content of the network packets that are exchanged.

Example: If you enable an FTP connection event signature, the sensor alerts the console when it detects any FTP connection, regardless of whether the content of the connection indicates an attack or other malicious behavior.

Connection event types

The network sensor policy contains pre-defined connection event signatures for different types of connections, such as WWW, FTP, or IRC. By default, the policy has two signatures for each type of connection event so that you can configure one signature for incoming traffic and another signature for outgoing traffic.

You can create your own custom connection event signatures if the pre-defined signatures do not cover the traffic you need to monitor.

Connection events and your policy

By default, no connection event signatures are enabled in a policy. If you want the network sensor to monitor connection events, you must enable and configure (if necessary) one or more connection event signatures.

Field descriptions

The following table describes the items on the Connection Events tab:

<table>
<thead>
<tr>
<th>Field or Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Enables or disables the decode/attack signature.</td>
</tr>
<tr>
<td>Event</td>
<td>Specifies the decode/attack name.</td>
</tr>
<tr>
<td>Priority</td>
<td>Indicates the priority level of each signature. This information is used to sort events into high, medium, and low priority and to generate reports. <strong>Note:</strong> If you change the priority level, it also changes the window in which the event is displayed in the console.</td>
</tr>
<tr>
<td>Response</td>
<td>Specifies the responses taken when the selected event occurs. Configures the sensor to respond when it detects an event that matches the signature. Each signature can have a combination of responses or no response at all. <strong>Reference:</strong> For more information about responses, see the “Working with Responses” chapter in the <em>RealSecure Workgroup Manager User Guide</em>.</td>
</tr>
</tbody>
</table>

Table 9: Field descriptions: Connection Events tab
To configure a connection event signature:

1. Open the policy to which you want to add a connection event signature.

   **Reference:** For information about how to open a policy, look up “policies, opening” in the Help.

2. Click the **Connection Events** tab.

3. Do one of the following:

   a. **Select the type of protocol that the connection uses from the Protocol box.**
   
   b. **Set the priority of this signature in the Priority box.**
   
   c. **Configure the source and destination information.**

   **Reference:** For more information about configuring the source and destination information, see “Specifying IP Addresses for Connection Events and Filters” on page 32 and “Using Network Services” on page 33.

4. Select the type of protocol that the connection uses from the **Protocol** box.

5. Set the priority of this signature in the **Priority** box.

6. Configure the source and destination information.

   **Reference:** For more information about configuring the source and destination information, see “Specifying IP Addresses for Connection Events and Filters” on page 32 and “Using Network Services” on page 33.

7. Select the responses that you want the sensor to take when it detects this type of connection.
Chapter 3: Configuring Signatures

Reference: For information about each response, see the “Working with Responses” chapter in the RealSecure Workgroup Manager User Guide.

8. Click **Save**.

9. Apply the policy to the sensor(s) that will use the new connection event signature.

Reference: To apply a policy, look up “policies, applying” in the Help.
Customizing Signatures for Connection Events

Introduction

This topic describes how to customize signatures on the Connection Events tab so that a policy matches your security plan needs.

Note: You cannot customize a pre-defined policy. Changes to pre-defined policies can only be made from derived policies.

Procedure

To customize signatures on the Connection Events tab:

1. In the Policy Editor window, select the Connection Events tab and continue as follows:

<table>
<thead>
<tr>
<th>If you want...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>to remove a signature associated with this policy</td>
<td>Select the row containing the signature in the Connection Events summary section and click Remove.</td>
</tr>
<tr>
<td>to change the priority of a signature</td>
<td>Click the Priority column next to the signature; then, select the correct priority.</td>
</tr>
<tr>
<td>the RealSecure system to respond when the selected event occurs</td>
<td>Click the Response column. The Responses window appears. Assign responses to the signature.</td>
</tr>
<tr>
<td>the RealSecure system to monitor the selected event only when coming from a particular source</td>
<td>Click the Src Address column. The Choose Address window appears. Specify the IP address of the source machine.</td>
</tr>
<tr>
<td>the RealSecure system to monitor the selected event only when going to a particular destination</td>
<td>Click the Dest Address column. The Choose Address window appears. Specify the IP address of the destination machine.</td>
</tr>
<tr>
<td>to assign a protocol for the selected signature</td>
<td>Click the Protocol column; then, select IP, TCP, UDP, or ICMP as the event protocol.</td>
</tr>
<tr>
<td>the RealSecure system to watch for activity from a particular port (or to edit ports information)</td>
<td>Click the Src Service/Type column. The Edit Service window appears. Select the service/type from the list. <strong>Note:</strong> You can edit service/types information from this window.</td>
</tr>
<tr>
<td>the RealSecure system to watch for activity going to a particular port (or to edit ports information)</td>
<td>Click the Dest Service/Code column. The Edit Service window appears. Select the service/code from the list. <strong>Note:</strong> You can edit service/code information from this window.</td>
</tr>
</tbody>
</table>

2. Repeat Step 1 for each signature that you are changing.
3. From the File menu, click Save.
   A confirmation message appears.
4. Click OK.
5. From the File menu, click Close.
6. Next, apply the policy to sensors.
Using Filters

Introduction
This topic describes the following:

- definition of filters
- when to use filters
- example of using filters
- how filters interact with signatures in a policy

Definition: filters
In the RealSecure system, filters allow the network sensor to ignore certain types of
network traffic. You can use filter network packets or network events.

Reference: For more information, see “Using Packet Filters” on page 25 and “Using Event Filters” on page 29.

When to use
Use filters to reduce the number of events that a sensor reports to the console, in the
database, and in reports. If you have hosts on your network that are secure and trusted or
hosts that you want the RealSecure system to ignore for any other reason, you can use
filters to your advantage.

Example
If you want the RealSecure system to ignore TCP connections to and from a trusted
computer, you create two filters: one for incoming TCP traffic and one for outgoing TCP
traffic. Creating these filters keeps the sensor from monitoring (and reporting) TCP
connections to and from this trusted host.

Filters and other signatures
When the RealSecure system detects traffic that matches a filter you have configured, it
ignores the traffic, even if the traffic contains a packet that matches another signature
enabled in the sensor’s policy.

Caution: Because filters cause the network sensor to ignore traffic, be sure you configure
the filter to only work on the hosts you trust or purposefully want to ignore. Creating a
filter to ignore TCP traffic to or from a broad range of IP addresses, for example, prevents
the sensor from detecting TCP-based intrusions to or from those hosts. Double-check the
configuration of new filters before applying the updated policy to a working sensor.
Using Packet Filters

Introduction

This topic describes the following:

- packet filters criteria
- packet filters field descriptions
- how to create a packet filter
- how to customize a packet filter
- how to remove a packet filter

Packet filters criteria

Packet filters determine which packets the intrusion detection system (IDS) processes. The sensor reads a packet from the network and determines if the packet matches a packet filter. If the packet matches a filter, then the IDS does not process the packet.

You can filter network packets based on the protocols described in Table 10:

<table>
<thead>
<tr>
<th>Packet Type</th>
<th>Filter Criteria</th>
</tr>
</thead>
</table>
| IP          | Source IP address or range of addresses  
|             | Destination IP address or range of addresses  |
| TCP or UDP  | Source IP address or range of addresses  
|             | Destination IP address or range of addresses  
|             | Source service and port  
|             | Destination service and port  |
| ICMP        | Source IP address or range of addresses  
|             | Destination IP address or range of addresses  
|             | Source ICMP type  
|             | Destination ICMP code  |

Table 10: Filter packet protocols

Field descriptions: Packet Filters

The following table describes the items on the Packet Filters tab:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Enables or disables the packet filter.</td>
</tr>
<tr>
<td>Filter</td>
<td>Specifies the filter name.</td>
</tr>
<tr>
<td>Src Address</td>
<td>Specifies the source IP address for the filter. The default source address for each filter is Any. Click this box to open the Enter Address Window, if you want to specify an address.</td>
</tr>
<tr>
<td>Dest Address</td>
<td>Specifies the destination IP address for the filter. The default destination for each filter is Any. Click this box to open the Enter Address Window, if you want to specify an address.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Click this box to select a protocol (ICMP, IP, TCP, or UDP).</td>
</tr>
<tr>
<td>Src Service/Type</td>
<td>Specifies the source service or type for the packet filter.</td>
</tr>
</tbody>
</table>

Table 11: Packet Filters tab field descriptions
Procedure: Adding a packet filter

To add a packet filter:

1. From the Managed Assets window, select a network sensor.
2. From the Sensor menu, select Policies.
   The Sensor Policies window appears.
3. Select the policy to which you want to add a packet filter.
   Note: If this policy does not exist, you must import it or derive it.
4. Click Customize.
   The Policy Editor window appears.
5. In the Packet Filters tab, click Add.
   The Enter a name window appears.
6. Type the name of this packet filter, and then click OK.
7. Configure the packet filter as follows:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a specific destination address or range of addresses</td>
<td>Click the Dest Address column for that filter, and then type the address information in the Choose Address window.</td>
</tr>
<tr>
<td>Configure a specific source address or range of addresses</td>
<td>Click the Src Address column for that filter; then, type the address information in the Choose Address window.</td>
</tr>
<tr>
<td>Change the protocol and service/type the filter monitors</td>
<td>Click the Protocol column for that filter and choose another protocol:</td>
</tr>
<tr>
<td></td>
<td>• IP. The Src Service/Type column and the Dest Service/Code column are not valid for this protocol.</td>
</tr>
<tr>
<td></td>
<td>• TCP or UDP. Click the Src Service/Type column to specify the source service and port for this protocol. Click the Dest Service/Code column to specify destination service and port for this protocol.</td>
</tr>
<tr>
<td></td>
<td>• ICMP. Click the Src Service/Type column to specify the ICMP packet type. Click the Dest Service/Code column to specify the ICMP packet code.</td>
</tr>
</tbody>
</table>

8. From the File menu, select Save.
   A confirmation message appears.
9. Click OK.
10. From the File menu, select Close.
### Procedure: Customizing a packet filter

To customize a packet filter:

1. In the Policy Editor window, select the Packet Filters tab.
2. Select the packet filter that you want to change.
   - Note: If the filter you want is not already in the policy, you must add it.
3. Click the **Src Address** column.
   - The Choose Address window appears.
4. Type the address and mask from which you want to filter packets.
5. Click the **Dest Address** column.
   - The Choose Address window appears.
6. Type the address and mask to which you want to filter packets.
7. In the **Protocol** column, select the protocol the event uses.
8. In the **Src Service/Type** column, select the source service or packet type that you want to filter.
9. If the Protocol is set to TCP or UDP, select the destination service port for which you want to filter packets in the Dest Service/Code column.
10. Repeat Steps 2 through 9 for each packet filter you want to change.
11. From the **File** menu, click **Save**.
   - A confirmation message appears.
12. Click **OK**.
13. From the **File** menu, click **Close**.
14. Apply the policy to the sensor(s) that you want to use the filter.

**Reference:** For more information about applying policies, look up “policies, applying” in the Help.

### Procedure: Removing a packet filter

To remove a packet filter:

1. From the Sensor Policies window, select the network sensor policy containing the filter you want to delete.
2. Click **Customize**.
   - The Policy Editor window appears.
3. Click the **Packet Filters** tab.
4. Select the row containing the packet filter you want to remove.
5. Click **Remove**.
   - A verification message appears.
6. Click **Yes**.
7. From the **File** menu, select **Save**.
   - A confirmation message appears.
8. Click **OK**.
9. From the **File** menu, select **Close**.
10. Apply the policy to the sensor(s).

**Reference:** For more information about applying policies, look up “policies, applying” in the Help.
Using Event Filters

Introduction

This topic describes the following:

- event filters criteria
- event filters field descriptions
- how to create an event filter
- how to customize an event filter
- how to remove an event filter

Event filters criteria

Event filters work after the IDS processes packets and detects an event. When the IDS generates an event, the sensor determines if the event matches an event filter. If the event matches a filter, then the sensor disregards the event.

You can use the following filter criteria:

- Source IP address or range of addresses
- Destination IP address or range of addresses
- Source service and port
- Destination service and port
- Event name

Field descriptions: Event Filters

The following table describes the items on the Event Filters tab:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Enables or disables the event filter.</td>
</tr>
<tr>
<td>Filter</td>
<td>Specifies the filter name.</td>
</tr>
<tr>
<td>SRC Address</td>
<td>Specifies the source IP address for the filter. The default source address for each filter is Any. Click this box to open the Enter Address Window, if you want to specify an address.</td>
</tr>
<tr>
<td>Src Service/Type</td>
<td>Specifies the source service or type for the event filter.</td>
</tr>
<tr>
<td>Dest Address</td>
<td>Specifies the destination IP address for the filter. The default destination for each filter is Any. Click this box to open the Enter Address Window, if you want to specify an address.</td>
</tr>
<tr>
<td>Dest Service/Code</td>
<td>Specifies the destination service or code for the event filter.</td>
</tr>
</tbody>
</table>
| Event Name          | Specifies the name of the event for which this filter will apply.  
                      **Note:** If you do not specify an event name, the filter applies to all events in the policy. |

Table 12: Event Filters tab field descriptions
Chapter 3: Configuring Signatures

**Procedure:**
**Creating an event filter**

To create an event filter:

1. Open the policy to which you want to add a filter.
   
   **Reference:** For information about how to open a policy, look up “policies, opening” in the Help.

2. Click the **Event Filters** tab.

3. Click **Add**.
   
   The **Enter a Name** window appears.

4. Type a name for the filter, and then click **OK**.
   
   The new filter is added to the bottom of the filters list.

5. Double-click **Filters** to open the list.

6. Select the filter.
   
   The properties of the filter appear in the right pane.

7. Select the type of protocol that the connection uses from the **Protocol** box.

8. Configure the source and destination information.
   
   **Reference:** For more information about configuring the source and destination information, see “Specifying IP Addresses for Connection Events and Filters” on page 32 and “Using Network Services” on page 33.

9. Click **Save**.

10. Apply the policy to the sensor(s) that you want to use the filter.

**Procedure:**
**Customizing an event filter**

To customize an event filter:

1. In the Policy Editor window, select the **Event Filters** tab.

2. Select the event filter that you want to change.
   
   **Note:** If the filter you want is not already in the policy, you must add it.

3. Click the **Src Address** column.
   
   The Choose Address window appears.

4. Select **Any** or type the specific address or range of addresses from which you want to filter events.

5. Click the **Dest Address** column.
   
   The Choose Address window appears.

6. Select **Any** or type the specific address or range of addresses for which you want to filter events.

7. In the **Protocol** column, select the protocol the event uses.

8. In the **Src Service/Type** column, select the source service or packet type that you want to filter.

9. If the Protocol is set to TCP or UDP, select the destination service port for which you want to filter events in the **Dest Service/Code** column.

10. In the **Event Name** column, select the event that you want to filter.

11. Repeat Steps 2 through 10 for each event filter you want to change.

12. From the **File** menu, click **Save**.
   
   A confirmation message appears.
13. Click **OK**.
14. From the **File** menu, click **Close**.
15. Apply the policy to the sensor(s) that you want to use the filter.

**Reference:** For more information about applying policies, look up “policies, applying” in the Help.

**Procedure:** Removing an event filter

If you want a network sensor policy to stop filtering certain types of network events, you can remove that event filter from the policy.

To remove an event filter:

1. From the Sensor Policies window, select the network sensor policy containing the filter you want to delete.
2. Click **Customize**.
   
   The Policy Editor window appears.
3. Click the **Event Filters** tab.
4. Select the row containing the event filter you want to remove.
5. Click **Remove**.
   
   A verification message appears.
6. Click **Yes**.
7. From the **File** menu, select **Save**.
   
   A confirmation message appears.
8. Click **OK**.
9. From the **File** menu, select **Close**.
10. Apply the policy to the sensor(s).

**Reference:** For more information about applying policies, look up “policies, applying” in the Help.
Specifying IP Addresses for Connection Events and Filters

Introduction

When you configure a connection event signature or create a filter, you can limit the scope by including or excluding a specific IP address or a range of IP addresses based on a network class.

Default settings

If you create a connection event or use one of the pre-defined connection event signatures, the signature monitors connections to or from any IP address (all addresses). Filters also use the Any address setting by default.

Procedure: Including a specific IP address

To include a specific IP address or a range of IP addresses:

1. Open the policy to which you want to add a connection event signature.
   Reference: For information about how to open a policy, look up “policies, opening” in the Help.

2. Click the Connection Events tab, the Event Filters tab, or the Packet Filters tab, depending on whether you are adding an address to a signature or to a filter.

3. Select the signature or filter you want to edit.
   The properties appear in the right pane.

4. Click the Source Address or the Destination Address column.
   The Choose Address window appears.

5. Choose the type of address you want to use.

<table>
<thead>
<tr>
<th>If you want to specify packets to or from...</th>
<th>Then...</th>
</tr>
</thead>
</table>
| one IP address                            | 1. Select IP Address.  
2. Type the IP address you want to specify in the Address box. |
| a range of IP addresses in a network class | 1. Select IP Address.  
2. Type an address in the Address box that is in the range you want to specify.  
3. Type a number in the Mask box to represent the level of network class.  
   Reference: For more information about using masks and other items in this window, click Help. |
| all IP addresses                          | • Select Any Address. |
| a network asset                           | • Select Network Asset, choose an asset from the list on the left.  
   Prerequisite: You must create an asset through View→Network Assets in the RealSecure console menu before you can select the asset in this window. See the RealSecure Help for more information. |

6. Click OK to save your changes.

7. Click Save to save your changes to the policy.

8. Apply the policy to the sensor(s) that you want to use the signature or filter.
   Reference: For more information about applying policies, look up “policies, applying” in the Help.
Using Network Services

Introduction
This topic describes the following:

- definition of network services
- purpose of using network services
- pre-defined network services
- creating a new network service
- editing a network service

Definition: network services
A network service associates a service name with a protocol (TCP, UDP, or ICMP) and one or more ports.

Purpose
When creating connection event signatures, use network services to have the signature monitor a specific service port. When the sensor detects an event that matches the signature, the service name appears in the alert on the console.

Pre-defined network services
The network sensor has several pre-defined network services, including the Any service (port = 0), which covers activity on all ports. You can customize these services or create new ones.

Procedure: Adding a network service
To add a network service:

1. Open the policy to which you want to add a connection event signature.
   Reference: For information about how to open a policy, look up “policies, opening” in the Help.
2. From either the Connection Events tab or the Packet Filters tab of the Policy Editor window, select the signature or filter you want to use the network service.
   The properties appear in the right pane.
3. Select Service (for TCP and UDP protocols) or ICMP Type (for the ICMP protocol) in the Source or Destination section.
   The Edit Service window appears.
4. Click Add.
   The Add Custom Service window appears.
5. From the Protocol list, select the protocol used by the new service.
6. In the Service box, type the name of this service.
7. In the Port # box, type the port used by this service.
8. Click OK to save the service, and OK again to return to the Policy Editor window.
9. From the File menu, select Save.
   A confirmation message appears.
10. Click OK.
11. Click Save.
12. Apply the policy to the sensor(s) that you want to use the signature or filter.
Chapter 3: Configuring Signatures

Reference: For more information about applying policies, look up “policies, applying” in the Help.

Procedure: Editing a network service

To edit a network service:

1. From the Sensor Policies window, select the policy containing the event or filter with the service you want to edit.

   Note: You cannot make any changes to the default policies delivered with the RealSecure product.

2. Click Customize.

   The Policy Editor window appears.

3. Click either the Connection Events tab or the Packet Filters tab, depending on what you want to edit.

4. Do the following:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change the source address</td>
<td>Click the Src Address column for that signature; then, type the address information in the Choose Address window.</td>
</tr>
<tr>
<td>Change the protocol the signature monitors</td>
<td>Click the Protocol column for that signature and choose another protocol. Which protocol did you choose? IP. For Packet Filters only, you can specify the source and destination addresses or address masks for which you want to filter packets. TCP or UDP. You can specify the source and destination ports for this protocol. Click those columns to edit the ports. ICMP. You can specify the type and code of the ICMP packet. Click those columns to edit them.</td>
</tr>
</tbody>
</table>

5. From the File menu, click Save.

   A confirmation message appears.

6. Click OK.

7. From the File menu, click Close.
Chapter 4

Creating User-Defined Signatures

Overview

Introduction

This chapter describes how to create and configure user-defined network sensor signatures.

In this chapter

The chapter contains the following topics:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating User-Defined Signatures</td>
<td>36</td>
</tr>
<tr>
<td>Regular Expressions in User-Defined Signatures</td>
<td>38</td>
</tr>
<tr>
<td>Using the Context Box in User-Defined Signatures</td>
<td>41</td>
</tr>
</tbody>
</table>
Creating User-Defined Signatures

Introduction

This topic describes the following:

- when to use user-defined signatures
- attributes of user-defined signatures that you can configure
- prerequisite to creating user-defined signatures with regular expressions
- how to create a user-defined signature

When to use

To monitor a type of event that the pre-defined signatures do not monitor, you can create a user-defined signature.

Attributes of user-defined signatures

When you create a user-defined signature, use the following fields in the policy editor to customize the attributes of the signature:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Enables and disables the signature.</td>
</tr>
<tr>
<td>Event</td>
<td>Changes the name of the user-defined event.</td>
</tr>
<tr>
<td>Priority</td>
<td>Defines the importance of each event. This information is used to sort</td>
</tr>
<tr>
<td></td>
<td>events into high, medium, and low priority and to generate reports.</td>
</tr>
<tr>
<td>Response</td>
<td>Configures the sensor to respond when it detects an event that matches the</td>
</tr>
<tr>
<td></td>
<td>signature. Each signature can have a combination of responses or no response.</td>
</tr>
<tr>
<td></td>
<td>Reference: For more information about responses, see the “Working with</td>
</tr>
<tr>
<td></td>
<td>Responses” chapter in the RealSecure Workgroup Manager User Guide.</td>
</tr>
<tr>
<td>Context</td>
<td>Specifies the type and part of a network packet for the sensor to scan.</td>
</tr>
<tr>
<td></td>
<td>Reference: See “Using the Context Box in User-Defined Signatures” on</td>
</tr>
<tr>
<td></td>
<td>page 41 for more information.</td>
</tr>
<tr>
<td>String</td>
<td>Specifies the text string in the packet (context) that determines whether an</td>
</tr>
<tr>
<td></td>
<td>event matches this signature. You can use wildcards and other expressions</td>
</tr>
<tr>
<td></td>
<td>in strings. See “Regular Expressions in User-Defined Signatures” on</td>
</tr>
<tr>
<td></td>
<td>page 38 for more information.</td>
</tr>
<tr>
<td>Add</td>
<td>Opens the Enter a Name window to add a user-defined event.</td>
</tr>
<tr>
<td>Remove</td>
<td>Removes a user-defined event.</td>
</tr>
</tbody>
</table>

Table 13: Field descriptions: User-Defined Events tab

Prerequisites

If the information that you want to use in the string box is not static text, you must use a regular expression. For more information about regular expressions, see “Regular Expressions in User-Defined Signatures,” on page 38.

Procedure

To create a user-defined event:

1. Open the policy to which you want to add a user-defined signature.

   Reference: For information about how to open a policy, look up “policies, opening” in the Help.
2. In the Policy Editor window, select the User-Defined Events tab.

3. Click Add.
   The Enter a Name window appears.

4. Type a name for the signature, and then click OK.
   The new signature is added to the bottom of the signatures list.
   **Note:** You can change the name later by double-clicking the current name and typing a new one.

   A list of user-defined signatures appear in the left pane.

6. Select the signature.
   The properties of the signature appear in the right pane.

7. Set the priority of this signature in the **Priority** box.

8. Select the type and part of the network packet that you want the sensor to scan from the **Context** box.
   **Reference:** For information about the various context options available in this box, see “Using the Context Box in User-Defined Signatures” on page 41.

9. Type the text or regular expression for the sensor to use to determine if an event is a match for this signature.
   **Reference:** For information about the regular expressions you can use in this box, see “Regular Expressions in User-Defined Signatures” on page 38.

10. Select the responses that you want the sensor to take when it detects an event that matches this signature.
    **Reference:** For information about each response, see the “Working with Responses” chapter in the RealSecure Workgroup Manager User Guide.

11. Click **Save**.

12. Apply the policy to the sensor(s) that you want to use the signature.
    **Reference:** For information about applying policies, look up “policies, applying” in the Help.
Regular Expressions in User-Defined Signatures

Introduction

This topic describes the following:

- definition of a regular expression
- when to use regular expressions
- the type of regular expression library the network sensor uses
- how to change the order of precedence in regular expressions
- reference books for regular expressions
- syntax you can use in regular expressions

Definition: regular expression

Regular expressions are a combination of static text and variables that the network sensor uses to detect patterns in network packets.

When to use

Use regular expressions in user-defined signatures if you need to detect more than a single, static text string.

Regular expression library

The network sensor uses a custom ISS regular expression library. Some of the regular expression syntax you can use with the network sensor is listed in Table 14.

Changing the order of precedence

Use parentheses in these regular expressions to offset the standard order of precedence.

Example: The natural order of precedence would interpret 4+2*4 as 12, because in the natural order of precedence, multiplication takes precedence over addition. However, you can use parentheses to change this precedence. For example, if you use (4+2)*4, the answer would be 24 instead of 12. This example describes a mathematical use of the order of precedence, but many other non-numerical uses exist.

Special considerations

Regular expressions that use alternative number systems, such as hexadecimal and octal number systems, may cause undesirable results. Consider the following rules when you use regular expressions:

- Do not use \x64 to indicate a match for the letter d. Use the letter d instead.
- Do not use \x73 to indicate a match for the letter s. Use the letter s instead.
- Do not use \x40 to indicate a match for the @ character. Use the @ character instead.

Reference

For more information about the order of precedence or other information about using regular expressions, see Mastering Regular Expressions: Powerful Techniques for Perl and Other Tools (O’Reilly Nutshell) by Jeffrey E. Friedl (Editor), Andy Oram (Editor).

Regular expression syntax

You can use the following syntax in the String box:

<table>
<thead>
<tr>
<th>This syntax...</th>
<th>Matches...</th>
</tr>
</thead>
<tbody>
<tr>
<td>(r)</td>
<td>r (where r is any arbitrary regular expression)</td>
</tr>
<tr>
<td>x</td>
<td>x (where x is any printable or escapable ASCII character)</td>
</tr>
</tbody>
</table>

Table 14: String standard expressions
Regular Expressions in User-Defined Signatures

<table>
<thead>
<tr>
<th>This syntax...</th>
<th>Matches...</th>
</tr>
</thead>
<tbody>
<tr>
<td>lr</td>
<td>l followed by r (where l and r are any arbitrary regular expressions)</td>
</tr>
<tr>
<td>\s</td>
<td>a space, or any character between tab and carriage return inclusive</td>
</tr>
<tr>
<td>\d</td>
<td>a decimal digit</td>
</tr>
<tr>
<td>&quot;</td>
<td>a double quote</td>
</tr>
<tr>
<td>'</td>
<td>a single quote</td>
</tr>
<tr>
<td>\</td>
<td>a backslash</td>
</tr>
<tr>
<td>\n</td>
<td>a newline (ASCII NL or LF)</td>
</tr>
<tr>
<td>\r</td>
<td>a carriage return (ASCII CR)</td>
</tr>
<tr>
<td>\t</td>
<td>a horizontal tab (ASCII HT)</td>
</tr>
<tr>
<td>\v</td>
<td>a vertical tab (ASCII VT)</td>
</tr>
<tr>
<td>\f</td>
<td>a formfeed (ASCII FF)</td>
</tr>
<tr>
<td>\b</td>
<td>a backspace (ASCII BS)</td>
</tr>
<tr>
<td>\a</td>
<td>a bell (ASCII BS)</td>
</tr>
<tr>
<td>\ooo</td>
<td>the specified octal character code (where o is a sequence of up to three octal digits: 0, 1, 2, 3, 4, 5, 6, or 7)</td>
</tr>
<tr>
<td>Example: \101 matches “a”</td>
<td></td>
</tr>
<tr>
<td>\xhh</td>
<td>the specified hexadecimal character code (where h is a sequence of two hex digits: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f, A, B, C, D, E, or F)</td>
</tr>
<tr>
<td>Example: \x61 matches “a”</td>
<td></td>
</tr>
<tr>
<td>.</td>
<td>any character except a newline character</td>
</tr>
<tr>
<td>@</td>
<td>nothing (represents an accepting position)</td>
</tr>
<tr>
<td>&quot;</td>
<td>nothing</td>
</tr>
<tr>
<td>[xy-z]</td>
<td>x, or anything between y and z inclusive (character class) (where x, y, and z are any printable or escaped ASCII characters)</td>
</tr>
<tr>
<td>[^xy-z]</td>
<td>anything that is not x, or between y and z inclusive</td>
</tr>
<tr>
<td>&quot;text&quot;</td>
<td>text literally without regard for meta-characters within (where text is any sequence of printable or escaped ASCII characters)</td>
</tr>
<tr>
<td>Note: The text is not treated as a unit. The syntax &quot;text&quot; is treated the same as &quot;t&quot; *e&quot; &quot;x&quot; &quot;t&quot;. Therefore, &quot;text&quot; matches &quot;tex&quot; followed by zero or more occurrences of &quot;t&quot;, not zero or more occurrences of &quot;text&quot;.</td>
<td></td>
</tr>
<tr>
<td>r?</td>
<td>r or nothing (optional operator)</td>
</tr>
<tr>
<td>r*</td>
<td>zero or more occurrences of r (Kleene closure)</td>
</tr>
</tbody>
</table>

Table 14: String standard expressions (Continued)
<table>
<thead>
<tr>
<th>This syntax...</th>
<th>Matches...</th>
</tr>
</thead>
<tbody>
<tr>
<td>r+</td>
<td>one of more occurrences of r (positive Kleene closure)</td>
</tr>
<tr>
<td>r(m)</td>
<td>r exactly m times (repeat operator) (where m is a positive integer)</td>
</tr>
<tr>
<td>r(m,n)</td>
<td>r at least m times, and at most n times (repeat operator) (where m and n are integers, m is not negative, and n is not smaller than m)</td>
</tr>
<tr>
<td>l</td>
<td>r</td>
</tr>
<tr>
<td>xr</td>
<td>x followed by r</td>
</tr>
<tr>
<td>^r</td>
<td>r only when it occurs at the beginning of a line</td>
</tr>
</tbody>
</table>

**Table 14:** String standard expressions (Continued)
Using the Context Box in User-Defined Signatures

Introduction
This topic describes the following:

- when to use the Context box
- Context box options
- where to find detailed descriptions of each context box option

When to use
When creating a user-defined signature, you must configure the sensor to scan a particular type and part of a network packet for information. Use the Context box to configure the sensor to scan the right part of the packet.

Context box options
You can choose one of the following options from the Context box:

- DNS_Query
- Email_Receiver
- Email_Sender
- Email_Subject
- File_Name
- News_Group
- Password
- SNMP_Community
- URL_Data
- URL_Post_Data
- URL_Raw_Data
- URL_Raw_Post_Data
- URL_User_Agent_Data
- User_Login_Name
- User_Probe_Name

Reference: These contexts are described in detail in Appendix A, “Context Descriptions for User-Defined Signatures,” on page 53.
Chapter 5

Troubleshooting

Overview

Introduction

This chapter contains policy file descriptions and troubleshooting information for the network sensor. Understanding how policy files work can help you troubleshoot policy file problems.

In this chapter

This chapter contains the following topics:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy File Descriptions</td>
<td>44</td>
</tr>
<tr>
<td>Isolating Policy Problems</td>
<td>46</td>
</tr>
</tbody>
</table>
Chapter 5: Troubleshooting

Policy File Descriptions

Introduction

This topic provides descriptions of policy files. Understanding how policy files work can help you troubleshoot policy file problems.

Policy file descriptions

The RealSecure network sensor uses the policy files described in Table 15. If current.policy is missing, the sensor loads default.policy. If default.policy is also missing, an error occurs and the sensor is not initialized.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>common.policy</td>
<td>The common.policy file contains the following information used by the daemon and the sensors:</td>
</tr>
<tr>
<td></td>
<td>• available cryptographic providers (sensors only)</td>
</tr>
<tr>
<td></td>
<td>• destination and community for any SNMP traps</td>
</tr>
<tr>
<td></td>
<td>• flags for automatic SNMP trap generation (on sensor start, on sensor policy change, etc.)</td>
</tr>
<tr>
<td></td>
<td>• response definitions</td>
</tr>
<tr>
<td>current.policy</td>
<td>When the sensor loads, it tries to load the current.policy file first. When the sensor is finished initializing, it rewrites its configuration back to current.policy. If the sensor is running, you can assume that current.policy contains the currently active policy.</td>
</tr>
<tr>
<td>Default.policy</td>
<td>The default policy file of the sensor. This file is loaded only if current.policy is missing. You can revert the sensor to a default configuration by deleting current.policy.</td>
</tr>
<tr>
<td>issCSF.policy</td>
<td>The main policy file for the Common Sensor Framework (CSF). CSF reads this policy to learn what sensor and response plug-ins it must load to become a fully functional sensor.</td>
</tr>
<tr>
<td>issDaemon.policy</td>
<td>The issdaemon.policy file contains daemon-specific information, such as:</td>
</tr>
<tr>
<td></td>
<td>• sensor initialization timeout: how long the daemon tries to connect to a sensor before it times out</td>
</tr>
<tr>
<td></td>
<td>• daemon port: the port number used by the daemon for sensor communication (normally 2998)</td>
</tr>
<tr>
<td></td>
<td>• master console: the console that has the master status of the sensor controlled by the daemon.</td>
</tr>
<tr>
<td></td>
<td>• information about applied updates</td>
</tr>
<tr>
<td></td>
<td>• location of sensor binaries</td>
</tr>
<tr>
<td>crypt.policy</td>
<td>The crypt.policy file contains information about the cryptographic providers chosen during the component install. This file lists the cryptographic providers in order of precedence. It also contains the auto import flag, if chosen during the install, which allows the component to auto import the console’s public key during the first connection only.</td>
</tr>
</tbody>
</table>

Table 15: Policy file descriptions
<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>update.policy</td>
<td>As new versions of the sensor ship with new signatures, the configuration for the new signatures are distributed in this file. The sensor loads current.policy, checks the version information of any update.policy files, and then loads them if the version matches the sensor's version. The resulting configuration is written to current.policy so that this file still represents what the sensor is currently running.</td>
</tr>
</tbody>
</table>

Table 15: Policy file descriptions (Continued)
Isolating Policy Problems

Introduction

This topic provides information about isolating and correcting possible policy problems.

Error messages indicating policy problems

Error messages that might indicate policy file problems appear in the Managed Assets window. These messages include the following:

- “No such file or directory” displays in the Control Status column when connecting to a sensor
- “Failure to transfer current policy when the control channel opened” displays in the Control Status column
- “Failure to read/transfer common.policy” displays in the Control Status column
- “Unknown” displays in the Policy column

Troubleshooting techniques

When error messages indicating possible policy file problems appear in the console, you can try the following techniques to isolate and correct the problem:

- Inspect the issDaemon directory and sensor component directory. Look for things such as file sizes of zero bytes, or no policy files listed.
- Check the event log (Windows) or the syslog (Unix) of the sensor for any unusual events.
- Reapply a policy to the sensor. For more information about applying policies to sensors, see the “Working with Policies” chapter of the RealSecure Workgroup Manager User Guide.
- Revert the sensor to a default policy configuration by deleting the current.policy file, and then applying a new policy to the sensor. See “Deleting current.policy” on page 48.
- Determine whether the problem may be the daemon. Start the daemon without automatically restarting the sensor, to determine if the daemon loads correctly. See “Determine whether the problem may be the daemon” on page 49.
- Start the sensor manually to detect sensor component problems. See “Starting the sensor manually to detect sensor component problems” on page 50.
- If the problem persists, contact ISS Technical Support. For technical support contact information, see “Getting Technical Support” on page viii.

Important: To maintain the sensor’s intended configuration, remember to change the newly applied policy to match the previous configuration after troubleshooting.

Stopping the issDaemon

Some troubleshooting techniques for policy problems require stopping the issDaemon. You can do this from the desktop (Windows only) or from the command line.
To stop the issDaemon, use the following decision table to determine your next action:

<table>
<thead>
<tr>
<th>For this operating system...</th>
<th>To use this method...</th>
<th>Do this...</th>
</tr>
</thead>
</table>
| **Windows 2000**             | Desktop               | To stop the issDaemon from the desktop:  
1. Select Start→Settings→Control Panel.  
The Control Panel appears.  
2. Double-click Administrative Tools.  
The Administrative Tools window appears.  
The Services window appears.  
4. Double-click issDaemon.  
The issDaemon Properties window appears.  
5. In the Service Status area, click *Stop*.  
The issDaemon stops. |

| **Windows 2000**             | Command line          | To stop the issDaemon from the command line, type:  
`C:\>net stop issdaemon`  
The issDaemon stops.  
**Note:** This procedure assumes that the product is installed on the default directory and is the first or only network sensor installed on the machine. |

| **Solaris**                  | Command line          | Log in as root.  
From the command line, type:  
`/etc/ini.d/realsecure stop`  
The issDaemon stops. |

---

**Starting the issDaemon**

Some troubleshooting techniques for policy problems require starting the issDaemon. You can do this from the desktop (Windows only) or from the command line. To start the issDaemon, use the following decision table to determine your next action:

<table>
<thead>
<tr>
<th>For this operating system...</th>
<th>To use this method...</th>
<th>Do this...</th>
</tr>
</thead>
</table>
| **Windows 2000**             | Desktop               | To start the issDaemon from the desktop:  
1. Select Start→Settings→Control Panel.  
The Control Panel appears.  
2. Double-click Administrative Tools.  
The Administrative Tools window appears.  
3. The Administrative Tools window appears.  
The Services window appears.  
5. Double-click issDaemon.  
The issDaemon(Properties) window appears.  
6. In the Service Status area, click *Start*.  
7. Click OK.  
The issDaemon starts. |
You can revert the sensor to a default policy configuration by deleting the current.policy file, and then applying a new policy to the sensor. This requires stopping the issDaemon, deleting the current.policy file, and then restarting the issDaemon. The sensor should restart automatically when the daemon is started. Upon restarting, the sensor uses default.policy until it receives a new policy file from the console.

**Important:** Do not delete current.policy while the sensor is running.

To delete current.policy:

1. In the Managed Assets window, select the sensor.
2. Select **Sensor**→**Stop Managing Sensor**.
   
   A confirmation message appears.
3. Click **Yes** to confirm.
4. Stop the issDaemon.

   **Reference:** For the procedure on stopping the issDaemon, see “Stopping the issDaemon” on page 46.
5. Locate the issDaemon.policy file. The issDaemon.policy file is located in the directory where the sensor was installed.
6. Locate and then delete current.policy. The current.policy file is located in the directory where the sensor was installed.

7. Restart the issDaemon.

   **Reference:** For the procedure on starting the issDaemon, see “Stopping the issDaemon” on page 46.
8. Using Windows Explorer, locate the transfer directory at the following location:

    C:\Program Files\ISS\RealSecure 6.5 Console\Transfer

9. Delete the files that contain the sensor’s IP address in the filename.
10. Did the sensor restart automatically?

    If **yes**, go to Step 11.

    If **no**, see “Determine whether the problem may be the daemon” on page 49.
11. In the Managed Assets window, select **Asset**→**Manage**.
12. Select the sensor, and then click **OK**.

13. Apply a default, customized or imported policy to the sensor.

   **Reference:** For more information about applying policies to sensors, see the Working with Policies chapter of the *RealSecure Workgroup Manager User Guide*.

### Determine whether the problem may be the daemon

You can determine whether the problem could be caused by the daemon. By default, the sensor will start automatically when the daemon is started. You can prevent the sensor from starting automatically by stopping the daemon, editing the `issDaemon.policy` file, and then restarting the daemon. If the daemon fails to load, then the problem may be caused by the daemon or one of its policy files. ISS recommends troubleshooting daemon problems with the help of Technical Support.

To determine if the problem may be caused by the daemon:

1. Stop the issDaemon.

   **Reference:** For the procedure on stopping the issDaemon, see “Stopping the issDaemon” on page 46.

2. Locate the `issDaemon.policy` file. The Windows default location for this file is:

   C:\Program Files\ISS\IssDaemon

   The Solaris default location for this file is:

   /opt/ISS/issDaemon

3. Open the `issDaemon.policy` file in a text editor such as Notepad.

4. Change the `auto_recovery` value for the selected sensor from 1 to 0.

   Setting the `auto_recovery` value to 0 causes the daemon to start without automatically starting the sensor.

5. Save and close the `issDaemon.policy` file, and then close the text editor.

6. Restart the issDaemon.

   **Reference:** For the procedure on starting the issDaemon, see “Starting the issDaemon” on page 47.

7. Check the running processes to determine whether the daemon loaded correctly. If the daemon does not load correctly, then the policy problem may be caused by the daemon.

To check the running processes, use the following decision table to determine your next action:

<table>
<thead>
<tr>
<th>For this operating system...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2000</td>
<td>1. Press CNTRL+ALT+DELETE. The Windows Security window appears. 2. Click <strong>Task Manager</strong>. The Windows Task Manager window appears. 3. Select the Processes tab, and ensure that the <code>issDaemon.exe</code> process is running.</td>
</tr>
</tbody>
</table>
| Unix                        | **At the command line, type:**  
   `han[admin]# ps -ax | grep iss` |
Chapter 5: Troubleshooting

### 8. Did the issDaemon load correctly?
- If *yes*, then you must start the sensor manually and determine if there are any sensor component problems. See “Starting the sensor manually to detect sensor component problems” on page 50.
- If *no*, then contact ISS Technical Support for further assistance. See “Getting Technical Support” on page xiv for contact information.

### 9. Stop the issDaemon.
*Reference:* For the procedure on stopping the issDaemon, see “Stopping the issDaemon” on page 46.

### 10. Locate the issDaemon.policy file. The default location for this file is:
- `C:\Program Files\ISS\IssDaemon`

### 11. Open the issDaemon.policy file in a text editor such as Notepad.

### 12. Change the auto_recovery value for the selected sensor to 1.

### 13. Save and close the issDaemon.policy file, and then close the text editor.

### 14. Restart the issDaemon.
*Reference:* For the procedure on starting the issDaemon, see “Starting the issDaemon” on page 47.

### 15. Did the sensor start automatically after starting the daemon?
- If *yes*, determine whether the policy problem has been corrected. If the problem persists, see “If you need further help” on page 51.
- If *no*, then you must start the sensor manually to determine if the policy problem has been corrected. See “Starting the sensor manually to detect sensor component problems” on page 50.

---

**Starting the sensor manually to detect sensor component problems**

The sensor may not start automatically when the daemon is started. This could happen if the sensor was in a stopped state before the daemon was stopped. You can start the sensor manually from the desktop (Windows only) or from the command line.

**Important:** Be sure that the issDaemon is stopped before starting the sensor manually. If you try to start the sensor manually without first shutting down the daemon, the following error message displays:

*Error creating FirstInstance Mutex*
To start the sensor manually and determine whether sensor component problems may exist:

1. Start the sensor, using the following decision table to determine your next action:

<table>
<thead>
<tr>
<th>To start the sensor from...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows command line</td>
<td>At the command line, type: issCSF “C:\Program Files\ISS\issSensors\network_sensor_1” network_sensor_1 NetworkEngine RealSecure NetworkEngine</td>
</tr>
<tr>
<td>Solaris</td>
<td>At the command line, type: ./issCSF -d /opt/ISS/issSensors/ network_sensor_1/ -c /opt/ISS/issDaemon/ crypt.policy -n network_sensor_1 -e NetworkEngine -h NetworkEngine -g RealSecure</td>
</tr>
</tbody>
</table>

2. Did the sensor start correctly?
   - If *yes*, then you must set the auto-recovery flag back to its original value. Go to Step 3.
   - If *no*, then contact ISS Technical Support for further assistance. See “Getting Technical Support” on page xiv for contact information.

3. Stop the issDaemon.
   
   **Reference:** For the procedure on stopping the issDaemon, see “Stopping the issDaemon” on page 46.

4. Locate the issDaemon.policy file. The Windows default location for this file is:
   
   C:\Program Files\ISS\IssDaemon
   
   The Solaris default location for this file is:
   
   /opt/ISS/issDaemon

5. Open the issDaemon.policy file in a text editor such as Notepad.

6. Set the auto_recovery value for the selected sensor to 1.

7. Save and close the issDaemon.policy file, and then close the text editor.

8. Restart the issDaemon.

   The sensor starts automatically.

   **Reference:** For the procedure on starting the issDaemon, see “Starting the issDaemon” on page 47.

If you need further help

If you still cannot isolate the problem, send copies of the sensor’s current.policy and common.policy files to ISS Technical Support for further assistance. See “Getting Technical Support” on page xiv for contact information. Include the output from the following commands:

```
tail var/adm/messages
netstat -a
ps -ef
```
Appendix A

Context Descriptions for User-Defined Signatures

Overview

Introduction

This appendix describes each Context in detail.

In this appendix

This appendix contains the following topics:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS_Query Context</td>
<td>55</td>
</tr>
<tr>
<td>Email_Receiver Context</td>
<td>56</td>
</tr>
<tr>
<td>Email_Sender Context</td>
<td>57</td>
</tr>
<tr>
<td>Email_Subject Context</td>
<td>58</td>
</tr>
<tr>
<td>File_Name Context</td>
<td>59</td>
</tr>
<tr>
<td>News_Group Context</td>
<td>60</td>
</tr>
<tr>
<td>Password Context</td>
<td>61</td>
</tr>
<tr>
<td>SNMP_Community Context</td>
<td>62</td>
</tr>
<tr>
<td>URL_Data Context</td>
<td>63</td>
</tr>
<tr>
<td>URL_Post_Data Context</td>
<td>64</td>
</tr>
<tr>
<td>URL_Raw_Data Context</td>
<td>65</td>
</tr>
<tr>
<td>URL_Raw_Post_Data Context</td>
<td>66</td>
</tr>
<tr>
<td>URL_User_Agent_Data Context</td>
<td>67</td>
</tr>
<tr>
<td>User_Login_Name Context</td>
<td>68</td>
</tr>
<tr>
<td>User_Probe_Name Context</td>
<td>69</td>
</tr>
</tbody>
</table>

Definition: contexts

Context is a parameter setting for network sensor user-defined signatures. The sensor uses the context setting to identify the type and particular part of a network packet to monitor.
**Example:** The email_subject context configures the sensor to monitor the subject line of email packets (messages).

**Reference:** For procedural information about using contexts, see “Creating User-Defined Signatures” on page 36.
DNS_Query Context

Introduction
This topic describes the DNS_Query context.

When to use this context
Most programs use domain names to access resources on the Internet. These programs search for the DNS name on a server to determine the specific IP of an Internet resource. Use the DNS_Query context to monitor access to particular sites or classes of sites without knowing specific IP addresses.

What it monitors
The DNS_Query context monitors the DNS name in DNS query and DNS reply packets over UDP and TCP. The sensor compares the information in the String box to the expanded (human-readable) version of the domain name in these packets.

Examples
For example, you could use the DNS_Query context along with a string value of www.microsoft.com to monitor users accessing the Microsoft Web site.

If you are concerned about users on your site accessing hacker-related materials on the Internet, you could monitor access to domains such as the following:

- hackernews.com
- rootshell.com

You could use this to generically monitor access to pornography from work or monitor other sites depending on corporate usage policies.

What it does not monitor
If a user accesses a site directly using an IP address, the DNS lookup does not occur and the sensor cannot, therefore, detect the event.

If you are trying to monitor for particular URLs, keep in mind that a domain name is only the first element in a URL. Use the URL_Data context (see “URL_Data Context” on page 63) to detect the rest of the URL.

Definition—first element in a URL: The first element in a URL is between the ":" and the first single slash. For example, //www.cnn.com is the first element in http://www.cnn.com/stories.
Email_Receiver Context

Introduction
This topic describes the Email_Receiver context.

When to use this context
Use the Email_Receiver context to monitor incoming or outgoing email to a particular recipient.

What it monitors
The Email_Receiver context monitors the receiver address part of the email header using the SMTP, POP, IMAP protocols. When the sensor detects an event that matches a signature using the Email_Receiver context, you can determine which protocol the email used by examining the details of the event.

Reference: For a procedure on examining event details, look up “events, inspecting” in the index of the RealSecure Help.

Examples
If, for instance, you suspect that “social engineering” manipulations of particular employees are being attempted, you might want to monitor for inbound email to those employees addresses, and log the IPs from which they come. Likewise, if you suspect some sort of proprietary information leak within your company to a particular outside email address, you could track email to that address using this context.

What it does not monitor
This context does not monitor email sent with the MAPI protocol.
## Email_Sender Context

<table>
<thead>
<tr>
<th><strong>Introduction</strong></th>
<th>This topic describes the Email_Sender context.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>When to use this context</strong></td>
<td>Use the Email_Sender context to monitor incoming or outgoing email from a particular recipient.</td>
</tr>
<tr>
<td><strong>What it monitors</strong></td>
<td>The Email_Sender context monitors the sender address part of the email header using the SMTP, POP, IMAP protocols. When the sensor detects an event that matches a signature using the Email_Sender context, you can determine which protocol the email used by examining the details of the event.</td>
</tr>
<tr>
<td><strong>Reference:</strong></td>
<td>For a procedure on examining event details, look up “events, inspecting” in the index of the RealSecure Help.</td>
</tr>
<tr>
<td><strong>Examples</strong></td>
<td>Like the Email_Recipient context, one of the best examples of using the Email_Sender context is to detect instances of social engineering or other employee manipulation (inbound) or to detect information leaks from your company (outbound).</td>
</tr>
<tr>
<td><strong>What it does not monitor</strong></td>
<td>This context does not monitor email sent with the MAPI protocol.</td>
</tr>
</tbody>
</table>
Email_Subject Context

Introduction
This topic describes the Email_Subject context.

When to use this context
Use the Email_Subject context to monitor the subject line of email.

What it monitors
The Email_Subject context monitors the subject line in the email header of messages using the SMTP, POP, and IMAP protocols.

Examples
Like the other email contexts, this context is best suited to monitoring information leaks. For example, you could create signatures to detect the use of important project names or file names. (Email_content is also very useful in this manner.)

You can also use Email_Subject to detect viruses, such as the ILOVEYOU virus. However, because viruses and other attacks have developed programs that systematically change the subject line, the Email_Content context is more reliable to use.

What it does not monitor
This context does not monitor email sent with the MAPI protocol.
# File_Name Context

## Introduction
This topic describes the File_Name context.

## When to use this context
Use the File_Name context to monitor access over the network to sensitive files in your organization.

## What it monitors
The File_Name context detects when someone (or a program) attempts to remotely read a file or write to a file with any of the following protocols:

- TFTP
- FTP
- Windows file sharing (CIFS or Samba)
- NFS

## Example
The infamous Explorer worm of 1999 is a good example. When this worm propagates over a Windows network, it attempts to write to certain files on remote Windows shares. You can monitor for attempts to access these files and stop the worm from propagating locally. In this case, monitor the `WIN.INI` and `ZIPPED_FILES.ZIP` file names.

## What it does not monitor
NFS can open files in many ways, some of which do not directly reference the name of the file. Therefore, using this context to monitor NFS access to a file is not 100% effective.
Appendix A: Context Descriptions for User-Defined Signatures

**News_Group Context**

**Introduction**  
This topic describes the News_Group context.

**When to use this context**  
Use the News_Group context to monitor the names of news groups that people at your company use.

**What it monitors**  
The News_Group context monitors people accessing news groups using the NNTP protocol.

**Example**  
You can use the context to detect subscriptions to news groups, such as hacker or pornography groups, that are inappropriate according to your company's Internet usage policy.
Password Context

Introduction
This topic describes the Password context.

When to use this context
Use the Password context to identify passwords that are passed in clear text over the network. When a password is not encrypted, an attacker can easily steal this password by monitoring traffic with a sniffer program from another site. Therefore, you should consider any passwords sent in clear text as compromised.

What it monitors
The Password context monitors programs or users sending passwords in clear text using the FTP, POP, IMAP, NNTP or HTTP protocols.

Examples
Other than monitoring clear text passwords to keep attackers from stealing passwords, you can use the Password context in other ways:

- monitoring compromised accounts to gain forensic data
- monitoring the accounts of employees that have been terminated
- detecting the use of default passwords

Example—Monitoring compromised accounts
For example, you can use this context to detect attempts to use accounts that you know have been compromised in the past. After cancelling a compromised account, you can create a signature to monitor attempt to use it. The information gained from monitoring this activity may lead you to the person that accessed the compromised data.

Example—Monitoring terminated employee accounts
Likewise, when employees are terminated, add searches for their passwords (if known) to detect unauthorized remote access attempts to their now-closed accounts.

Example—Detecting the use of default passwords
Finally, a very common security vulnerability is the use of some pre-defined password on an account name for software or systems installed “out of the box.” The X-Force database contains many records detailing the names of such accounts. By setting up signatures to look for default passwords that are relevant to your site, you could detect attempts by attackers to probe for common vulnerabilities.

Reference: For more information about default passwords, look up passwords in the X-Force database at http://xforce.iss.net.

Using these signatures with Internet Scanner
If you scan this network with Internet Scanner, a signature using this context to check for default passwords may detect many instances of this event in response to a password scan.

What it does not monitor
This context does not monitor encrypted passwords.
## SNMP_Community Context

<table>
<thead>
<tr>
<th>Introduction</th>
<th>This topic describes the SNMP_Community context.</th>
</tr>
</thead>
<tbody>
<tr>
<td>When to use this context</td>
<td>Use the SNMP_Community context to monitor the use and possible abuse of SNMP community strings.</td>
</tr>
<tr>
<td>What it monitors</td>
<td>The SNMP_Community context monitors any packet containing an SNMP community string.</td>
</tr>
<tr>
<td>Definition—SNMP community strings</td>
<td>An SNMP community string is a clear text password in an SNMP message. This password authenticates each message. If the password is not a valid community name, then the message is rejected.</td>
</tr>
<tr>
<td>Security implications</td>
<td>If an unauthorized person gains knowledge of your community strings, that person could use that information to retrieve valuable configuration data from your equipment or even reconfigure your equipment.</td>
</tr>
<tr>
<td>Security recommendations</td>
<td>ISS strongly recommends that you use highly unique community strings and that you reconfigure them periodically.</td>
</tr>
<tr>
<td>Examples</td>
<td>The following paragraphs describe two ways to use this context:</td>
</tr>
<tr>
<td></td>
<td>• detecting people trying to use old community name strings</td>
</tr>
<tr>
<td></td>
<td>• detecting the use of default community strings</td>
</tr>
<tr>
<td>Example—Detecting people trying to use old strings</td>
<td>If you change the SNMP community strings, create a signature using this context to have the RealSecure sensor search people trying to use the old strings.</td>
</tr>
<tr>
<td>Example—Detecting the use of default strings</td>
<td>The X-Force database contains information about several vulnerabilities that involve default community strings on common equipment. Attackers can attempt to gain access to your equipment by using these default passwords. To have RealSecure detect this kind of activity, you can create signatures using this context to monitor for the default passwords that are relevant to the equipment at your site. These signatures could detect attackers attempting to probe for these common vulnerabilities.</td>
</tr>
<tr>
<td>Reference</td>
<td>For more information about default passwords, look up SNMP in the X-Force database at <a href="http://xforce.iss.net">http://xforce.iss.net</a>.</td>
</tr>
<tr>
<td>Using these signatures with Internet Scanner</td>
<td>If you scan this network with Internet Scanner, a signature using this context to check for SNMP community strings may detect many instances of this event in response to a SNMP scan.</td>
</tr>
</tbody>
</table>
URL_Data Context

Introduction
This topic describes the URL_Data context.

When to use this context
Use the URL_Data context to monitor various security issues or policy issues related to HTTP GET requests.

Definition—HTTP GET request: An HTTP GET request occurs when a client, such as a Web browser, requests a file from a Web server. For example, when a user types a URL into a browser, the browser sends an HTTP GET request for that page. The HTTP GET request is the most common way to retrieve files on a Web server.

What it monitors
The URL_Data context monitors the contents of a URL (minus the domain name or address itself) for particular strings, when accessed through an HTTP GET request.

Examples
You can use this context to have the sensor monitor for attacks involving vulnerable CGI scripts or other sorts of attacks against Web servers. For example, ISS Advisory #32, released on August 9, 1999, describes how to use this context to search for an attempt to exploit a vulnerability in a Microsoft Internet Information Server component.

Reference: For more information, see Vulnerabilities in Microsoft Remote Data Service at http://xforce.iss.net/alerts/advise32.php.

You could also use this context to generically search for certain types of computer misuse in an organization, such as attempts to access some pornography.

What it does not monitor
This context does not monitor the domain name associated with an HTTP GET request.

Reference: For information about monitoring access based on the domain, see “DNS_Query Context” on page 55.
Appendix A: Context Descriptions for User-Defined Signatures

URL_Post_Data Context

Introduction
This topic describes the URL_Post_Data context.

When to use this context
Use the URL_Post_Data context to monitor various security issues or policy issues related to HTTP Post requests.

Definition—HTTP Post request: An HTTP POST request occurs when a client, such as a Web browser, sends a file to a Web server.

What it monitors
The URL_Post_Data context monitors the contents of a formatted URL, when accessed through an HTTP Post request.
# URL_Raw_Data Context

**Introduction**
This topic describes the URL_Raw_Data context.

**When to use this context**
Use the URL_Raw_Data context to monitor various security issues or policy issues related to HTTP GET requests.

**Definition—HTTP GET request:** An HTTP GET request occurs when a client, such as a Web browser, requests a file from a Web server. For example, when a user types a URL into a browser, the browser sends an HTTP GET request for that page. The HTTP GET request is the most common way to retrieve files on a Web server.

**What it monitors**
The URL_Raw_Data context monitors the contents of an unformatted URL for particular strings, when accessed through an HTTP GET request.
## URL_Raw_Post_Data Context

**Introduction**
This topic describes the URL_Raw_Post_Data context.

**When to use this context**
Use the URL_Raw_Post_Data context to monitor various security issues or policy issues related to HTTP POST requests.

**What it monitors**
The URL_Raw_Post_Data context monitors the contents of an unformatted URL for particular strings, when accessed through an HTTP POST request.
URL_User_Agent_Data Context

Introduction
This topic describes the URL_User_Agent_Data context.

When to use this context
Use the URL_User_Agent_Data context to monitor various security issues or policy issues related to Web browser version information.

What it monitors
The URL_User_Agent_Data context monitors the contents of a URL for particular strings, when accessed through a Web browser.
Appendix A: Context Descriptions for User-Defined Signatures

User_Login_Name Context

Introduction
This topic describes the User_Login_Name context.

When to use this context
Use the User_Login_Name context to detect user names that are exposed in plain text during authentication requests. This context works for many protocols, so you can use it to track attempts to use a particular account regardless of which protocol the attacker uses.

What it monitors
The User_Login_Name context monitors for plain text user names in authentication requests using the FTP, POP, IMAP, NNTP, HTTP, Windows, or R* protocols.

Examples
You can use this context to track attempts to use compromised accounts or attempts by recently dismissed employees to access their old accounts online.

For example, if you know the account named "FredJ" was compromised in an attack, configure a signature using this context to search for attempts to access the account. This signature could catch attempts by an attacker to return to a compromised computer.
**User_Probe_Name Context**

<table>
<thead>
<tr>
<th><strong>Introduction</strong></th>
<th>This topic describes the User_Probe_Name context.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>When to use this context</strong></td>
<td>Use the User_Probe_Name context to identify attempts to gain access to computers on your network using default program passwords.</td>
</tr>
<tr>
<td><strong>What it monitors</strong></td>
<td>The User_Probe_Name context monitors any user name associated with FINGER, SMTP, VRFY, and SMTP EXPN.</td>
</tr>
<tr>
<td><strong>Security implications</strong></td>
<td>An attacker can use these default accounts to gain access to your servers or other computers in the future.</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Like the Password and SNMP_Community contexts, you can use the X-Force database to build a list of default accounts and passwords relevant to the systems and software on your network.</td>
</tr>
</tbody>
</table>

**Reference:** For more information about default passwords, look up SNMP in the X-Force database at [http://xforce.iss.net](http://xforce.iss.net).
Index

a
adding a packet filter 26
Advanced button
  customizing signature attributes 13
advanced policy properties
  customizing 19
Advanced Properties window
  field descriptions 17
Attack Detector policy 9
Attacks and Audits (Maximum Coverage) policy 9

C
CLI 2
  definition 2
CLI (Command Line Interface) 2
collision domain 3
Command Line Interface 2
command line interface (CLI)
  applying changes to sensors 6
common.policy 44
configuring a signature
  groups of 12
  prerequisites for 12
connection events
  definition of 20
  group description in policy editor 12
  how to configure for your policy 21
  types of 20
Connection Events tab
  field descriptions 20
Context box
  options 41
  role of 41
  use in configuring the sensor 41
contexts
  about 53
  DNS_Query 55
  Email_Receiver 56
  Email_Sender 57
  Email_Subject 58
  File_Name 59
  News_Group 60

Password 61
SNMP_Community 62
URL_Data 63–67
URL_Post_Data 64
URL_Raw_Data 65
URL_Raw_Post_Data 66
URL_User_Agent_Data 67
User_Login_Name 68
User_Probe_Name 69
controlling frequency of responses 16
conventions, typographical
  in commands vii
  in procedures vii
  in this manual vii
creating a user-defined event 36
creating custom signatures 6
current.policy 44
customizing advanced properties of policies 19

d
Default.policy 44
detecting an intrusion 5
DMZ Engine (DMZ Engine X.X) policy 9
DNS_Query context 55

e
editing policy files 10
editing protocol ports 15
Email_Receiver context 56
Email_Sender context 57
Email_Subject context 58
Engine Inside Firewall policy 9
Event Filtering section
  advanced property for signature customization 16
  controlling responses 16
  event filters 12
  Event Filters tab
    field descriptions 29
    event propagation
      advanced property for signature customization 16
      definition of 5
  Explorer worm example 59
Index

f
File_Name context 59
filters 6, 24
creating 30
Event Filters tab 12
including an IP address 32
FINGER, monitoring user name associated with 69
Flood Protection check box 16
For Windows Networks policy 9
frequency of responses, controlling 16

g
gigabit adapter 3
gigabit network sensor 3

h
high-performance gigabit packet driver 3
HTTP GET request 63, 65
HTTP POST request 64, 66

i
ignoring network traffic 6
ILOVEYOU virus example 58
Internet Security Systems
technical support viii
Web site viii
intrusion
responding to 5
IP addresses
masks 32
specifying 32
issCSF.policy 44
issDaemon.policy 44

l
LOGDB
controlling frequency of responses 16

m
masks 32
monitoring network connections 6

n
network connections
monitoring 6
network segment 3
network sensor
network segments 3
policies 5
regular expression library 38
using filters to ignore traffic 6
network service
pre-defined 33
News_Group context 60

o
Optional Parameters list 16
order of precedence
changing in regular expressions 38

p
Packet Filters 12
packet filters 25
adding 26
Packet Filters tab
field descriptions 25
Password context 61
policy
adding a connection event signature 32
common.policy 44
current.policy 44
customizing 5
Default.policy 44
definition of 8
editing with text editor 10
isolating problems 46
issCSF.policy 44
issDaemon.policy 44
location of 10
pre-defined 8
troubleshooting policy files 43
update.policy 45
viewing, creating, and editing 8
policy editor tabs
Connection Events 12
Event Filters 12
Packet Filters 12, 25
Security Event 12
User-Defined Events 12
policy files
Index

descriptions 44
Pre-defined network service 33
pre-defined policies 8
pre-defined policy 8
Attack Detector 9
Attacks And Audits (Maximum Coverage) 9
DMZ Engine (DMZ Engine X.X) 9
Engine Inside Firewall 9
For Windows Networks 9
Protocol Analyzer X.X 9
Session Recorder X.X 10
Web Watcher X.X 10
pre-defined signature
configuring 14
definition of 13
Priority column 20
Priority field
customizing signature attributes 13
Protocol Analyzer X.X policy 9
protocol ports 15
ing 15
role of 15
Protocol Ports button
customizing signature attributes 14

r
regular expressions
in user-defined signatures 38
special considerations for using 38
removing an event filter 31
responding to an intrusion 5
Response list
customizing signature attributes 13

s
Security Events tab 12
customizing signature attributes 13
sensor
policies 5
Session Recorder X.X Policy 10
signature
creating a custom signature 6
definition of pre-defined 13
groups of 12
prerequisite to configuring 12
SMTP EXPN, monitoring user name associated with 69
SMTP, monitoring user name associated with 69
SNMP community strings 62
SNMP_Community context 62
specifying addresses 32
standard policies 8
String box, syntax for 38

t	tabs in the policy editor
Connection Events 12
Event Filters 12
Packet Filters 12
Security Events 12
User-Defined Events 12
technical support, Internet Security Systems viii
text editor
using to edit policy files 10
troubleshooting policy files 43
tuning 14
typographical conventions vii

u
Unix start-up procedure 49
update.policy 45
URL_Data context 63–67
user interface
console 2
User_Login_Name context 68
User_Probe_Name context 69
user-defined event
creating 36
User-Defined Events tab 12
user-defined signature
attributes of 36
contexts 53
regular expressions 38
role of 36
using filters 24

v
VIEWSESSION
controlling frequency of responses 16
VRFY, monitoring user name associated with 69
## Index

<table>
<thead>
<tr>
<th>W</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web site, Internet Security Systems    viii</td>
</tr>
<tr>
<td>Web Watcher X.X policy          10</td>
</tr>
<tr>
<td>Windows 2000 start-up procedure    47, 49</td>
</tr>
<tr>
<td>Workgroup Manager         2</td>
</tr>
</tbody>
</table>
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 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 computer and networking hardware and software, or (iv) interaction with software or firmware not provided by ISS. If Licensee failed to properly install or use the Software, or if ISS informed Licensee by telephone or written notice that repair or replacement of the Software may not be practicable, ISS may require the termination of any such nonconformity, then ISS or, if ISS reserves ownership of the Software, the manufacturer is Internet Security Systems, Inc., 6303 Barfield Road, Atlanta, GA 30328, USA.

5. Warranty Disclaimer - ISS DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTIES ARE HEREBY DISCLAIMED, WHETHER EXPRESS OR IMPLIED, TO THE EXTENT PERMITTED BY LAW. ISS CANNOT AND DOES NOT GUARANTEE THE COMPLETE EXCLUSION OF ERRORS IN THE SOFTWARE OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT ALL SOFTWARE ERRORS WILL BE CORRECTED. ISS DISCLAIMS ANY LIABILITY FOR INDUCEMENT TO INFRINGEMENT OF ANY PATENT, COPYRIGHT, TRADE SECRET, OR OTHER PROPRIETARY RIGHT. ISS DISCLAIMS ANY LIABILITY FOR UNINTENDED CONSEQUENCES AND DAMAGES ARISING FROM USE OF THE SOFTWARE, OR DAMAGES ARISING FROM THE TERMINATION OF ANY CONTRACT OR TORT (INCLUDING NEGLIGENCE AND STRICT PRODUCTS LIABILITY) FOR ANY SPECIAL, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING, BUT NOT LIMITED TO, LOSS OF DATA OR COMPUTER HARDWARE MALFUNCTION, EVEN IF ISS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

6. Support and Maintenance - During the term for which Licensee has paid the applicable support and maintenance fees, ISS will, upon request, provide 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 Support and Maintenance Plan. 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 Plan 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 Plan and 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 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 computer and networking hardware and software, or (iv) interaction with software or firmware not provided by ISS. If Licensee failed to properly install or use the Software, or if ISS informed Licensee by telephone or written notice that repair or replacement of the Software may not be practicable, ISS may require the termination of any such nonconformity, then ISS or, if ISS reserves ownership of the Software, the manufacturer is Internet Security Systems, Inc., 6303 Barfield Road, Atlanta, GA 30328, USA.

5. Warranty Disclaimer - ISS DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTIES ARE HEREBY DISCLAIMED, WHETHER EXPRESS OR IMPLIED, TO THE EXTENT PERMITTED BY LAW. ISS CANNOT AND DOES NOT GUARANTEE THE COMPLETE EXCLUSION OF ERRORS IN THE SOFTWARE OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT ALL SOFTWARE ERRORS WILL BE CORRECTED. ISS DISCLAIMS ANY LIABILITY FOR INDUCEMENT TO INFRINGEMENT OF ANY PATENT, COPYRIGHT, TRADE SECRET, OR OTHER PROPRIETARY RIGHT. ISS DISCLAIMS ANY LIABILITY FOR UNINTENDED CONSEQUENCES AND DAMAGES ARISING FROM USE OF THE SOFTWARE, OR DAMAGES ARISING FROM THE TERMINATION OF ANY CONTRACT OR TORT (INCLUDING NEGLIGENCE AND STRICT PRODUCTS LIABILITY) FOR ANY SPECIAL, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING, BUT NOT LIMITED TO, LOSS OF DATA OR COMPUTER HARDWARE MALFUNCTION, EVEN IF ISS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

6. Support and Maintenance - During the term for which Licensee has paid the applicable support and maintenance fees, ISS will, upon request, provide 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 Support and Maintenance Plan. 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 Plan 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 Plan and Support Policy.
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