INTERNET
SECURITY
SYSTEMS®

INTERNET|SECURITY|SYSTEMS®
proventia® network
Intrusion Detection System

A and AX Appliance User Guide

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

November 30, 2006

Contents

Preface

Overview

Purpose

This guide is designed to help you create policies for Proventia Network Intrusion Detection System (IDS) A and AX appliances. It also explains how to manage the appliances using Proventia Manager software.

Scope

This guide describes the features of the Proventia Manager and explains how to configure configure policy settings and manage the appliance.

Audience

This guide is intended for network security system administrators responsible for setting up, configuring and managing Proventia Network IDS appliances in a network environment. A fundamental knowledge of network security policies and IP network configuration is helpful.

What's new in this release

This release supports the 1.4 firmware release for the Proventia Network IDS A and AX appliances. The new features in this release include the following:

- **Proventia Manager**

  Proventia Manager is a browser-based, local management interface that enables you to manage a single appliance. Through Proventia Manager, you can create policies, view events, manage appliance settings, and configure updates for the appliance.

  Proventia Manager also offers you the ability to multi-select items in a list, as well as Sorting, Grouping, and Filtering features that make searching for and editing events easy.

- **Responses**

  The responses contained within your response policy determine how the appliance should act when it detects an intrusion or other important event in your system. You create responses and apply them to your security policies as needed. You can configure the following response types:

  - **Email**. Send email alerts to an individual address or email group.
  - **Log Evidence**. Log important alert information to a saved file.
  - **SNMP**. Send SNMP traps to a consolidates SNMP server.
  - **User-specified**. Send alert responses based on special requirements you have for monitoring the network.

- **Protection Domains**

  Protection domains let you define security or user-defined event policies for different network segments monitored by a single appliance. Protection domains act like virtual sensors, as though you had several appliances monitoring the network. They work exclusively in conjunction with security and user-defined events, to help you monitor your network. You can define protection domains by ports, VLANs, or IP address ranges.

- **Response Filters**

  Response filters let you refine your security policy by allowing you more granular control. You can define exceptions to the current policy for a particular protection domains, so each policy is fine-tuned for the network segment it monitors.

- **Ignore response available for Security Events and Response Filters**

  Manually set the Ignore response to tell the appliance to ignore events that are not a threat to your network, reducing the number of events you need to track.

- **Enhanced diagnostics and statistics**

  Using the Driver, Packet Analysis, and Protection statistics, you can view view network traffic the appliance has monitored to troubleshoot or to determine important trends across the network.

Important: If you plan to manage the appliance through SiteProtector, you must update SiteProtector to the appropriate Database Service Pack (DBSP). See the Readme for more information.

About Proventia Appliance Documentation

Introduction

This guide explains how to configure intrusion detection, packet filter settings, and other policy settings for Proventia Network IDS appliances using the Proventia Manager software (local management interface). It also provides information for managing the appliances using both the Proventia Configuration Menu and the Proventia Manager.

Locating additional documentation

Additional documentation described in this topic is available on the ISS Web site at http://www.iss.net/support/documentation/.

Related publications

See the following for more information about the appliance:

Document	Contents
Proventia Network IDS A Appliance Quick Start Guide	Instructions for installing firmware updates and initially configuring the Proventia A Intrusion Detection appliances.
Proventia Network IDS AX Appliance Getting Started Guide	Instructions for connecting and configuring Proventia Network IDS AX appliances.
Proventia Network Intrusion Products Help	Help located in Proventia Manager and the Proventia Network Intrusion Products' (A, AX, G, and GX series appliances) Policy Editors in SiteProtector.
Proventia Intrusion Detection Appliance Data Sheet	General information about previous Proventia Network IDS appliance features.
Proventia Network IDS Intrusion Detection Appliance FAQ	Frequently asked questions about the appliance and its functions.
Readme File	The most current information about product issues and updates, and how to contact Technical Support located at http://www.iss.net/download/.

Table 1: *Reference documentation*

Conventions Used in this Guide

Introduction

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

In procedures

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

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

Table 2: *Typographic conventions for procedures*

Command conventions

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

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

Table 3: *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 frequently asked questions (FAQs), white papers, online user documentation, current versions listings, detailed product literature, and the Technical Support Knowledgebase (http://www.iss.net/support/knowledgebase/).

Support levels

ISS offers three levels of support:

- Standard
- Select
- Premium

Each level provides you with 24-7 telephone and electronic support. Select and Premium services provide more features and benefits than the Standard service. Contact Client Services at clientservices@iss.net if you do not know the level of support your organization has selected.

Hours of support

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

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

Table 4: *Hours for technical support*

Contact information

The following table provides electronic support information and telephone numbers for technical support requests:

Regional Office	Electronic Support	Telephone Number
North America	Connect to the MYISS section of our Web site: www.iss.net	**Standard:** (1) (888) 447-4861 (toll free) (1) (404) 236-2700 **Select and Premium:** Refer to your Welcome Kit or call your Primary Designated Contact for this information.
Latin America	support@iss.net	(1) (888) 447-4861 (toll free) (1) (404) 236-2700

Table 5: *Contact information for technical support*

Regional Office	Electronic Support	Telephone Number
Europe, Middle East, and Africa	support@iss.net	(44) (1753) 845105
Asia-Pacific, Australia, and the Philippines	support@iss.net	(1) (888) 447-4861 (toll free) (1) (404) 236-2700
Japan	support@isskk.co.jp	Domestic: (81) (3) 5740-4065

Table 5: *Contact information for technical support*

Chapter 1

Introducing Proventia Network Intrusion Detection System Appliances

Overview

Introduction

This chapter introduces the Proventia Network Intrusion Detection System appliances and describes how their features monitor the network with a minimum of configuration.

In this chapter

This chapter contains the following topic:

Intrusion Detection

Introduction

Proventia Network Intrusion Detection System (IDS) appliances monitor the network for malicious attacks while preserving network bandwidth and availability. These appliances are purpose-built, Layer 2 network security appliances that you can deploy either at the gateway or the network to monitor intrusion attempts, denial of service (DoS) attacks, malicious code, backdoors, spyware, peer-to-peer applications, and a growing list of threats without requiring extensive network reconfiguration.

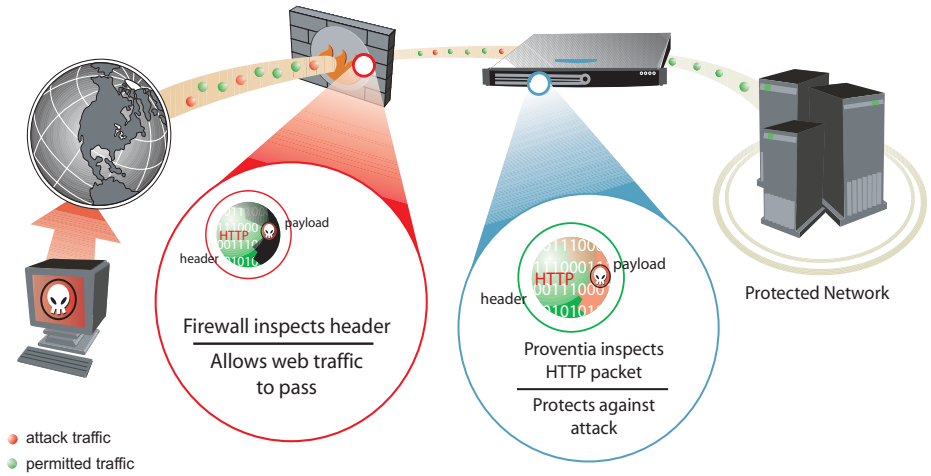

Figure 1: *Intrusion detection overview*

Figure 1 displays how the IDS appliances monitor your network. With flexible deployment options and out-of-the-box functionality, these appliances ensure accurate, high-performance monitoring at both the network perimeter and across internal networks and internal network segments.

Protection features

Proventia intrusion detection features include proven detection technologies, along with the latest security updates. These appliances understand the logical flow and state of traffic, to help you monitor network threats.

Proventia Network IDS appliances offer the following features to monitor the network:

- **Packet filters**

  You can create packet filters that enable the appliance to ignore incoming packets from particular IP addresses, port numbers, protocols, or VLANs, thereby allowing the appliance to focus on packet content that may truly affect or threaten your network.

- **Automatic security content updates based on the latest security research**

  You can automatically download and activate updated security content. The security updates you receive are a result of ISS's X-Force Research and Development Team's ongoing commitment to provide the most up-to-date protection against known and unknown threats.

- **Virtual Patch™ protection**

  Proventia's Virtual Patch capability provides a valuable time buffer, eliminating the need for you to immediately patch all vulnerable systems. You can wait until you are ready to manually update appliances or until scheduled updates occur, rather than having to patch and reboot systems that could potentially bring down the network.

- **SNMP support**

  Using SNMP-based traps, you can monitor key system problem indicators or respond to security or other appliance events using SNMP responses.

Management features

You can create and deploy security policies, manage alerts, and apply updates for your appliances either locally or through a central appliance management system.

Proventia Network IDS appliances offer you the following management capabilities:

- **Proventia Configuration Menu**

  The Proventia Configuration Menu is your local configuration interface. Use this tool to configure your appliance settings.

- **Proventia Manager**

  Proventia Manager offers a browser-based graphical user interface (GUI) for local, single appliance management. You can use Proventia Manager for the following functions:

  - monitoring appliance's status
  - configuring packet filters
  - managing appliance settings and activities
  - reviewing alert details
  - managing security policies with protection domains.

- **Proventia® Management SiteProtector**

  SiteProtector is the ISS management console. With SiteProtector, you can manage components and appliances, monitor events, and schedule reports. By default, your appliance is set up for you to manage it through the Proventia Manager, but if you are managing a group of appliances along with other sensors, you may prefer the centralized management capabilities that SiteProtector provides.

  When you register your appliance with SiteProtector, SiteProtector controls the following management functions of the appliance:

  - Packet filters
  - Intrusion detection settings
  - Alert events
  - Automatic appliance and security content updates

  Reference: For instructions on managing the appliance through SiteProtector, see the SiteProtector user documentation at http://www.iss.net/support/documentation/ or the SiteProtector Help.

Chapter 2

Configuring the Appliance

Overview

Introduction

This chapter describes how to configure the IDS appliance to connect to the network. It also outlines other appliance settings you can configure at any time, such as backup and restore settings and SNMP settings.

In this chapter

This chapter contains the following topics:

Before You Begin

Introduction

If you reinstalled the appliance firmware, you must reconfigure the appliance settings through Proventia Setup.

If you upgraded the firmware, your appliance settings were preserved. The only steps you must complete for initial configuration are accepting the Software License Agreement and establishing a password for Proventia Manager access. If you want to change other appliance settings, review the checklist provided below and copy any information you need to remember.

Configuration settings checklist

Use the checklist in Table 6 to obtain the information you need to configure your Proventia A appliance.

✓	Setting	Description
❑	Appliance hostname	The unique computer name for your appliance **Example:** *myappliance*
	Your setting:	
❑	Appliance domain name	The domain suffix for the network **Example:** *mydomain.com*
	Your setting:	
❑	Appliance domain name server	This is the IP address of the server you are using to perform domain name lookups (DNS search path). (optional). **Example:** *10.0.0.1*
	Your setting:	
❑	Management Port IP Address	An IP address for the management network adapter.
	Your setting:	
❑	Management port subnet mask	The subnet mask value for the network that will connect to your management port.
	Your setting:	
❑	Management port default gateway (IP address)	This is the IP address for the management gateway.
	Your setting:	

Table 6: *Information checklist*

Using Proventia Setup

Introduction

Proventia Setup is the program you use to configure initial appliance settings. If you connected the appliance directly to a computer using a serial Console cable, you are ready to log in and begin configuring. See "Completing the initial configuration."

If you want to configure the appliance from a remote computer, follow the procedure below, which explains how to connect to the appliance using Hyperterminal. You may use another terminal emulation program, such as PuTTY, to connect to the appliance, but those procedures are not outlined here. Follow the instructions listed in the documentation for your program.

Connecting to the appliance remotely

To connect to the appliance remotely using Hyperterminal:

1. On your computer, select **Start→ Programs→ Accessories→ Communications.**
2. Select **Hyperterminal**.
3. Create a new connection using the following settings:

Setting	Value
Communications Port	Typically COM1 (depending on computer setup)
Emulation	VT100
Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

4. Press ENTER to establish a connection.

   When the connection is established, the Proventia Setup Configuration Menu appears.

   Tip: If you are unable to establish a connection, ensure the appliance has power and that you have started the appliance.

Completing the initial configuration

To complete the initial configuration for the appliance:

1. At the unconfigured login prompt, type the user name **admin**, and then press ENTER.
2. To enter the password, type the default password **admin**.
3. Select **Start**, and then press ENTER.
4. Read the Software License Agreement, and then select **Accept** to continue.

5. Follow the on-screen instructions.

   The following table describes the required information.

Information	Description
Change Password	• **Admin Password**—To access the Proventia Setup Configuration Menu on the appliance, you must provide this password. This password can be the same as the root password. • **Root Password**—When you access the appliance from a command line, you must provide this password. • **Proventia Manager Password**—When you access Proventia Manager, you must provide this password. This password can be the same as the root password.
Network Configuration Information	• **IP Address**—The IP address of the management network adapter. • **Subnet Mask**—The subnet mask value for the network that connects to the management interface. • **Default Gateway**—The IP address for the management gateway.
Host Configuration	The appliance uses domain names and DNS information to send email and SNMP responses. If you do not configure this information during setup, you must specify the IP address of the appliance's mail server each time you define an email or SNMP response. • **Hostname**—The computer name for the appliance. Example: myappliance. • **Domain Name**—The domain suffix (DNS search path) for the network. Example: mycompany.com. • **Primary Name Server**—The IP address for the DNS used to perform domain name lookups. Example: 10.0.0.1 • **Secondary Name Server**—The IP address for the secondary DNS used to perform domain name lookups.
Time Zone Configuration	These settings determine the time zone for the appliance.
Date/Time Configuration	You must set the date and time for the appliance as it appears in the management interface, so you can accurately track events as they occur on the network.
Agent Name Configuration	The Agent Name is the appliance name as it appears in the management interface. This name should correspond to a meaningful classification in the network scheme, such as the appliance's geographic location, business unit, or building address.
Port Link Configuration	Port link settings determine the appliance's performance mode, or how the appliance handles its connection to the network. You can select the speed (the rate at which traffic passes between the appliance and the network) and the duplex mode (which direction the information flows). Select link speeds and settings compatible with your particular network and in relation to the other devices that bracket the Proventia A appliance. If you are not sure about your network settings, select Auto to enable the appliance to negotiate the speed and duplex mode with the network automatically. **Note**: After the initial appliance configuration, you can only change port link speed and duplex settings for the monitoring ports through Proventia Manager. For more information, see "Managing Network Adapter Cards".

6. When you have entered all the information, the appliance applies the settings.

   When prompted, press ENTER to log off the appliance.

Once you have completed the initial configuration steps, you can use the Configuration Menu to configure other appliance settings, such as backup and recovery settings, and SNMP settings.

Configuring Other Appliance Settings

Introduction

Through the Configuration Menu, you can view or edit the appliance settings you configured during the initial setup. You can also manage the following important appliance settings:

Select this menu option...	To do this...
Appliance Information	View information about the appliance.
Appliance Management	• Back up the current configuration. • Restore current configuration or factory default. • Disable remote root access to the appliance. • Reboot or shut down the appliance.
Agent Management	• View the version or status information for the Agent, Engine, or Daemon. • Change the agent name.
Network Configuration	• Change the IP address, subnet mask, or gateway. • Change the host name, domain name, or the primary and secondary DNS. • Change management port link settings.
Time Configuration	• Change the time zone, date, or time for the appliance. • Configure the network time protocol.
Password Management	Change the admin, root, or Proventia Manager passwords.
SNMP Configuration	Enable the appliance to send SNMP traps when appliance system-related events occur.

Table 7: *Configuration Menu*

Appliance information

You can view the following information about appliance settings:

Item	Description
Serial Number	The appliance's serial number.
Base Version	The firmware version with which the appliance was shipped from the factory.
XPU Version	The latest X-Press Update (XPU) or security content update installed on the appliance.
Firmware Version	The latest firmware version installed on the appliance.
Agent Name	The agent model name, such as Proventia_A1204.
Host Name	The name given to the appliance when it was installed, as it appears on the network. This is the name that appears in the management interface.
IP Address	The IP address you use to manage the appliance through Proventia Manager and SiteProtector.

Table 8: *Appliance information*

Item	Description
Netmask	The subnet mask value for the network that connects to the management port.
Gateway	The IP address for the management gateway.
Primary DNS	The IP address of the primary server you use to perform domain name lookups (DNS search path).
Secondary DNS	The IP address of the secondary server you use to perform domain name lookups (DNS search path).

Table 8: *Appliance information (Continued)*

Appliance management

From the Appliance Management Menu, you can perform the following tasks:

Task	Description
Back up the current configuration	When you back up the current configuration, all custom information is saved to an image file that resides on a special backup partition on the appliance's hard drive. When you restore an image from the current backup file, the hard drive is re-imaged with the information you have saved, and everything is overwritten except the special backup partition.
Restore the configuration	You have two options for restoring the configuration: • **Backup configuration**—Restores the appliance settings to the most current backup configuration. • **Factory default**— Restores the appliance settings to the default settings for the latest firmware version or update you have installed. **Note**: This option preserves the current host, network, time zone, and password settings.
Disable remote root access	You can disable remote access to the root user. If you disable remote access, the root user can only log on to the appliance from a local console. After you disable access, only the admin user has remote access permission. You can re-enable remote root access by logging into the appliance as the root user through a terminal emulation session, and then typing `enable-root-access` at the command prompt.
Reboot or shut down the appliance	You can also reboot or shut down the appliance from the Proventia Manager.

Table 9: *Appliance management tasks*

Agent management

From the Agent Management Menu, you can perform the following tasks:

Task	Description
View the agent status	You can view the agent, engine, and daemon status.
Change the agent name	The agent name is the appliance name that appears in the management console, either Proventia Manager or SiteProtector. If you change the agent name, the new name appears in SiteProtector after the next heartbeat.

Table 10: *Agent management tasks*

Network configuration

From the Network Configuration Menu, you can perform the following tasks:

Task	Description
Change IP Settings	You can change the IP address, subnet mask, or gateway for the appliance. For example, you might change these settings if you moved the appliance to a different location or network area.
Change host name settings	You can change the hostname, domain name, and primary and secondary name servers for the appliance. For example, you might change these settings if your DNS server has changed.
Change management port link settings	You can change the link speed and duplex settings for the management port. Select link speeds and settings compatible with your particular network and in relation to the other devices that bracket the appliance. **Note**: After the initial configuration, you can only change port link speed and duplex settings for the monitoring (Protected) ports through Proventia Manager or SiteProtector. For more information, see “Managing Network Adapter Cards” on page 98.

Table 11: *Network configuration tasks*

Time configuration

From the Time Configuration Menu, you can perform the following tasks:

Task	Description
Change the date and time	The time and date you set for the appliance determines when appliance events are recorded and how they appear in the management interface.
Change the time zone	Ensure you have the correct time zone set for the appliance. Once this is set, you should not have to change this setting unless you physically relocate the appliance.
Set the network time protocol	The network time protocol (NTP) synchronizes the local date and time with the network time server. If you specify more than one time server, the appliance gets a number of samples from each server you specify to determine the correct time.

Table 12: *Time configuration tasks*

Password management

From the Password Management Menu, you can perform the following tasks:

Task	Description
Change admin, root, or Proventia Manager passwords	You can also change passwords through Proventia Manager. See “Configuring User Access” on page 109.
Disable the boot loader password	The boot loader password protects the appliance from unauthorized user access during the boot process. The boot loader password is the same password as the root password. You can disable the boot loader password; the root password remains active.

Table 13: *Password management tasks*

SNMP configuration

When you enable SNMP from the Configuration Menu, you are enabling the appliance to send information about system health-related events such as low disk space, low swap space, very high CPU usage, or physical intrusions. These settings do not affect SNMP responses assigned to events that occur on the network. For information about SNMP responses to events, see “Configuring SNMP Responses” on page 99.

From the SNMP Configuration Menu, you can perform the following tasks:

Task	Description
Enable SNMP	Guides you through providing the information the appliance needs to communicate with the SNMP manager. You will be asked to provide the following: • System location, contact, and name • IP address for the main trap receiver • Communication port number (port 162 by default) • Community string (public or private) • Trap version
Disable SNMP	Stops the appliance from sending system related information to the SNMP manager.
Start or stop the SNMP daemon	Allows you to reset communication with the SNMP service.
View SNMP system information	View the current SNMP settings for the appliance.
Add or delete a trap receiver	The trap receiver IP address is the server address where the SNMP Manager is running. The SNMP Host must be accessible to the appliance to send SNMP traps. Allows you to add additional trap receivers to receive messages from the appliance, or to delete a trap receiver you no longer want to receive messages.
Enable read access for the trap receiver	Allows the trap receiver to collect information about system-related events. **Caution**: If you choose to allow SNMP read access, UDP port 161 will be opened on the protection firewall.

Table 14: *SNMP configuration tasks*

Chapter 3

Using Proventia Manager

Overview

Introduction

This chapter describes how to use Proventia Manager, the local management interface, to perform updates, make adjustments, and augment configuration settings.

In this chapter

This chapter contains the following topics:

Accessing Proventia Manager

Introduction

Proventia Manager is the Web-based management interface for the appliance.

Use Proventia Manager to perform the following tasks:

- monitor the status of the appliance
- configure and manage settings
- review and manage appliance activities

Logging on to Proventia Manager

To log on to the Proventia Manager interface:

1. Open Internet Explorer.
2. Type `https://` <appliance IP address>.
3. Log in using the user name `admin` and the Proventia Manager password.
4. If a message informs you that you need Java Runtime Environment (JRE), install it, and then return to this procedure.
5. Select **Yes** to use the Getting Started procedures.

   Note: ISS recommends that you use the Getting Started procedures to help you customize the appliance settings. If this window does not appear, you can also access the Getting Started procedures from the Help.
6. Click **Launch Proventia Manager**.

Navigating Proventia Manager

Introduction

If you plan to use the Proventia Manager to manage the appliance, you should familiarize yourself with its navigation features.

About the navigation buttons

The following buttons appear on every page in the Proventia Manager:

Click this button...	To do this...
SYSTEM LOGS	Access the System Logs page.
ALERTS	Access the Alerts page for the area you have selected in the left navigation pane.
HELP	Access the online Help.
	Minimize or maximize the navigation pane.

Table 15: *Navigation buttons*

About the left navigation pane

In the left pane, you select the item in the tree that you want to configure. Some items have more than one component for you to configure. Expand the tree to display a sub-list of configurable elements in that area.

The following table describes each area of Proventia Manager:

This item...	Lets you view or configure...
Notifications	In the Notifications area, you can view high-level Alert Event Log information, System Logs, system (appliance) alert information. See “Viewing Alerts and System Information” on page 111 for more information.
Intrusion Detection	In the Intrusion Detection area, you can configure responses, protection domains, and event types that help you monitor the network for intrusions. You can also view important security alert and determine how the appliance should respond when it detects intrusions. See the following topics for more information: • “Working with Security Events” on page 53 • “Configuring Responses” on page 43 • “Configuring Other Intrusion Detection Settings” on page 67
Packet Filters	In the Packet Filters area, you can create and edit packet filter rules to filter out packets you do not want the appliance to monitor. See “Configuring Packet Filters” on page 87 for more information.

Table 16: *Left navigation pane*

This item...	Lets you view or configure...
System	In the System area, you can configure and view information about various aspects of the appliance. You can configure user access, network adapter cards, alerts, and advanced parameters to help you monitor the appliance. You can also view and download important system logs, manage licenses, and reboot the appliance from this area. See the following topics for more information: • "Configuring Local Tuning Parameters" on page 95 • "Managing System Settings" on page 105
Statistics	The Statistics area lets you view important statistics about appliance activity, such as Protection, Packet, and Driver information. See "Viewing Statistics" on page 117 for more information.
Updates	Use the Updates area to configure and manage updates for the appliance, so that you have the latest protection available for your network. See "Updating the Appliance" on page 23 for more information.
Support	The Support area provides contact information for Technical Support, as well as helpful links to provide you assistance with the appliance. See "Getting Technical Support" on page ix for more information.

Table 16: *Left navigation pane (Continued)*

About icons

The following table describes icons that appear in Proventia Manager as you work:

Icon	Description
	Click this icon to add an item to the list.
	Click this icon to edit an item in the list.
	Click this icon to remove an item (or items) from the list. You can use the standard [SHIFT]+click or [CTRL]+click methods to select adjacent or non-adjacent items in the list. **Note**: In some cases, when you click Remove, an item is not removed from the list, but it is disabled and reset to its default state.
	Click this icon to group items by column in a table. For example, you could group security events by severity. This means that your high, medium, and low severity events each have their own group, making it easier for you to search for events.
	Click this icon to reset table groupings to their default settings.
	Click this icon to select the columns you want to display on a page.
	Select an item in the list and click this icon to move the item up the list.
	Select an item in the list and click this icon to move the item down the list.

Table 17: *Proventia Manager policy icons*

Icon	Description
	Select an item in the list and click this icon to copy the item to the clipboard. **Tip**: You can use the standard [SHIFT]+click or [CTRL]+click methods to select adjacent or non-adjacent items in the list.
	Click this icon to paste a copied item from the clipboard into a list. After you paste the item, you can edit it.
	If this icon appears on a page or next to a field on a page, then you must enter required data in a field, or the data you have entered in a field is invalid.

Table 17: *Proventia Manager policy icons (Continued)*

About saving changes

Each time you navigate from one location to another in the Proventia Manager, you should click the Save Changes button to ensure the changes are applied. If you do not save information before navigating to another page, you are prompted to save your information. To move to another page without saving changes, you should click the Cancel Changes button so that you are not prompted to save before you click the new link.

Installing the License File

Introduction

The Licensing page displays important information about the current status of the license file, including expiration dates. Additionally, this page allows you to access the License Information page, which includes information about how to acquire a current license. Proventia IDS appliances require a properly configured license file. If you have not installed the appropriate license file, you cannot manage the appliance through Proventia Manager or SiteProtector.

To purchase a license, contact your local sales representative.

Use the procedure below to install the license file. This is necessary to make your appliance run at full capability. Installation involves saving the license file information to the appropriate location so that the Proventia Manager software can locate and acknowledge it.

Prerequisites

Before you install the license file, complete the following:

- register your customer license
- download the license from the ISS Registration Center

Installing the license file

To install the license file:

1. In Proventia Manager, select **System→Licensing**.
2. Click **Browse**.
3. Locate the license file that you downloaded.
4. Click **OK**.
5. Click **Upload**.

Working with Proventia Manager

Introduction

When you open the Proventia Manager, the Home page provides an immediate snapshot of the appliance's current status. This page includes the following navigation, information and reporting options:

- device name (the appliance name specified during setup)
- detection status
- system status
- alerts for each module
- important messages

Viewing detection status

The detection status area describes the current status of the intrusion detection component. Selecting a component name links you to the component status page.

The following status icons show you the current status of a component:

This icon...	Indicates...
	The component is active.
	The component is stopped.
	The component is in an unknown state. This status requires immediate attention.

Table 18: *Protection status icons*

Viewing system status

On the Home page, the System Status group box describes the system's current status.

The following table describes the data available in the System Status area:

Statistic	Description
Model Number	The model number of the appliance.
Base Version Number	The base version of the appliance software. **Note:** The base version is the software version shipped with the appliance, or the software version of the most recent firmware update.
Uptime	How long the appliance has been online, in the following format: `x days, x hours, x minutes`
Last Restart	The last time the appliance was restarted, in the following format: `yyyy-mm-dd hh:mm:ss` **Example:** `2004-05-04 16:24:37`
Last Firmware Update	The last time appliance firmware was updated, in the following format: `yyyy-mm-dd hh:mm:ss - version: x.x` **Example:** `2004-05-04 16:25:56 - version: 1.7`

Table 19: *System Status statistics*

Statistic	Description
Last Intrusion Detection Update	The last time appliance security content was updated, in the following format: `yyyy-mm-dd hh:mm:ss - version: x.x` **Example:** `2004-01-25 12:34:36 - version: 1.7`
Last System Backup	The last time a system backup was created, in the following format: `yyyy-mm-dd hh:mm:ss` **Example:** `2004-05-04 15:49:01`
Backup Description	The backup type on the appliance: • Factory Default • Full System Backup

Table 19: *System Status statistics (Continued)*

Viewing important messages

The Home page displays important messages about licensing and updates. If you have not configured the appliance to download updates automatically, these messages may appear with a link to the appropriate Proventia Manager page.

Chapter 4

Updating the Appliance

Overview

Introduction

This chapter describes how to update the appliance using Proventia Manager. You can manually download and install firmware updates and security updates, or you can configure the appliance to automatically download and install some or all updates at designated times.

In this chapter

This chapter contains the following topics:

Updating the Appliance

Introduction

Ensure the appliance is always running the latest firmware and intrusion detection updates. The appliance retrieves updates from the ISS Download Center, accessible over the Internet.

You can update the appliance in two ways:

- configure automatic updates
- find, download, and install updates manually

Types of updates

You can install the following updates:

- **Firmware updates**. These updates include new program files, fixes or patches, enhancements, or online Help updates.
- **Intrusion detection updates**. These updates contain the most recent security content provided by ISS's X-Force.

You can find updates on the Updates to Download page, and you can schedule automatic update downloads and installations from the Update Settings page.

Note: Some firmware updates require you to reboot the appliance. For more information about product issues and updates, see the Proventia A Intrusion Detection Appliance Readme on the ISS Download Center at http://www.iss.net/download/.

Finding available updates

When you click the Find Updates button on the Update Status page, the appliance checks for the following:

- updates already downloaded to the appliance and ready to be installed
- updates available for download from the ISS Download Center

If the appliance finds updates to download or install, an alert message displays a link to the appropriate page (the Download Updates or Install Updates page).

Update packages and rollbacks

A rollback removes the last intrusion detection update installed on the appliance. You cannot roll back firmware updates.

Note: ISS recommends that you perform a full system backup before you install a firmware update. If you enable automatic firmware updates, you should enable the Perform Full System Backup Before Installation option.

After an update is installed, the appliance deletes the update package so the downloaded package is no longer on the appliance. If you roll back the update, the appliance is available for update downloads and installation the next time updates are available or at the next scheduled automatic update.

SiteProtector management

If you use SiteProtector to manage the appliance, you can install an update while the appliance is registered with the SiteProtector Agent Manager. You can also configure it to use the SiteProtector X-Press Update Server to download and install available updates.

Consider using the X-Press Update Server under the following conditions:

- If you have deployed a large number of appliances, you can save bandwidth. The appliances can request updates from one Update Server, as opposed to using bandwidth to download the same updates for each appliance from the ISS Download Center.
- If you want to download updates in a more secure environment and do not want every appliance to have Internet access for downloads, the appliance can request updates from the Update Server. In this case, only the Update Server requires the Internet connection.

See the SiteProtector documentation or online help for information about configuring the X-Press Update Server settings. You will also find helpful information in Knowledgebase Article 3020 on the ISS Web site.

Virtual Patch™ technology

Automatic security updates come from ISS X-Force using Virtual Patch technology. The Virtual Patch process protects systems against attack during the interval between discovery of a vulnerability and the manual application of a security patch.

The Virtual Patch is an important component of ISS's Dynamic Threat Protection platform. By combining the functionality of vulnerability detection, intrusion detection, management, and advanced correlation tools, you can have a unified view of system-wide intrusion protection capabilities to protect against known and unknown threats.

Troubleshooting download problems

If you experience problems in Proventia Manager after you apply a firmware update, try the following steps:

1. Close the Web browser.
2. Clear the Java cache.
3. Restart the Web browser, and then log on to Proventia Manager.

For more information about how to clear the Java cache, refer to the operating system documentation.

Updating the Appliance Automatically

Introduction

Use the Update Settings page to configure the appliance to automatically check for and install updates. You define the following settings to configure automatic updates for the appliance:

- when to check for updates
- when to download and install security updates
- when to download firmware updates
- how and when to install firmware updates
- which firmware update version(s) to install

Note: When you install a firmware update, the appliance may lose link temporarily.

Example

You want to configure the appliance to check for updates daily at 3:00 A.M. If it finds any updates (either firmware or security updates), you want it to automatically download all of the updates, and then install the security updates immediately. As the final steps, at 5:00 A.M., you want the appliance to automatically perform a system backup and then install the available firmware updates.

The following table describes the appliance update process with these settings:

Stage	Description
1	At 3:00 AM, the appliance checks the ISS Download Center for updates.
2	The appliance downloads security and firmware updates.
3	The appliance installs security updates immediately.
4	At 5:05 AM, the appliance does the following: • reboots, and then creates a system backup • installs the firmware update, and then reboots if necessary

Table 20: *An example of the update process*

Procedure

To update the appliance automatically:

1. On the **Update Settings** page, complete or change the settings as indicated in the following table.

Section	Setting	Description
Automatically Check for Updates	Check for updates daily or weekly	If you enable this option, select the **Day Of Week** and **Time Of Day** the appliance should check for updates. **Note**: Set the appliance to check for updates at least one (1) hour prior to installing scheduled automatic updates to ensure the appliance has downloaded all the necessary updates.
	Check for updates at given intervals	Checks for updates several times a day. Type a value in the **Interval (minutes)** box, or move the slider bar to select a value. The minimum interval is 60 minutes; the maximum is 1440.
Security Updates	Automatically Download	Automatically downloads security updates.
	Automatically Install	Automatically installs security updates.
Firmware Updates	Automatically Download	Automatically downloads firmware updates.
Firmware Updates - Install Options	Perform Full System Backup Before Installation	Enables the appliance to reboot and perform a full system backup before it installs any updates. **Note**: Each time the appliance performs a backup, it overwrites the previous system backup.
	Do Not Install	Downloads firmware updates but does not install them. See "Updating the Appliance Manually" on page 28 for more information.
	Automatically Install Updates	Automatically installs firmware updates. **Note**: When the appliance automatically installs updates, it may be offline for several minutes.
Firmware Updates - When To Install	Delayed	Installs updates on the **Day Of Week** and **Time Of Day** you specify. **Note**: You must configure automatic installation to occur at least one (1) minute after the appliance finishes downloading updates.
	Immediately	Installs updates as soon as they are downloaded. **Important**: ISS does not recommend this option.
	Schedule One Time Install	Installs one update instance at the **Date** and **Time** you specify.
Firmware Updates - Which Version To Install	All Available Updates	Installs all update versions, including the most recent one.
	Up To Specific Version	Installs all versions up to the **Version** number you specify.

2. Save your changes.

Updating the Appliance Manually

Introduction

If you have not configured automatic updates for the appliance or if you want to install an available update off-schedule, you can find and manually install updates. You must complete the following tasks to update the appliance manually:

- Finding and downloading available updates
- Installing updates

Note: When you install a firmware update, the appliance may lose link temporarily.

Finding and downloading available updates

To find and download available updates:

1. In Proventia Manager, select **Updates→Available Downloads**.
2. If your appliance model requires it, the Export Administration window appears.

   Review the agreement, select **Yes**, and then click **Submit**.
3. The Updates to Download window appears and displays the following message if updates are available: "There are updates available. Click here to see details."

   Click the link in the message.
4. On the Updates to Download page, click **Download All Available Updates**.

Installing updates

To install updates:

1. In Proventia Manager, select **Updates→Available Installs**.
2. If your appliance model requires it, the Export Administration Regulation window appears.

   Review the agreement, select **Yes**, and then click **Submit**.
3. On the Available Installs page, select the updates you want to install, and then click **Install Updates**.

   Note: Some firmware updates require you to reboot the appliance. For detailed information about each firmware update, review the Proventia A Intrusion Detection Appliance Readme on the ISS Download Center at http://www.iss.net/download.
4. View the installation status in the Update History table on the Update Status page.

Using Update Tools

Introduction

Use the Update Tools page to find updates or to roll back an update. A rollback removes the last update installed on the appliance. You cannot roll back firmware updates.

Cumulative updates and rollbacks

XPU updates are cumulative. The following example describes how the appliance behaves when rolling back cumulative updates.

Example

If you install version 1.1 but do not install version 1.2, and then you install version 1.3, version 1.2 is installed with version 1.3.

However, if you roll back from version 1.3, the appliance does not rollback to version 1.2. A rollback to the last applied update takes the appliance back to version 1.1.

Update packages and rollbacks

After an update is installed, the appliance deletes the update package, so the downloaded package is no longer on the appliance. If you roll back the update, then that update appears as available for download and installation the next time you find updates or at the next scheduled automatic update. For more information, see "Updating the Appliance Automatically" on page 26.

Finding available updates

To find available updates:

1. In Proventia Manager, select **Updates→Tools**.
2. Click **Find Updates**.
3. If the appliance finds updates to download or install, an alert message displays the link to the Available Downloads or Available Installs page.

   Click the appropriate link to download or install the latest updates.

Rolling back updates

To roll back updates:

1. In Proventia Manager, select **Updates→Tools**.
2. Click **Rollback Last Intrusion Detection Update**, and then click **OK**.
3. Press F5 to refresh the page and check the progress of the rollback.

Configuring Update Advanced Parameters

Introduction

You can tune update parameters for the appliance. Update parameters can determine the following behavior:

- whether the appliance searches for updates on the Internet
- whether the appliance deletes update files one they are installed
- how the appliance communicates with the SiteProtector X-Press Update Server (if SiteProtector management is enabled)

About advanced parameters

Advanced parameters are composed of name/value pairs. Each name/value pair has a default value.

For example, the parameter np.packet filter.log is a parameter that determines whether to log the details of packets that match packet filter rules you have enabled. The default value for this parameter is *on*.

You can edit the value of any parameter that appears in the list on the Advanced Parameters tab. If the parameter does not appear in the list, it does not mean the parameter has no default value. You simply need to add the parameter to the list with the new value.

Update advanced parameters

The appliance contains the following pre-configured update advanced parameters, listed in Table 21:

Note: Only the first two parameters appear on the Update Settings Advanced Parameters tab if you are managing the appliance through the Proventia Manager. If you have enabled SiteProtector management, you can configure the other default parameters for communicating with SiteProtector's Update Server.

Parameter	Type	Default Value	Description
Update.disable.remote.discovery	boolean	false	Specifies whether the appliance should look for updates on the Internet.
Update.preserve.update.files	boolean	false	Specifies whether to delete update files once they have been successfully installed.
Update.certificate.file	string	etc/httpd/conf/ss.crt/ca-bundle.crt	Specifies the SSL Cert Authority file to use when connecting to the Update Server.
Update.proxy.auth	boolean	false	Authorizes the use of the HTTP proxy server when connecting to the Update Server.
Update.proxy.enable	boolean	false	Enables the use of the HTTP proxy server when connecting to the Update Server.

Table 21: *Update advanced parameters*

Parameter	Type	Default Value	Description
Update.proxy.password	string	none	Specifies the password to the HTTP proxy server authentication for connecting to the Update Server.
Update.proxy.port	number	none	Specifies the port number of the HTTP proxy server for connecting to the Update Server.
Update.source.url	string	https://www.iss.net/XPU If the appliance is not connected to the Internet, use https//:<Update Server IP Address or name>:3994/xpu (Name is case sensitive.)	Specifies the address of the Update Server.
Update.proxy.user	string	none	Specifies the user name to the HTTP proxy server authentication for connecting to the Update Server.

Table 21: *Update advanced parameters*

Adding update advanced parameters

To add update advanced parameters:

1. Select **Update Settings**.
2. If needed, review the Export Agreement, select **Yes**, and then click **Submit**.
3. Select the **Advanced Parameters** tab.
4. Click **Add**.
5. Complete the settings as indicated in the following table.

Setting	Description
Name	Type a unique name for the parameter.
Comment	Type a unique description for the parameter.
Value	Select one of the following values: • **Boolean**. Select the Enabled check box to set the value as True, or clear it to set the value as False. • **Number**. If you select this option, type a numeric Value. • **String**. If you select this option, type the associated text string Value.

6. Click **OK**.
7. Save your changes.

Working with update advanced parameters

To edit, copy, or remove update advanced parameters:

1. Select **Update Settings**.
2. Select the **Advanced Parameters** tab, and then do one of the following:

If you want to...	Then...
Edit	**Tip**: You can edit some properties directly on the Advanced Parameters tab by double-clicking the item you want to configure. 1. Select the parameter, and then click the **Edit** icon. 2. Select or clear the **Enabled** check box. 3. Edit the parameter, and then click **OK**.
Copy	1. Select the parameter, and then click the **Copy** icon. 2. Click the **Paste** icon. 3. Edit the parameter as needed, and then click **OK**.
Remove	1. Select the parameter. 2. Click the **Remove** icon.

3. Save your changes.

Chapter 5

Managing the Appliance through SiteProtector

Overview

Introduction

This chapter describes how to set up the appliance so you can manage it through the SiteProtector Console.

In this chapter

This chapter contains the following topics:

Managing with SiteProtector

Introduction

SiteProtector is the ISS management console. With SiteProtector, you can manage components and appliances, monitor events, and schedule reports. By default, your appliance is set up for you to manage it through the Proventia Manager, but if you are managing a group of appliances along with other sensors, you may prefer the centralized management capabilities that SiteProtector provides.

What you manage with SiteProtector

When you register the appliance with SiteProtector, SiteProtector controls the following management functions of the appliance:

- Packet filters
- Intrusion detection settings
- Alert events
- Automatic updates

To change any settings for the functions listed here, you must use SiteProtector.

You can manage update and installation settings in Proventia Manager or in SiteProtector.

Note: When you register the appliance with SiteProtector, some areas of the Proventia Manager become read-only. When you unregister the appliance from SiteProtector, the Proventia Manager becomes fully functional again.

What you manage with Proventia Manager

You must manage the following local functions directly on the appliance, even when the appliance is registered with SiteProtector:

- enabling or disabling SiteProtector management
- manual updates

How the SiteProtector Agent Manager works

When you enable SiteProtector management, you assign the appliance to an Agent Manager. Agent Managers manage the command and control activities of various agents and appliances registered with SiteProtector and facilitate data transfer from appliances to the Event Collector, which manages real-time events it receives from appliances.

The Agent Manager also sends any policy updates to appliances, based on their policy subscription groups. Policy subscription groups are groups of agents or appliances that share a single policy. This is why you should determine the group to which the appliance will belong before you register it with SiteProtector: eventually, the group's policy is shared down to the appliance itself.

For more information about the Agent Manager, see the SiteProtector documentation or online Help.

How SiteProtector management works

When you register the appliance with SiteProtector, the appliance sends its first *heartbeat* to the Agent Manager to let it know it exists. A heartbeat is an encrypted, periodic HTTP request the appliance uses to indicate it is still running and to allow it to receive updates from the Agent Manager. When you register the appliance with SiteProtector, you indicate the time interval (in seconds) between heartbeats.

When the Agent Manager receives the heartbeat, it places the appliance in the group you specified when you set up registration. If you did not specify a group, it places the appliance in the default group "A-Series." If you clear the group box when you register the appliance, it places the appliance in Ungrouped Assets.

At that first heartbeat, if you selected to allow local appliance settings to override group settings, then the appliance maintains its local settings. If you did not select to allow local appliance settings to override group settings, then the Agent Manager immediately "pushes" the group's policy files to the appliance, even if the group's policy settings are undefined. For example, if you set packet filter rules on the appliance, and then you registered the appliance with a group that had no packet filter rules defined, the group policy would overwrite the local policy, and the appliance would no longer have packet filters enabled.

At the second heartbeat and each heartbeat thereafter, the Agent Manager "pushes" the group policy to the appliance. However, you can change some local appliance settings through SiteProtector. Any local policy settings you change on a specific appliance takes precedence over the group policy settings for that appliance only; the group policy settings remain in effect for all other appliances in the group.

How appliance updates work with SiteProtector

Once you register the appliance with SiteProtector, you must still update it regularly to maximize performance and to ensure it runs the most up-to-date firmware, security content, and database. ISS recommends that you schedule automatic database updates, security content updates, and firmware update downloads and installations.

Note: You can download and install firmware updates in Proventia Manager even if the appliance is registered with SiteProtector.

Use the Update Settings page to schedule the following automatic update options:

- downloading and installing firmware updates
- downloading and installing security content updates
- updating the database.

How SiteProtector handles appliance events

You can specify the events that generate and deliver an alert to SiteProtector. When an event occurs, the appliance sends an alert to SiteProtector. You can use the event information in the alert to create valuable reports. The alerts sent to SiteProtector still appear in the Alerts page in the Proventia Manager, if those alerts are configured for logging.

SiteProtector management options

When you register the appliance with a SiteProtector group, you can do the following:

- allow the appliance to inherit sensor group settings
- manage some or all of settings for a single appliance in the group independently in SiteProtector, so that the appliance maintains those individual settings regardless of group settings

Configuring SiteProtector Management

Introduction

Enabling SiteProtector management automatically does the following:

- Registers the appliance with SiteProtector
- Places the appliance in a specified SiteProtector group
- Directs the appliance to report to a specified Agent Manager

Use the Management page in Proventia Manager to set up and enable SiteProtector management for the appliance.

Once you have registered your appliance, you must add the Proventia A license file in SiteProtector. This enables you to apply updates through SiteProtector. See your SiteProtector documentation for more information about adding license files for agents and appliances.

Important: To manage the appliance with SiteProtector, you must run SiteProtector version 2.0, Service Pack 6.0 or later.

Before registering the appliance

ISS recommends that you do the following before you register the appliance with SiteProtector:

- Verify the name of the SiteProtector sensor group to which you want to assign the appliance.
- Verify the IP address and port for each SiteProtector Agent Manager that you want to use with the appliance.
- Ensure the appliance has the latest firmware update installed.

You can schedule automatic downloads and installations of firmware updates to the appliance, without unregistering the appliance from SiteProtector.

Reference: See "Updating the Appliance" on page 23 for more information.

Configuring SiteProtector management

To configure SiteProtector management:

1. In Proventia Manager, select **System→Management**.
2. Complete or change the settings as indicated in the following table.

Setting	Description
Register with SiteProtector	Select the check box to register the appliance with SiteProtector.
Local Settings Override SiteProtector Group Settings	Select this option to have the appliance maintain any local settings you have configured *at the first heartbeat*. If you do not select this option, the appliance will inherit the settings of the SiteProtector group you specify *at the first heartbeat*. **Note**: At the second heartbeat and each heartbeat thereafter, any policy settings you have changed at the group level will be sent to the appliance.

Setting	Description
Desired SiteProtector Group for Sensor	Type the name of the SiteProtector group to which the appliance should belong. If you do not specify a group, then the appliance will be added to the default “A Series” group. **Important**: You must assign the appliance to a group that contains only other Proventia A appliances.
Heartbeat Interval (secs)	Type the number of seconds the appliance should wait between sending heartbeats to SiteProtector. **Note**: This value must be between 300 and 86,400 seconds.

3. Click **Save Changes**.
4. Add the Agent Manager(s) with which you want the appliance to communicate. See "Configuring the Agent Manager.”

Configuring the Agent Manager

To configure the Agent Manager:

1. In Proventia Manager, select **System→Management**.
2. Ensure you have enabled registration with SiteProtector.
3. In the Agent Manager Configuration area, click **Add**.
4. Complete or change the settings as indicated in the following table.

Setting	Description
Authentication Level	Select an option from the list. **Note**: ISS recommends that you accept the default option *first-time trust*.
Agent Manager Name	Type the Agent Manager name exactly as it appears in SiteProtector. This setting is case-sensitive.
Agent Manager Address	Type the Agent Manager's IP address.
Agent Manager Port	Accept the default value 3995. **Note**: You can type a new port number, but you must also configure the new port number locally on the Agent Manager itself.
User Name	If the appliance must log into an account to access the Agent Manager, type the user name for that account here. **Note**: The account user name is set on the Agent Manager.
User Password	Click **Set Password**, type and confirm the password, and then click **OK**.
Use Proxy Settings	If the appliance must go through a proxy to access the Agent Manager, select the **Use Proxy Settings** check box, and then type the **Proxy Server Address** and **Proxy Server Port**.

5. Click **OK**.
6. Click **Save Changes**.

Verifying successful registration

To verify the appliance registered successfully with SiteProtector:

1. Open the SiteProtector Console.
2. In the left pane, select the group where you added the appliance.

   Note: If you did not specify a group when you registered appliance, it appears in the default group "A Series." If you cleared the default group, the appliance may appear in Ungrouped Assets.
3. Select the **Sensor** or **Agent** tab.

   The appliance should appear on the Sensor tab, and its status should show as "Active."

Disabling SiteProtector Management

To disable SiteProtector management:

1. In Proventia Manager, select **System→Management**.
2. Clear the **Register with SiteProtector** check box.
3. Click **Save Changes**.

Navigating SiteProtector

Introduction

If you are planning to use SiteProtector to manage the appliance, you should familiarize yourself with the navigation features that allow you to create, manage, and view the appliance's current policies.

For general information about navigating the SiteProtector Console, see the SiteProtector Help for your current version.

About policies and settings

You can configure the following appliance policies and settings in SiteProtector:

Select this item...	To do this...
Intrusion Detection	Configure responses, protection domains, and event types that help monitor the network for intrusions. You can also view important security alert and intrusion information, and determine how the appliance should respond to detected intrusions. See the following topics for more information: • "Working with Security Events" on page 53 • "Configuring Responses" on page 43 • "Configuring Other Intrusion Detection Settings" on page 67
Packet Filters	Create and edit packet filter rules to filter out packets you do not want the appliance to monitor. See "Configuring Packet Filters" on page 87 for more information.
Local Tuning Parameters	Configure local tuning parameters for the appliance, including: • appliance error, warning, and informational alerts • network adapter card settings • advanced parameters for the appliance itself, including update parameters and intrusion detection parameters See "Configuring Local Tuning Parameters" on page 95 for more information.
Statistics	View important statistics about appliance activity, such as Protection, Packet, and Driver information. See "Viewing Statistics" on page 117 for more information.
Updates	Configure and manage updates for a single appliance, so that you have the latest protection available for the network. See "Updating the Appliance" on page 23 for more information.

Table 22: *Policies and settings*

About icons

The following table describes icons that appear on the Policy page as you work:

Icon	Description
	Click this icon to add an item to the list.
	Click this icon to edit an item in the list.

Table 23: *Policy editor icons in SiteProtector*

Icon	Description
	Click this icon to remove an item (or items) from the list. You can use the standard [SHIFT]+click or [CTRL]+click methods to select adjacent or non-adjacent items in the list. **Note**: In some cases, when you click Remove, an item is not removed from the list, but it is disabled and reset to its default state.
	Click this icon to group items by column in a table. For example, you could group security events by severity. This means that your high, medium, and low severity events each have their own group, making it easier for you to search for events.
	Click this icon to reset table groupings to their default settings.
	Click this icon to select the columns you want to display on a page.
	Select an item in the list and click this icon to move the item up the list.
	Select an item in the list and click this icon to move the item down the list.
	Select an item in the list and click this icon to copy the item to the clipboard. **Tip**: You can use the standard [SHIFT]+click or [CTRL]+click methods to select adjacent or non-adjacent items in the list.
	Click this icon to paste a copied item from the clipboard into a list. After you paste the item, you can edit it.
	If this icon appears on a page or next to a field on a page, then you must enter required data in a field, or the data you have entered in a field is invalid.

Table 23: *Policy editor icons in SiteProtector*

About saving changes

You should save your changes before you navigate to another policy. In SiteProtector 2.0 SP6.1, you click Save All on the Console toolbar to save your changes before navigating to a new policy.

Opening an IPS policy in SiteProtector

To open an IPS policy in SiteProtector:

1. In the SiteProtector Console, do one of the following
   - To edit a group level policy, right-click the group in the left pane, and then select **Manage Policy** on the pop-up menu.
   - To edit a policy for a single appliance, on the **Agent** tab, right-click the appliance, and then select **Manage Policy** on the pop-up menu.
2. On the Policy tab, select Network IDS from the **Agent Type** drop-down menu.
3. To open the policy, do one of the following:
   - Select the policy for the group or appliance in the left pane. The policy opens in the right pane.

- Select the group or appliance in the left pane, and then right-click the policy in the right pane and select **Manage Policy** on the pop-up menu.

Note: To ensure that a policy at the group or appliance level overrides a policy at the Site level, right-click the policy, and then select Override. See "Configuring Policy Inheritance" in the SiteProtector Help for more information.

4. Edit the policy as necessary.
5. Click **Save All** on the toolbar to save your changes.

Chapter 6

Configuring Responses

Overview

Introduction

This chapter describes how to configure responses for the appliance. Responses determine how the appliance should react when it detects an intrusion or other important events on the network.

In this chapter

This chapter contains the following topics:

About Responses

Introduction

Your response policy determines how the appliance acts when it detects intrusions or other important events. You create responses and then apply them to events as necessary.

You can configure the following response types:

Important: Quarantine responses are not valid for Proventia Network IDS appliances.

- **Email**. Send email alerts to an individual address or email group.
- **Log Evidence**. Log alert information to a saved file.
- **SNMP**. Send SNMP traps to a consolidated SNMP server.
- **User Specified**. Send alerts based on special requirements you have for monitoring the network.

About the Block response

The Block response is a default response that blocks attacks by dropping packets and sending resets to TCP connections for TCP events only. All other event types are unaffected by the Block response.

About the Ignore response

You can set the Ignore response for security events, which tells the appliance to disregard packets that match criteria specified within an event. You can also set this response through response filters. If you select this response when you create response filters or security events, the appliance does not act when it detects the matching packets.

Basically, you use the Ignore response only to filter security events that do not threaten the network. For more information, see “Configuring Response Filters” on page 62.

About response objects in SiteProtector

If you are managing the appliance through SiteProtector and you want to configure responses for events, you select Response Objects. Response objects are containers that allow you to centralize data so that if the data changes, you can modify the response object instead of each instance of the data.

Note: If you are using SiteProtector to manage the appliance, ISS recommends that you use Central Responses to create event responses. See "Configuring Central Responses" in the SiteProtector Help for more information.

Configuring Email Responses

Introduction

You can configure email notifications to send to individuals or groups whom the appliance should notify when events occur. You can also select the event parameters to include in the message to provide important information about detected events.

Adding email responses

To add or change email responses:

1. Do one of the following:
   - In Proventia Manager, select **Responses**.
   - In SiteProtector, select **Response Objects**.
2. Select the **Email** tab.
3. Click **Add**.
4. Complete the settings as indicated in the following table.

Setting	Description
Name	Type a meaningful name for the response. **Tip**: This name appears when you select responses for events, so you should give the response a name that allows users to easily identify what they are selecting.
SMTP Host	Type the fully qualified domain name or IP address of the mail server. **Note**: The SMTP Host must be accessible to the appliance to send email notifications.
From	Type an individual or group email address. Separate individual email addresses with semicolons.
To	Type an individual or group email address. Separate individual email addresses with semicolons.
Sensor Parameters	Type a **Subject** and **Body** for the message. You can also expand the list and select parameters to add to the message. The appliance populates valid parameters for the event; any invalid parameters retain the original tag format, such as <ObjectName>.

5. Click **OK**.
6. Save your changes.

Working with email responses

To edit, copy, or remove email responses:

1. Do one of the following:
   - In Proventia Manager, select **Responses**.
   - In SiteProtector, select **Response Objects**.
2. Select the **Email** tab, and then do one of the following:

If you want to...	Then...
Edit	**Tip**: You can edit some properties directly on the Email tab by double-clicking the item you want to configure. 1. Select the response, and then click the **Edit** icon. 2. Select or clear the **Enabled** check box. 3. Edit the response, and then click **OK**.
Copy	1. Select the response, and then click the **Copy** icon. 2. Click the **Paste** icon. 3. Edit the response as needed, and then click **OK**.
Remove	1. Select the response. 2. Click the **Remove** icon.

3. Save your changes.

Configuring the Log Evidence Response

Introduction

You can configure the appliance to log the summary of an event. The Log Evidence response creates a copy of the packet that triggers an event and also records information that identifies the packet, such as Event Name, Event Date and Time, and Event ID. Evidence logs show you what an intruder did or tried to do to the network.

The appliance logs packets that trigger events to the /var/iss/ directory.

Configuring the log evidence response

To configure the log evidence response:

1. Do one of the following:
   - In Proventia Manager, select **Responses**.
   - In SiteProtector, select **Response Objects**.
2. Select the **Log Evidence** tab.
3. Complete or change the following settings as indicated in the following table.

Setting	Description
Maximum Files	Type the maximum number of files that can be stored in the log. The default is 10 files. When the log reaches the maximum file number, it begins again with zero (0) and overwrites the existing files.
Maximum File Size (in KB)	Type the maximum file size that can be stored in the log. The default is 10000 KB.
Log File Prefix	Type the log file name prefix. The default is "evidence."
Log File Suffix	Type the log filename extension. The default is ".enc"

4. Save your changes.

Configuring SNMP Responses

Introduction

You can configure Simple Network Management Protocol (SNMP) notification responses for Connection, Security, and User Defined Events that pull certain values and send them to an SNMP manager.

How SNMP works

Simple Network Management Protocol (SNMP) is a set of protocols used for managing networks. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to SNMP management applications, such as HP OpenView. SNMP agents only communicate with SNMP management applications located in the same community. A community is set by the user for basic authentication purposes.

About the ISS MIB file

To display the ISS-assigned Event Name in SNMP trap messages, you can import or compile the ISS MIB file (`iss.mib`) into an SNMP management application such as HP OpenView. The ISS MIB file defines the format of ISS SNMP traps, and is used by your management application to provide translations of the numeric Object Identifiers (OIDs) contained in the trap messages. You can download the iss.mib file from the ISS Download Center at http://www.iss.net/download/. For more information about using the SNMP management application, see the SNMP management application software documentation.

Adding SNMP responses

To add SNMP responses:

1. Do one of the following:
   - In Proventia Manager, select **Responses**.
   - In SiteProtector, select **Response Objects**.
2. Select the **SNMP** tab.
3. Click **Add**.
4. Complete the settings as indicated in the following table.

Setting	Description
Name	Type a meaningful name for the response. **Tip**: This is the name that appears when you select responses for events, so you should give the response a name that allows users to easily identify what they are selecting.
Manager	Type the server IP address where the SNMP Manager is running. The SNMP Host must be accessible to the appliance to send SNMP traps.
Community	Type a valid name (public or private) used to authenticate with the SNMP agent.

5. Click **OK**.
6. Save your changes.

Working with SNMP responses

To edit, copy, or remove SNMP responses:

1. Do one of the following:
   - In Proventia Manager, select **Responses**.
   - In SiteProtector, select **Response Objects**.
2. Select the **SNMP** tab.
3. Do one of the following:

If you want to...	Then...
Edit	**Tip**: You can edit some properties directly on the SNMP tab by double-clicking the item you want to configure. 1. Select the response, and then click the **Edit** icon. 2. Select or clear the **Enabled** check box. 3. Edit the response, and then click **OK**.
Copy	1. Select the response, and then click the **Copy** icon. 2. Click the **Paste** icon. 3. Edit the response as needed, and then click **OK**.
Remove	1. Select the response. 2. Click the **Remove** icon.

4. Save your changes.

Configuring User Specified Responses

Introduction

You can configure user-specified responses to events, such as executing an application or script.

Using executables or shell scripts

For user-specified responses, you can use a Linux binary or shell script file in an executable, including any command-line options or arguments (such as event name or source address).

After you create the response, you must manually copy the executable to the appliance. You can define as many different user-specified responses as needed, but the appliance can only execute one response for a specific event. To run a series of executables, you must place all commands in a shell script that the appliance can run.

Adding user specified responses

To add user specified responses:

1. Do one of the following:
   - In Proventia Manager, select **Responses**.
   - In SiteProtector, select **Response Objects**.
2. Select the **User Specified** tab.
3. Click **Add**.
4. Complete the settings as indicated in the following table.

Setting	Description
Name	Type a meaningful name for the response. **Tip**: This is the name that appears when you select responses for events, so you should give the response a name that allows users to easily identify what they are selecting.
Command	Type a command associated with the response.
Sensor Parameters	Expand the list, select a parameter, and then click **Add**. Repeat this step for each parameter you want to add to the response. You can click **Move Up** or **Move Down** to place the parameters in the appropriate order.

5. Click **OK**.
6. Save your changes.

Working with user specified responses

To edit, copy, or remove user specified responses:

1. Do one of the following:
   - In Proventia Manager, select **Responses**.
   - In SiteProtector, select **Response Objects**.
2. Select the **User Specified** tab.

3. Do one of the following:

If you want to...	Then...
Edit	**Tip**: You can edit some properties directly on the User Specified tab by double-clicking the item you want to configure. 1. Select the response, and then click the **Edit** icon. 2. Select or clear the **Enabled** check box. 3. Edit the response, and then click **OK**.
Copy	1. Select the response, and then click the **Copy** icon. 2. Click the **Paste** icon. 3. Edit the response as needed, and then click **OK**.
Remove	1. Select the response. 2. Click the **Remove** icon.

4. Save your changes.

Chapter 7

Working with Security Events

Overview

Introduction

This chapter describes how to configure security events and response filters. These help you create a security policy that determines how the appliance responds to and reports security events that occur on the network.

In this chapter

This chapter contains the following topics:

Configuring Protection Domains

Introduction

Protection domains let you define security policies for different network segments monitored by a single appliance. Protection domains act like virtual sensors, as though you had several appliances monitoring the network. They work exclusively in conjunction with security events, to help you protect the network. You can define protection domains by ports, VLANs, or IP address ranges.

When to use

You use protection domains when you want to monitor groups of different network segments from a single appliance using global policies that centralize intrusion detection.

Use protection domains as follows:

- to define and apply multiple protection domains to a single appliance
- to apply multiple policies to a single appliance, which lets you tune the responses to specific network traffic on one or more networks

Protection domains and security events

The appliance always uses a global security policy. This means that the appliance handles security events in the same manner for all areas of the network. The appliance always uses this single global policy to handle security events, unless you define protection domains and edit security event policies to suit each domain.

Once you have configured protection domains, you use them in conjunction with security policies that handle security events occurring on the network.

You can create specific security policies for specific protection domains, or you can tweak the global policy for specific domains as you see fit. These policies tell the appliance what properties signal an event and how to respond if the event occurs.

Note: Certain Flood and Sweep signatures are not supported with user-defined Protection Domains. These attacks generally affect multiple targets, which are potentially spread across Protection Domains. You should enable these signatures for the Global Protection Domain so they are reported correctly.

Adding protection domains

To add or change protection domains:

1. On the **Protection Domains** page, click **Add**.
2. Complete or change the settings as indicated in the following table.

Setting	Description
Enabled	Select this check box to enable the protection domain.
Protection Domain Name	Type a descriptive name for the domain.
Comment	Type a unique description for the domain.
Adapter	Select an appliance monitoring adapter or a list of monitoring adapters. **Note**: The appliance ignores port configurations that do not apply to the specific appliance. For example, the appliance may only allow you to configure two adapter ports, even though there are additional ports available for configuration.

Setting	Description
VLAN Range	Type the range of virtual LAN tags.
IP Address Range	Type the range of source and destination IP addresses.

3. Click **OK**.
4. Save your changes.

Working with protection domains

To edit, copy, or remove protection domains:

1. Select **Protection Domains**.
2. Do one of the following:

If you want to...	Then...
Edit	**Tip**: You can edit some properties directly on the Protection Domains page by double-clicking the item you want to configure. 1. Select the domain, and then click the **Edit** icon. 2. Select or clear the **Enabled** check box. 3. Edit the domain, and then click **OK**.
Copy	1. Select the domain, and then click the **Copy** icon. 2. Click the **Paste** icon. 3. Edit the domain as needed, and then click **OK**.
Remove	1. Select the domain. 2. Click the **Remove** icon.

3. Save your changes.

Configuring Security Events

Introduction

The Security Events page lists hundreds of attacks and security events. A security event is 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 events in the active security policy, which you can edit to meet the network's needs.

About the global protection domain

All security events are listed under the Global Protection Domain. The appliance always uses a global security policy, which means it handles security events in the same manner for all areas of your network. Configure events at the global level that you want to apply across all segments in your network. Global policy settings apply to any event the appliance detects; however, if an event is enabled for both a protection domain and the global policy, and the event occurs in the protection domain, the appliance uses the protection domain's policy, not the global policy.

Adding security events

To add security events:

Note: The settings that appear in this procedure correspond to the columns that appear on the Security Events tab.

1. Select **Security Events**.
2. On the **Security Events** tab, click **Add**.
3. Complete or change the settings as indicated in the following table.

Setting	Description
Enabled	Select the check box to enable the event as part of the security policy.
Protection Domain	If you have protection domains configured, select one from the list. You can only apply one event to one domain at a time; to configure this event for another domain, you will have to copy and rename the event, and then assign it to the other domain. **Note**: The protection domain will appear as "Global" in the list if you have not configured (or are not using) protection domains.
Attack/Audit	If you are creating a custom event, this area is unavailable. If you are editing an event in the list, this area displays whether this is an audit or attack event. • Audit events match network traffic that seeks information about the network. • Attack events match network traffic that seeks to harm the network.
Tag Name	Type a unique descriptive name for the event. If you are editing an existing event, the event name appears. Click **Signature Information** to view a brief description of the event.
Severity	Select a severity level for the event: Low, Medium, or High.
Protocol	Type the protocol for the event. For existing events, this setting displays the protocol type and is read-only.
Ignore Events	Select this check box to have the appliance ignore events that match the criteria set for this event.

Setting	Description
Display	Select how you want to display the event in the management console: • **No Display**. Does not display the detected event. • **WithoutRaw**. Logs a summary of the event. • **WithRaw**. Logs a summary and the associated packet capture.
Block	Select this check box to send resets to TCP connections for TCP events only. All other events are unaffected by this option.
Log Evidence	Select this check box to log the packet that triggered the event to the /var/iss/ directory.
Responses	To enable responses, select one of the following tabs: • **Email**. Select an email response from the list. • **SNMP**. Select an SNMP response from the list. • **User Defined**. Select one or more check boxes to enable user-defined responses. **Note**: You can click **Edit** to change the properties of any response in the list. Fore more information, see “Configuring Responses” on page 43.
XPU	For existing events only, displays the XPU in which the vulnerability check was released. This setting is read-only.
Event Throttling	Type an interval value in seconds. At most, one event that matches an attack is reported during the interval you specify. The default value is 0 (zero), which disables event throttling.
Check Date	For existing events only, displays the month and the year the vulnerability check was created. This setting is read-only.
User Overridden	If you are creating a new event, this check box is enabled by default to indicate a custom event. In the list on the Security Events tab, this item appears as checked for both custom events and existing events that you have edited. This setting is read-only.

4. Click **OK**.
5. Save your changes.

Working with security events

To edit, copy, or remove security events:

1. Select **Security Events**.
2. Select the **Security Events** tab, and then do one of the following:

If you want to...	Then...
Edit	**Tip**: You can edit some properties directly on the Security Events tab by double-clicking the item you want to configure. 1. Select the event, and then click the **Edit** icon. 2. Select or clear the **Enabled** check box. 3. Edit the event, and then click **OK**.
Copy	**Tip**: Copying and pasting security events is much easier if you group and filter the events first. See "Grouping security events" on page 60 or "Filtering security events" on page 61 for more information. 1. Select the event, and then click the **Copy** icon. 2. Click the **Paste** icon. 3. Edit the event as needed, and then click **OK**.
Remove	1. Select the event. 2. Click the **Remove** icon. **Important**: You can only remove custom events. If you select a predefined event that you have edited and click Remove, the event is reset to its default settings and remains in the list.

3. Save your changes.

Editing multiple security events

To edit multiple security events:

1. Select **Security Events**.
2. On the **Security Events** tab, do one of the following:
   - To select multiple events, press [CTRL], and then select each event.
   - To select a range of events, press [SHIFT], and then select the first and last events in the range.
3. Click **Edit**.

   Every item you edit is changed for every selected event.

   A blue triangle icon appears next to any item in the selected events that has a different value. If you change the value of a field with this icon, the value changes to the new setting for all selected events, and the blue triangle icon no longer appears next to the field.

   For example, if you select to edit two events and one has blocking enabled and the other does not, a blue triangle appears next to Block. If you enable the block response for the event where it was originally disabled, then both events have blocking enabled, and the blue triangle disappears.
4. Click **OK**.
5. Save your changes.

Assigning a Protection Domain to Multiple Security Events

Introduction

After you have configured the protection domains, you can assign them to multiple security events. The saves you time when you are configuring the security policy for each protection domain on the network.

Procedure

To assign a protection domain to multiple security events:

1. Select **Security Events**.
2. On the **Security Events** tab, select the events as follows:
   - To select multiple events, press the CTRL key, and then select each event.
   - To select a range of events, press the SHIFT key, and then select the first and last events in the range.
3. Click **Copy**.
4. Click **Paste**.
5. Select all entries with the red X icon, and then click **Edit**.
6. Select the **Protection Domain** that you want to assign to the selected events.
7. Edit any additional settings.

   For more information, see "Adding security events" on page 56.
8. Click **OK** to return to the Security Events page.
9. Save your changes.

Viewing Security Event Information

Introduction

The Security Events tab lists hundreds of attacks and security events. You can customize how events appear to make viewing and searching easier.

About filters and regular expressions

Security events filters use regular expressions to limit the number of events returned.

Regular expressions (also known as regex) are sets of symbols and syntax that you use to search for text that matches the patterns you specify. If you have ever performed a wildcard search, you have used regular expressions.

At the most basic level, the following wildcard search types are supported:

- *. Returns all events.
- *word*. **Example**: *http* includes all HTTP events.
- word*. **Example**: http* includes all event names beginning with HTTP.
- *word. **Example**: *http includes all event names ending with HTTP.

Selecting columns to display

To select columns to display:

1. Select **Security Events**.
2. On the **Security Events** tab, click **Select Columns**.
3. Select the check box next to the columns that you want to appear.
4. Click **OK**.
5. Save your changes.

Note: If you have grouped and sub-grouped events, the columns for those events no longer appear in the Security Events tab. Instead, they appear as items in a grouping tree that you can expand or collapse.

Grouping security events

To group security events:

1. Select **Security Events**.
2. On the **Security Events** tab, click **Group By**.
3. From the All Columns list, select the column by which you want to group events, and then click **Add**.

   The columns you select appear in the Group By These Columns list.
4. Repeat **Step 3** for each column by which you want to group events.

   Each column you select to group by creates a subgroup underneath the last "group" you created.
5. Click **OK**.
6. Collapse or expand the groups on the Security Events tab to view events.
7. Save your changes.

Filtering security events

To filter security events:

1. Select **Security Events**.
2. On the **Security Events** tab, select the **Filter** check box to enable filtering.
3. Click **Filter**.
4. In the **Regular Expressions** area, type the regular expression by which you want to filter. This search feature is not case-sensitive.

   Note: To use this feature, you should be familiar with how regular expressions work.
5. For each category, select the filters you want to apply. The default is *Any*, which results in the appliance searching for any result that matches the regular expression you entered.
6. Click **OK**.
7. Save your changes.

Resetting security event values

To reset security event values:

1. Select **Security Events**.
2. On the **Security Events** tab, do one of the following:
   - Reset Events. Highlight the events to reset, and then click **Remove**. Pre-defined events that you edited are restored to default values but remain in the list. Custom events are removed from the list.
   - Reset Groups. Click **Reset Groupings**. All grouping is removed from the events.
   - Reset Filters. Clear the **Filters** check box to disable any filters you have set.
3. Save your changes.

Configuring Response Filters

Introduction

Response filters help you refine the security policy by controlling the number of events to which the appliance responds and the number of events reported to the management console. You can also define exceptions to the current policy for particular protection domains, so each policy is fine-tuned for the network segment it monitors.

You use response filters to do the following:

- configure responses for security events that trigger based off network criteria specified in the filter
- reduce the number of security events an appliance reports to the console

For example, if you need to temporarily monitor additional events on a certain segment of the protection domain, you can add the events to monitor through a response filter, rather than editing the security policy itself or creating a new security policy just for that network segment.

Attributes of event filters

Response filters have the following configurable attributes:

- adapter
- virtual LAN (VLAN)
- source or target IP address
- source or target port number (all ports or a port associated with a particular service) or ICMP type/code (one or the other will be used)

Filters and other events

When the appliance detects traffic that matches a response filter, the appliance executes the responses specified in the filter. Otherwise, the appliance executes the security event as specified in the event itself.

Note: If a security event is disabled, its corresponding response filters are also disabled.

Response filter order

The response filters follow rule ordering. For example, if you add more than one filter for the same security event, the appliance executes the responses for the first match. The appliance reads the list of filters from top to bottom.

Adding response filters

To add response filters:

Note: The settings that appear in this procedure correspond to the columns that appear on the Response Filters tab.

1. Select **Security Events**.
2. Select the **Response Filters** tab.
3. Click **Add**.

4. Complete or change the settings as indicated in the following table.

Setting	Description
Enabled	The filter is enabled by default. To disable the filter, clear the check box.
Protection Domain	Select the protection domain for which you want to set this filter. **Note**: For a response filter to be active, the corresponding security event must be enabled for the protection domain you specify here.
Event Name	Displays a truncated event name. Click the button to add events. **Tip**: You can add multiple events at one time. Use the filter settings to sort through the list.
Event Name Info	Displays additional information about the event, if necessary. This setting is read-only.
Comment	Type a unique description for the event filter.
Severity	Select an event severity level to filter by: high, medium, or low.
Adapter	Select the appliance port(s) on which the response filter will be applied. **Note**: The appliance ignores port configurations that do not apply to the specific appliance. For example, the appliance may only allow you to configure two adapter ports, even though there are additional ports available for configuration.
VLAN	Type the range of virtual LAN tags where the response filter will be applied.
Event Throttling	Type an interval value in seconds. At most, one event that matches an attack will be reported during the interval you specify. The default value is 0 (zero), which disables event throttling.
Ignore Events	Select this check box to have the appliance ignore events that match the criteria set for this event.
Display	Select how to display the event in the management console: • **No Display**. Does not display the detected event. • **WithoutRaw**. Logs a summary of the event. • **WithRaw**. Logs a summary and the associated packet capture.
Block	Select this check box to send resets to TCP connections for TCP events only. All other events are unaffected by this option.
ICMP Type/Code	Type ICMP types or codes for either side of the packet, or click **Well Known** to select often-used types and codes.
Log Evidence	Select this check box to log the packet that triggered the event to the /var/iss/ directory.

Setting	Description
Responses	To enable responses, select one of the following tabs: • **Email**. Select an email response from the list. • **SNMP**. Select an SNMP response from the list. • **User Defined**. Select one or more check boxes to enable user-defined responses. **Note**: Click **Edit** to change the properties of any response in the list. For more information, see "Configuring Responses" on page 43.
IP Address and Port	For the Source and/or Target IP addresses or ports you want to filter by, complete or change the following settings as listed in Step 5.

5. Complete the following IP Address and Port settings as indicated in the following table.

Setting		Description
Address	Not	Select this check box to exclude addresses you specify.
	Any	Select this option to include all addresses.
	Single Address	Select this option to filter on one address, and then type the **Address**.
	Address Range	Select this option to filter on an address range, and then type the first and last addresses in the **Range**. **Note**: Do not use 0.0.0.0-255.255.255.255 as the Site range. If you use this as the Site range, random IP addresses are added to the ungrouped assets folder, such as IP addresses from Web sites, et cetera.
	Network Address/# Network Bit (CIDR)	Select this option to include an IP address on a subnet. Type the IP address and mask. The mask is the network identifier, and is a number from 1 to 32; for example: 128.8.27.18 / 16.
Port	Not	Select this check box to exclude ports you specify.
	Any	Select this option to include all addresses.
	Single Port	Select this option to include a single port, and then type the **Port** number.
	Port Range	Select this option to include a port range, and then type the first and last address in the **Range**.

6. Click **OK**.
7. Save your changes.

Changing the order of response filters

To change the order of response filters:

1. Select **Security Events**.
2. Select the **Response Filters** tab.
3. Select an entry, and then click the **Up** or **Down** icons to move the filter.
4. Save your changes.

Working with response filters

To edit, copy, or remove response filters:

1. Select **Security Events**.
2. Select the **Response Filters** tab, and then do one of the following:

If you want to...	Then...
Edit	**Tip**: You can edit some properties directly on the Response Filters tab by double-clicking the item you want to configure. 1. Select the filter, and then click the **Edit** icon. 2. Select or clear the **Enabled** check box. 3. Edit the filter, and then click **OK**.
Copy	1. Select the filter(s), and then click the **Copy** icon. 2. Click the **Paste** icon. 3. Edit the filter as needed, and then click **OK**.
Remove	1. Select the filter(s). 2. Click the **Remove** icon.

3. Save your changes.

Viewing Response Filter Information

Introduction

The Response Filters tab lists response filters you have defined.

Selecting columns to display

To select columns to display:

1. Select **Security Events**.
2. Select the **Response Filters** tab.
3. Click **Select Columns**.
4. Select the check box next to the columns that you want to appear on the tab.
5. Click **OK**.
6. Save your changes.

Note: If you have grouped and sub-grouped filters, the columns for those events no longer appear in the Response Filters tab. Instead, they appear as items in a grouping tree that you can expand or collapse.

Grouping response filters

To group response filters:

1. Select **Security Events**.
2. Select the **Response Filter**s tab.
3. Click **Group By**.
4. From the **All Columns** list, select the column by which you want to group filters, and then click **Add**.

   The columns you select appear in the Group By These Columns list.
5. Repeat Step 4 for each column by which you want to group filters.

   Each column you select to group by creates a subgroup underneath the last "group" you created.
6. Click **OK**.
7. Collapse or expand the groups on the Response Filters tab to view filters.
8. Save your changes.

Filtering response filters

To filter response filters:

1. Select **Security Events**.
2. Select the **Response Filter**s tab.
3. Select the **Filter** check box to enable filtering.
4. Click **Filter**.

   For each category, select the filters you want to apply. The default is Any, which results in the appliance searching for any result for that category.
5. Click **OK**.
6. Save your changes.

Chapter 8

Configuring Other Intrusion Detection Settings

Overview

Introduction

This chapter describes how to configure and manage other intrusion detection settings, such as user-defined events and connection events. It also discusses how to view global tuning parameters for the appliance and monitor X-Force blocking.

In this chapter

This chapter contains the following topics:

Configuring Connection Events

Introduction

Connection events are user-defined notifications of open connections to or from particular addresses or ports. They are generated when the appliance detects network activity at a designated port, regardless of the type of activity or network packets, or the content of network packets exchanged.

The Connection Events page lists pre-defined connection events for different connection types, such as WWW, FTP, or IRC. Use this page to customize these events or to create your own events to cover the traffic you need to monitor.

For example, you can define a signature that causes a connection event to alert the console whenever someone connects to the network using FTP.

Note: The connections are always registered against the destination port you specify, so to monitor an FTP connection, you must use the FTP port. One entry per connection is sufficient for traffic in each direction.

How connection events work

Connection events occur when network traffic connects to the monitored network through a particular port, from a particular address, with a certain network protocol. The appliance detects these connections using packet header values. Connection events do not necessarily constitute an attack or other suspicious activity, but they are network occurrences that might interest a Security Administrator.

Note: Connection events do not monitor the network for any particular attack signatures. You use security events to monitor for these types of attacks. See "Configuring Security Events" on page 56 for more information.

About removing connection events

You can remove any connection event from the list. However, if you edited a pre-defined connection event and now decide you want to remove it, be aware that the event is not returned to its pre-defined state. The event is removed from the list entirely. If you want to use this event again in the future, it will no longer be available.

Consider disabling the event and keeping it in the list. This way, if you want to use it again at another time, the event is still available to you in some form.

Adding connection events

To add connection events:

Note: The settings in this procedure correspond to the columns that appear on the Connection Events page.

1. On the **Connection Events** page, click **Add**.
2. Complete the settings as indicated in the following table.

Setting	Description
Enabled	The event is enabled by default. If necessary, clear the check box to disable the event.
Event Name	Type a unique descriptive name for the event. If you are editing a pre-defined event, the name appears here as read-only.

Setting	Description
Comment	Type a unique description for the event.
Severity	Select a severity level for the event: Low, Medium, or High.
Event Throttling	Type an interval value in seconds. At most, one event that matches an attack is reported during the interval you specify. The default value is 0 (zero), which disables event throttling.
Protocol	Type the protocol for the event. If you select the ICMP protocol, type the ICMP types or codes for either side of the packet, or click **Well Known** to select often-used types and codes.
Display	Select how you want to display the event in the management console: • **No Display**. Does not display the detected event. • **WithoutRaw**. Logs a summary of the event. • **WithRaw**. Logs a summary and the associated packet capture.
Block	Select this check box to send resets to TCP connections for TCP events only. All other events are unaffected by this option.
Log Evidence	Select this check box to log the packet that triggered the event to the /var/iss/ directory.
IP Address and Port	See Step 4.
Responses	See Step 5.

3. As needed, complete the following **IP Address and Port** settings as indicated in the following table.

Setting		Description
Address	Not	Select this check box to exclude addresses you specify.
	Any	Select this option to include all addresses.
	Single Address	Select this option to filter on one address, and then type the **Address**.
	Address Range	Select this option to filter on an address range, and then type the first and last addresses in the **Range**. **Note**: Do not use 0.0.0.0-255.255.255.255 as the Site range. If you use this as the Site range, random IP addresses are added to the ungrouped assets folder, such as IP addresses from Web sites, et cetera.
	Network Address/# Network Bit (CIDR)	Select this option to include an IP address on a subnet. Type the IP address and mask. The mask is the network identifier, and is a number from 1 to 32; for example: 128.8.27.18 / 16.

Setting		Description
Port	Not	Select this check box to exclude ports you specify.
	Any	Select this option to include all addresses.
	Single Port	Select this option to include a single port, and then type the **Port** number.
	Port Range	Select this option to include a port range, and then type the first and last address in the **Range**.

4. As needed, complete the following Response settings as indicated in the following table. Click **Edit** to change the properties of a response in the list. For more information, see "Configuring Responses" on page 43.

Response	Description
Email	Select an email response from the list.
SNMP	Select an SNMP response from the list.
User Defined	Select one or more check boxes to enable user-defined responses.

5. Click **OK**.
6. Save your changes.

Filtering connection events

To filter connection events:

1. On the **Connection Events** page, select the **Filter** check box to enable filtering.
2. Click **Filter**.
3. For each category, select the filters you want to apply.

   By default, all filters are set to *Any*, which results in the appliance searching for any result for that category.
4. Click **OK**.
5. Save your changes.

Working with connection events

To edit, copy, or remove connection events:

1. On the **Connection Events** page, do one of the following:

If you want to...	Then...
Edit	**Tip**: You can edit some properties directly on the Connection Events page by double-clicking the item you want to configure. 1. Select the event, and then click the **Edit** icon. 2. Select or clear the **Enabled** check box. 3. Edit the event, and then click **OK**.
Copy	1. Select the event, and then click the **Copy** icon. 2. Click the **Paste** icon. 3. Edit the event as needed, and then click **OK**.
Remove	1. Select the event. 2. Click the **Remove** icon. See “About removing connection events” on page 68 for more information.

2. Save your changes.

Configuring User-Defined Events

Introduction

Enabled events in a policy determine what an appliance detects. You create user-defined events around contexts, which basically specify the type and part of a network packet you want the appliance to scan for events.

About the global protection domain

Notice that all events are listed under the global protection domain. The appliance always uses a global policy, which means that it handles events in the same manner for all areas of your network. You should configure events at the global level that you want to apply across all segments in your network. If you want to configure user-defined event policies for specific segments on your network, you should create protection domains for each segment.

Note the following:

- If you have two user-defined events with the same name, one assigned to the global protection domain and one assigned to a custom protection domain, and the event is triggered on the appliance, only the event assigned to the custom domain generates an alert. In this case, the custom domain always takes precedence over the global domain.
- If you have two user-defined events that are the same but have different names, when one event is triggered, each events generates its own alert. In this case, neither event takes precedence.

Important: The appliance considers two events with the same name the same event, even if their context or query strings differ.

For information about creating protection domains, see “Configuring Protection Domains” on page 54.

Adding user-defined events

To add user-defined events:

Note: The settings listed in this procedure correspond to the columns that appear on the User Defined Events page.

1. On the **User Defined Events** page, click **Add**.
2. Complete the settings as indicated in the following table.

Setting	Description
Enabled	The event is enabled by default. To disable it, clear the check box.
Name	Type a unique name for the event.
Protection Domain	If you have protection domains configured, select one from the list. You can only apply one event to one domain at a time; to configure this event for another domain, copy and rename the event, and then assign it to the other domain. **Note**: The protection domain appears as "Global" in the list if you have not configured (or are not using) protection domains.
Comment	Type a unique description for the event.
Severity	Select an event severity level to filter by: high, medium, or low.

Setting	Description
Context	Select the type and part of the network packet that the appliance should scan. For more information, see “User-Defined Event Contexts” on page 75.
Search String	Type the text string in the packet (context) that determines whether an event matches this signature. You can use wildcards and other expressions in strings. For more information, see “Regular Expressions in User-Defined Events” on page 80.
Event Throttling	Type an interval value in seconds. At most, one event that matches an attack is reported during the interval you specify. The default value is 0 (zero), which disables event throttling.
Display	Select how to display the event in the management console: • **No Display**. Does not display the detected event. • **WithoutRaw**. Logs a summary of the event. • **WithRaw**. Logs a summary and the associated packet capture.
Block	Select this check box to send resets to TCP connections for TCP events only. All other events are unaffected by this option.
Log Evidence	Select this check box to log the packet that triggered the event to the /var/iss/ directory.
Responses	To enable responses, select one of the following tabs: • **Email**. Select an email response from the list. • **SNMP**. Select an SNMP response from the list. • **User Defined**. Select one or more check boxes to enable user-defined responses. **Note**: Click **Edit** to change the properties of any response in the list. For more information, see “Configuring Responses” on page 43.

3. Click **OK**.

   The event appears at the bottom of the list.

4. Save your changes.

Working with user-defined events

To edit, copy, or remove user-defined events:

1. On the **User Defined Events** page, do one of the following:

If you want to...	Then...
Edit	**Tip**: You can edit some properties directly on the User Defined Events page by double-clicking the item you want to configure. 1. Select the event, and then click the **Edit** icon. 2. Select or clear the **Enabled** check box. 3. Edit the event, and then click **OK**.
Copy	1. Select the event, and then click the **Copy** icon. 2. Click the **Paste** icon. 3. Edit the event as needed, and then click **OK**.
Remove	1. Select the event. 2. Click the **Remove** icon.

2. Save your changes.

User-Defined Event Contexts

Introduction

When you create a user-defined event signature, you select a context that tells the appliance the type and particular part of a network packet to monitor for events. After you specify the context, you add a string that tells the appliance exactly what to look for when it scans the packet. See "Regular Expressions in User-Defined Events" on page 80 for more information.

For example, the email_subject context configures the appliance to monitor the subject line of email packets (messages).

DNS_Query 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.

- **Monitors**

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

  If a user accesses a site directly using an IP address, the DNS lookup does not occur, and the appliance cannot detect the event.

  To monitor for a particular URL, remember that the domain name is only the first element. For example, //www.cnn.com is the first element in http://www.cnn.com/stories. Use the URL_Data context (see "URL_Data context" on page 78) to detect the rest of the URL.

- **Examples**

  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

Email_Receiver context

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

- **Monitors**

  The Email_Receiver context monitors the receiver address part of the email header using the SMTP, POP, IMAP protocols. When the appliance 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.

  Note: This context does not monitor email sent with the MAPI protocol.

- **Examples**

  If you suspect that someone is using "social engineering" to manipulate certain employees, you can monitor inbound email to those employees' addresses and log the source IPs. Or if you suspect someone is leaking proprietary information within your company to a particular outside email address, you could track email to that address.

Email_Sender context

Use the Email_Sender context to monitor incoming or outgoing email from a particular recipient.

- **Monitors**

  The Email_Sender context monitors the sender address part of the email header using the SMTP, POP, IMAP protocols. When the appliance detects an event that matches a signature using the Email_Sender context, you can examine the details of the event to determine which protocol the email used.

  Note: This context does not monitor email sent with the MAPI protocol.

- **Examples**

  Use the Email_Sender context to detect instances of social engineering or other employee manipulation (inbound) or to detect information leaks from your company (outbound).

Email_Subject context

Use the Email_Subject context to monitor the subject line of email.

- **Monitors**

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

  Note: This context does not monitor email sent with the MAPI protocol.

- **Examples**

  You can create signatures to detect information leaks by monitoring for important project names or file names.

  You can also use Email_Subject to detect viruses, such as the ILOVEYOU virus.

  Tip: Because viruses and other attacks have developed programs that systematically change the subject line, use the Email_Content context to track these virus types.

File_Name context

Use the File_Name context to monitor who accesses sensitive files over the network in your organization.

- **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

  Note: NFS can open files without directly referencing the file name. Using this context to monitor NFS access to a file may not be 100% effective.

- **Example**

  When the Explorer worm of 1999 propagated over a Windows network, it attempted to write to certain files on remote Windows shares. With a worm like this, you can monitor for attempts to access files and stop the worm from propagating locally.

News_Group context

Use the News_Group context to monitor the names of news groups that people at your company access.

- **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

Use the Password context to identify passwords passed in clear text over the network. When a password is not encrypted, an attacker can easily steal it by monitoring traffic with a sniffer program from another site.

- **Monitors**

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

  You can also use the Password context to do the following:

  - monitor compromised accounts to gain forensic data
  - monitor the accounts of terminated employees
  - detect the use of default passwords

  Note: This context does not monitor encrypted passwords.

- **Examples**

  Monitoring compromised accounts: After cancelling a compromised account, you can create a signature to monitor outside attempts to use it and find the person that accessed the compromised data.

  Monitoring terminated employee accounts: Add searches for terminated employees' passwords to detect unauthorized remote access attempts to their closed accounts.

  Detecting the use of default passwords: Set up signatures to look for default passwords relevant to your site to detect attackers probing for common vulnerabilities.

  Note: The X-Force database contains many records detailing the names of such accounts. For more information about default passwords, look up passwords in the X-Force database at http://xforce.iss.net.

- **Using this signature with Internet Scanner**

  If you scan the network using 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.

SNMP_Community context

Use the SNMP_Community context to monitor the use and possible abuse of SMNP community strings.

- **Monitors**

  The SNMP_Community context monitors any packet containing an SNMP community string. 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.

  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 to reconfigure your equipment.

  Important: ISS strongly recommends that you use highly unique community strings and that you reconfigure them periodically.

- **Examples**

  Detecting people trying to use old strings: If you change the SNMP community strings, create a signature using this context to have the appliance search for people trying to use the old strings.

  Detecting the use of default strings: The X-Force database contains information about several vulnerabilities involving default community strings on common equipment. Attackers can attempt to access to your equipment by using these default passwords. To have the appliance detect this activity, create signatures using this context to monitor for the default passwords relevant to the equipment at your site. These signatures can detect attackers attempting to probe for these common vulnerabilities.

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

- **Using this signature with Internet Scanner**

  If you scan your network using 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.

URL_Data context

Use the URL_Data context to monitor various security issues or policy issues related to HTTP GET requests. An HTTP GET request occurs when a client, such as a Web browser, requests a file from a Web server. The HTTP GET request is the most common way to retrieve files on a Web server.

- **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.

  Note: This context does not monitor the domain name associated with an HTTP GET request.

- **Example**

  Use this context to have the appliance monitor for attacks involving vulnerable CGI scripts. 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 whether employees using computers to access company-banned sites, such as pornography sites.

User_Login_Name context

Use the User_Login_Name context to detect user names 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 no matter what protocol the attacker uses.

- **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.

- **Example**

  Use this context to track attempts to use compromised accounts or if you suspect recently dismissed employees have attempted to access their old accounts online. 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.

User_Probe_Name context

Use the User_Probe_Name context to identify attempts to access to computers on your network using default program passwords.

- **Monitors**

  The User_Probe_Name context monitors any user name associated with FINGER, SMTP, VRFY, and SMTP EXPN. An attacker can use these default accounts to access to your servers or other computers in the future.

- **Example**

  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.

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

Regular Expressions in User-Defined Events

Introduction

Regular expressions (strings) are a combination of static text and variables the appliance uses to detect patterns in the contexts (network packets) you specify for user-defined event signatures. Use regular expressions when you create user-defined event signatures if you need the appliance to detect more than a single static text string.

Regular expression library

The appliance uses a custom ISS regular expression library called Deterministic Finite Automata or DFA regular expression.

Changing the order of precedence

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

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.

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 regular expression syntax in a user-defined event signature:

Meta-Character	Description
(r)	matches r
x	matches x
xr	matches x followed by r
\s	matches either a space or a tab (not a newline)
\d	matches a decimal digit
\"	matches a double quote
\'	matches a single quote
\\	matches a backslash
\n	matches a newline (ASCII NL or LF)
\r	matches a carriage return (ASCII CR)
\t	matches a horizontal tab (ASCII HT)
\v	matches a vertical tab (ASCII VT)
\f	matches a formfeed (ASCII FF)
\b	matches a backspace (ASCII BS)
\a	matches a bell (ASCII BS)
\ooo	matches the specified octal character code

Table 24: *String standard expressions*

Meta-Character	Description
\xhhh	matches the specified hexidecimal character code
.	matches any character except newline
\@	matches nothing (represents an accepting position)
“”	matches nothing
[xy-z]	matches x, or anything between y and z inclusive (character class)
[^xy-z]	matches anything but x, or between y and z inclusive • the caret must be the first character, otherwise it is part of the set literally • enter the dash as the first character if you want to include it
“text”	matches text literally without regard for meta-characters within • the text is not treated as a unit
r?	matches r or nothing (optional operator)
r*	matches zero or more occurrences of r (kleene closure)
r+	matches one of more occurrences of r (positive kleene closure)
r{m,n}	matches r at least m times, and at most n times (repeat operator)
r|l	matches either r or l (alternation operator)
r/l	matches r only if followed by l (lookahead operator)
^r	matches r only at the beginning of a line (bol anchor)
r$	matches r only at the end of the line (eol anchor)
r, l	matches any arbitrary regular expression
m, n	matches an integer
x,y,z	matches any printable or escaped ascii character
text	matches a sequence of printable or escaped ascii characters
ooo	matches a sequence of up to three octal digits
hhh	matches a sequence of hex digits

Table 24: *String standard expressions (Continued)*

Viewing User-Defined Event Information

Introduction

The User Defined Events page displays all of the custom event signatures you have created for the appliance. You can control how user-defined events appear in this view, to make managing and searching events easier.

Selecting columns to display

To select columns to display:

1. On the **User Defined Events** page, click **Select Columns**.
2. Select the check box next to the columns that you want to appear.
3. Click **OK**.

   Note: If you have grouped and sub-grouped events, the columns for those events no longer appear in the User-Defined Events page. Instead, they appear as items in a grouping tree that you can expand or collapse.
4. Save your changes.

Grouping user-defined events

To group user-defined events:

1. On the **User Defined Events** page, click **Group By**.
2. From the All Columns list, select the column by which you want to group events, and then click **Add**.

   The columns you select appear in the Group By These Columns list.
3. Repeat Step 3 for each column by which you want to group events.

   Each column you select to group by creates a subgroup underneath the last "group" you created.
4. Click **OK**.
5. Collapse or expand the groups on the User Defined Events tab to view events.
6. Save your changes.

Filtering user-defined events

To filter user-defined events:

1. On the **User Defined Events** page, select the **Filter** check box to enable filtering.
2. Click **Filter**.
3. For each category, select the filters you want to apply.

   The default is *Any*, which results in the appliance searching for any result that matches the regular expression you entered.
4. Click **OK**.
5. Save your changes.

Configuring OpenSignature

Introduction

OpenSignature (formerly Trons) uses a flexible rules language to allow you to write customized, pattern-matching IDS signatures to detect specific threats that are not already preemptively covered in IPS products. This feature is integrated into the ISS Protocol Analysis Module (PAM) as a rule interpreter.

Risks associated with OpenSignature

The capabilities of custom signature development are very broad. With this flexibility comes added risk. Poorly written rules or signatures could impact sensor performance or have other consequences. Risks of using your own custom signatures include but are not limited to the following:

- unacceptable appliance performance
- throwing PAM into an infinite loop (crashing PAM)
- blocking all network traffic to a specific segment (inline mode with or without bypass)
- a required resolution involving reinstalling the appliance's factory image to return to a "good" state

Caution: ISS does not guarantee appliance performance if you choose to use OpenSignature. Enable this functionality at your own risk. ISS Customer Support is not available to help you write or troubleshoot custom rules for your environment. If you require assistance to create custom signatures, please contact ISS Professional Services.

OpenSignature syntax

The syntax options for each custom rule are as follows:

`<action>: alert`

`<protocol>: tcp, udp, icmp, ip`

`<IP and netmask>`: single IP address (a.b.c.d), range of IP addresses (a.b.c.d-w.x.y.z), network address using CIDR notation (a.b.c.0/24)

The Negation operator is indicated with an '!':

```
alert tcp !192.168.1.0/24
```

This means an alert prompts you when anything other than what is indicated with the '!' is used.

Important: If you have improperly formatted an OpenSignature rule, you may receive a PAM configuration error response.

Enabling the OpenSignature Parser

To enable the OpenSignature Parser:

1. Select Global Tuning Parameters.
2. On the Tuning Parameters tab, click **Add**.
3. Complete the settings as indicated in the following table:

Setting	Description
Name	Type the following to enable OpenSignature: `pam.trons.enabled`
Value	Type the following: `true`

4. Save your changes.

Adding or changing rules

To add or change rules:

1. On the **TronsRule** page, click **Add**, or highlight the rule you want to edit, and then click **Edit**.

   Tip: You can edit some properties directly on the TronsRule page by double-clicking the item you want to configure.

2. Complete or change the settings as indicated in the following table.

Setting	Description
Enabled	Select the check box to enable the rule.
Comment	Type a unique description for the rule.
Rule String	Type the text string that tells the appliance when an event is triggered and how to respond to the event.
Event Throttling	Type an interval value in seconds. At most, one event that matches an attack is reported during the interval you specify. The default value is 0 (zero), which disables event throttling.

3. Click **OK**.
4. Save your changes.

Configuring Global Tuning Parameters

Introduction

Global tuning parameters affect intrusion detection settings at the group and site levels.

Use Global Tuning Parameters to configure (or tune) certain parameters and apply them globally to a group of appliances to better meet your security needs or enhance the performance of the hardware. Generally, you edit or configure global tuning parameters for groups of appliances you manage through SiteProtector, but you can view the global tuning parameters that affect a specific appliance through Proventia Manager.

You can also specify whether you want to use blocking responses recommended by ISS X-Force. While ISS recommends that you not disable X-Force blocking as a general rule, you may need to disable this option at times so that you can determine whether current suspicious activity on the network is valid, or so that you can protect against explicit threats to the network.

How global parameters differ from local parameters

Global tuning parameters differ from local tuning parameters as follows:

- Global tuning parameters are intrusion detection settings that affect a group of intrusion detection appliances.
- Local tuning parameters are settings that affect a specific intrusion detection appliance, such as network adapter card settings.

  Because local tuning parameters are specific to a particular appliance, you can configure them only at the device level.

Where applicable, local tuning parameters you have enabled take precedence over global tuning parameters.

Components you can tune

You can tune the following components on a group of appliances:

- intrusion detection responses
- intrusion detection security risks
- packet filters
- automatic updates

See “Configuring Advanced Parameters” on page 100 for information about applying advanced parameters to a single appliance.

About advanced parameters

Advanced parameters are composed of name/value pairs. Each name/value pair has a default value.

For example, the parameter np.packet filter.log is a parameter that determines whether to log the details of packets that match packet filter rules you have enabled. The default value for this parameter is on.

You can edit the value of any parameter that appears in the list on the Advanced Parameters tab. If the parameter does not appear in the list, it does not mean the parameter has no default value. You simply need to add the parameter to the list with the new value.

Adding tuning parameters

To add tuning parameters:

1. Select **Global Tuning Parameters**.
2. On the **Tuning Parameters** tab, click **Add**.
3. Complete the settings as indicated in the following table.

Setting	Description
Name	Type a name for the parameter. **Example**: np.log.count
Value	Type a value according to the value type associated with the parameter: • **Boolean**. Select a value of True or False. • **Number**. Enter the appropriate number for the parameter. **Example**: 10 • **String**. Type the value for the parameter, such a log file location.
Comment	Type a unique description for the parameter. **Example**: Number of event log files.

4. Click **OK**.
5. Save your changes.

Working with global tuning parameters

To edit, copy, or remove global tuning parameters:

1. Select **Global Tuning Parameters**.
2. Select the **Tuning Parameters** tab, and then do one of the following:

If you want to...	Then...
Edit	**Tip**: You can edit some properties directly on the Tuning Parameters tab by double-clicking the item you want to configure. 1. Select the parameter, and then click the **Edit** icon. 2. Select or clear the **Enabled** check box. 3. Edit the parameter, and then click **OK**.
Copy	1. Select the parameter, and then click the **Copy** icon. 2. Click the **Paste** icon. 3. Edit the parameter as needed, and then click **OK**.
Remove	1. Select the parameter. 2. Click the **Remove** icon.

3. Save your changes.

Configuring X-Force Default Blocking

Introduction

When you use X-Force Default Blocking, the block response is enabled automatically for events (or signatures) that X-Force recommends.

Procedure

To configure default blocking:

1. Select **Global Tuning Parameters**.
2. Select the **X-Force Default Blocking** tab.
3. X-Force blocking is enabled by default. To disable it, clear the **Use X-Force blocking recommendations** box.
4. Save your changes.

Chapter 9

Configuring Packet Filters

Overview

Introduction

You can configure packet filters to filter out packets you do not want the appliance to monitor across your network. You specify this information in rule statements.

In this chapter

This chapter contains the following topics:

Configuring Packet Filter Rules

Introduction

You can add packet filter rules to ignore packets as the move across the network. You can manually add these rules, or you can enable the appliance to construct rules using the values you specify. This offers you greater flexibility when configuring packet filter settings.

Packet filter rule criteria

You can define packet filter rules using any combination of the following criteria:

- Adapter
- VLAN range
- Protocol (TCP, UDP, or ICMP)
- Source or target IP address and port ranges

Adding packet filter rules

To add packet filter rules:

5. On the **Packet Filter Settings** page, click **Add**.
6. Complete the settings as indicated in the following table.

Setting	Description
Rule ID	Displays the rule's order in the list.
Enabled	Select this check box to enable the rule.
Rule Comment	Type a unique description for the rule.
Log	Select whether to log details of the packets that match the rule in the Packet Filter log located in the /var/iss/event directory.
Rule Type	Select a rule type from the list: • **Constructed**. Select this option to enable the Proventia Manager to construct the packet filter rule for you using the values you specify. • **Manually Entered**. Select this option to construct your own packet filter rules. Type the **Packet Filter Rule** statement in the area provided. For more information, see “Packet Filter Rules Language” on page 90.
VLAN	Enter a range of VLAN tags.

Setting	Description
Protocol	Select a protocol from the list. If you select *Any* as the protocol for a rule, the following criteria is applied if the following conditions are met: • If you set an ICMP code, then an ICMP clause is added to the rule. • If you set a source or destination port, then both a UDP and a TCP clause are added to the rule. • If you set a Protocol Number greater than zero (0), then a protocol number clause is added to the rule. • If you do not specify any protocol settings, then an IP clause is added to the rule. The source and destination IP addresses will also be added if you have specified them. **Note**: If you set a Protocol value other than Any, the packet filter rule is set to that protocol only.
IP Address and Port	Configure the source and target IP addresses and ports.

7. Click **OK**.
8. Save your changes.

Working with packet filter rules

To edit, copy, or remove packet filter rules:

1. Select **Packet Filter Settings**.
2. Do one of the following:

If you want to...	Then...
Edit	**Tip**: You can edit some properties directly on the Packet Filter Rules tab by double-clicking the item you want to configure. 1. Select the rule, and then click the **Edit** icon. 2. Select or clear the **Enabled** check box. 3. Edit the rule, and then click **OK**.
Copy	1. Select the rule, and then click the **Copy** icon. 2. Click the **Paste** icon. 3. Edit the rule as needed, and then click **OK**.
Remove	1. Select the rule. 2. Click the **Remove** icon.

3. Save your changes.

Packet Filter Rules Language

Introduction

A packet filter rule consists of several statements (or clauses) that define the traffic for which the rule applies. When you manually create packet filter rules for the appliance to use, you can use the syntax listed in this topic.

Packet Filter clauses

A packet filter rule consists of several clauses chained together to match specific criteria for each packet. The clauses represent specific layers in the protocol stack. Each clause can be broken down into conditions and expressions. The expressions are the variable part of the rule in which you plug in the address, port, or numeric parameters.

You can use the following packet filter clauses:

- **Adapter clause**

  Specifies a set of adapters from A through H that attaches the rule to a specific adapter. The adapter clause indicates a specific adapter where the rule is applied. The supported adapter expressions are **`any`** and the letters **`A`** through **`H`**. If you do not specify an adapter clause, the rule matches packets on any adapter.

  ```
  adapter <adapter-id>
  adapter A
  adapter any
  adapter A,C
  adapter A-C
  ```

- **Ethernet clause**

  Specifies either a network protocol type or virtual LAN (VLAN) identifier to match the 802.1 frame. You can use the Ethernet clause to filter 801.1q VLAN traffic or allow/deny specific types of Ethernet protocols. You can find the list of protocol types at http://www.iana.org/assignments/ethernet-numbers. Ethernet protocol constants can be specified in decimal, octal, hexadecimal, or alias notation. To make it easier to block specific types of Ethernet traffic, you can specify an alias instead of the well-known number. In some cases, the alias blocks more than one port (for example, IPX and PPPoE).

  ```
  ether proto <protocol-id>
  ether proto {arp|aarp|atalk|ipx|mpls|netbui|pppoe|rarp|sna|xns}
  ether vid <vlan-number>
  ether vid <vlan-number> proto <protocol-id>
  ```

  ```
  ether proto !arp
  ether vid 1 proto 0x0800
  ether vid 2 proto 0x86dd
  ether vid 3-999 proto 0x0800,0x86dd
  ```

- **IP datagram clause**

  Specifies the transport level filtering fields such as IPv4 addresses, TCP/UDP source or destination ports, ICMP type or code, or a specific IP protocol number. The IP datagram clause identifies the protocol that resides inside the IP datagram and the protocol-specific conditions that must be satisfied in order for the statement to match. Currently, only ICMP, TCP, and UDP conditions are supported, but you can specify filters based on any IP protocol. If you do not specify an IP datagram clause, the statement will match any IP datagram protocol.

  The first and second statements below block source and destination IP packets that match the IP address expression. The third statement below blocks source or destination IP packets that match the IP address expression. The fourth statement

below blocks IP packets that match the protocol type. The fifth statement is a combination of the first and second statements. The sixth statement is a combination of the first, second, and fourth statements.

```
1. ip src addr <IPv4-addr>
2. ip dst addr <IPv4-addr>
3. ip addr <IPv4-addr>
4. ip proto <protocol-type>
5. ip src addr <IPv4-addr> dst addr <IPv4-addr>
6. ip src addr <IPv4-addr> dst addr <IPv4-addr> proto <protocol-type>
```

Examples

```
ip addr 192.168.10.1/24
ip addr 192.168.10.0-192.168.10.255
```

Packet Filter conditions

TCP and UDP Conditions

You can specify TCP and UDP port numbers in decimal, octal, or hexadecimal notation. The port's value range is 0 through 65534.

```
tcp src port <TCP-UDP-port>
tcp dst port <TCP-UDP-port>
tcp dst port <TCP-UDP-port> src port <TCP-UDP-port>
udp src port <TCP-UDP-port>
udp dst port <TCP-UDP-port>
udp dst port <TCP-UDP-port> src port <TCP-UDP-port>
```

ICMP conditions

You can specify ICMP conditions in decimal, octal, or hexadecimal notation. You can find the valid number for type and code at http://www.iana.org/assignments/icmp-parameters.

```
icmp type <protocol-type>
icmp code <message-code>
icmp type <protocol-type> code <message-code>
```

Expressions

An expression describes a list of header values that must match the clause's protocol parser. Each clause is directly responsible for matching a specific layer in the protocol stack. The syntax and accept range of values is determined by the clause. The expression can be a single value, a comma separated list of values, or a range set. Currently, expressions exist to specify adapter numbers, IPv4 addresses, TCP and UDP port numbers, ICMP message type and codes, and IP datagram protocol numbers.

```
<value>
<value>, <value>
<value> - <value>
```

Expressions that begin with an exclamation marks (**!**) are called a *not-expressions*. Not-expressions will match all values except those you specify. Not-expressions that do not match any values will generate an error.

IPv4 address expression examples

The `<n>` can be either hex or decimal number in a range from 0 to 255. All hex numbers must have a `0x` prefix. The following table lists examples.

Example	Description
n.n.n.n	Single address
n.n.n.n, n.n.n.n	Address list
n.n.n.n/<netmask>	Specific address using CIDR format; netmask value must range from 1 to 32
n.n.n.n - n.n.n.n	Address range, where first value is greater than last

Table 25: *IPv4 address syntax*

TCP/UDP ports, protocol identifiers, or numbers

The values listed for any constant must be within the fields required range; otherwise the parser refuses the parse clause.

```
0xFFFF
65535
0, 1, 2
0 - 2
! 3 - 65535
```

Complete packet filter rule examples

The following statements are examples of complete packet filter rules. If you do not specify a protocol, the rule assumes and uses the **`any`** protocol.

- `adapter A ip src addr xxx.xxx.x.x`

  (where x is a number in the IP address)
- `adapter A ip src addr xxx.xxx.x dst addr any tcp src port 20 dst port 80`

  (where x is a number in the IP address)
- `adapter any ip src addr any dst addr xxx.xxx.xx.x`
- `adapter any ip src addr any dst addr any icmp type 8`
- `tcp`
- `adapter B icmp`
- `udp`

Tuning Packet Filter Logging

Introduction

Using Local Advanced Parameters, you can tune the way packet filter logging behaves for the appliance. You can specify values such as the number of packet filter logs, the log name, or the maximum log size.

Packet Filter logging parameters

You can edit the following packet filter logging parameters:

Name	Description	Values
np.packet filter.log	Determines whether to log the details of packets that match packet filter rules that are enabled.	string Default: on
np.packet filter.log.count	Number of packet filter log files.	number Default: 10
np.packet filter.log.prefix	Prefix of packet filter log file name.	string Default: /var/iss/fw
np.packet filter.log.size	Maximum size of a packet filter log file in bytes.	number Default: 1400000
np.packet filter.log.suffix	Suffix of packet filter log file name.	string Default: .log

Table 26: *Packet Filter advanced parameters*

Procedure

To tune the packet filter log settings:

1. Select **Local Tuning Parameters**.
2. Select the **Advanced Parameters** tab.
3. Select the parameter you want to change, and then click **Edit**.
4. Complete or change the settings as indicated in the following table.

Setting	Description
Enabled	Select this check box to enable the parameter.
Name	Displays the name of the parameter. **Note**: ISS recommends that you do not edit the parameter's name.
Comment	Describes the parameter. Type a new description if necessary.
Value	Edit the value for the parameter. **Note**: ISS recommends that you keep the default parameter value.

5. Click **OK**.
6. Save your changes.

Chapter 10

Configuring Local Tuning Parameters

Overview

Introduction

Local tuning parameters affect intrusion detection settings at the device level for individual appliances. This chapter describes how to configure local tuning parameters for the appliance, such as the alert queue, the network card adapter properties, and advanced parameters.

In this chapter

This chapter contains the following topics:

Configuring Alerts

Introduction

You can configure alert messages that notify you about appliance-related events. You can also determine what action the appliance should take when an event causes an alert, such as sending an email to the appliance administrator, or running an executable in response to the event.

Alert types

You can enable three types of sensor event alerts:

- **Error**. These alerts notify you when a sensor system error has occurred.
- **Warning**. These alerts notify you when a problem has occurred on the appliance itself.
- **Informative**. These alerts notify you about what actions users may have performed on the appliance, such as changing passwords, downloading logs, or editing a parameter.

System alerts and SNMP

Through the Configuration Menu on the appliance, you can configure the appliance to send SNMP traps in the event of system health-related events such as the following:

- no free disk space
- disk failure
- overly-high CPU usage

When the appliance detects these problems, it can send an SNMP trap to the SNMP receiver that was specified when the appliance was installed. These system-related alerts can be sent as SNMPv1 or SNMP v2c traps. See "SNMP configuration" on page 23 for information about configuring SNMP system health-related alerts.

Procedure

To configure an alert:

1. Select **Local Tuning Parameters**.
2. Select the **Alerts** tab.
3. In the area for the alert type (Sensor Error, Warning, Informative) to configure, select the **Enable** check box.
4. Select a **Priority** for the alert: Low, Medium, or High.
5. Select the **Display on console** check box to enable the alert to appear in the console.

   Note: In Proventia Manager, alerts appear on the Alerts tab. In SiteProtector, alerts appear on the Analysis tab in the Console.
6. To send an SNMP trap, complete or change settings indicated in the following table.

Setting	Description
Send SNMP Trap	Select the check box to enable the option, and then do one of the following: • To use a previously configured SNMP trap, select one from the list, and then go to Step 7. • To configure a new SNMP trap, click **Configure SNMP**.

Setting	Description
Configure SNMP	Click **Add**, and then specify the following: • **Name**. Type the name of the SNMP trap or response. • **Manager**. Type the IP address where the SNMP Manager is running. The appliance must be able to access the SNMP Host to send SNMP traps. • **Community**. Type the appropriate community name (public or private).

7. To send an email notification, complete or change the settings as indicated in the following table.

Setting	Description
Send Email	Select the check box to enable the option, and then do one of the following: • To use a previously configured email notification, select one from the list, and then go to Step 8. • To configure a new email notification, click **Configure Email**.
Configure Email	Click **Add**, and then specify the following: • **Name**. Type a meaningful name. • **SMTP Host**. Type the mail server (as a fully qualified domain name or IP address). **Note**: The SMTP Host must be accessible to the appliance to send email notifications. • **From**. Type individual or group email address(es). Separate addresses with commas. • **To**. Type individual recipient or email group(s). Separate addresses with commas. • **Subject**. Type a subject, or select Common Parameters from the list. When you select common parameters, they are populated with the corresponding event information. • **Body**. Type the message body, or select Common Parameters from the list. When you select common parameters, they are populated with the corresponding event information.

8. Save your changes.

Managing Network Adapter Cards

Introduction

You can view and manage settings for the appliance's network adapter cards.

Important: If you change any settings on this page, the appliance may lose link temporarily.

Editing network adapter card properties

To edit network adapter card properties:

1. On the **Local Tuning Parameters** page, select the **Adapter Management** tab.
2. Select an adapter in the list, and then click **Edit**.
3. Type a meaningful name to associate with the **Port**.

   Note: The port names correspond to the labels 1A, 1B, 2C, 2D, 3E, 3F, 4G, and 4H on the front of the appliance. The ports are arranged as pairs of ports on a card as follows:

   - 1A with 1B on Card1
   - 2C with 2D on Card2
   - 3E with 3F on Card3
   - 4G with 4H on Card4
4. From the **TCP Resets** drop-down, specify whether kills should be sent through this port or through the TCP Reset (external kill) port.

   Note: TCPReset is not available for Proventia A201 appliances.
5. For the **Port/Duplex Speed Settings**, select the method the network adapter should use to determine link speed and mode.

Method	Description
Auto Negotiate	Allows two interfaces on a link to select the best common mode automatically, the moment a cable is connected. **Note**: ISS recommends that you use this setting unless you have to change the setting for a switch or other network device that does not support auto-negotiation, or if the auto-negotiation process is taking too long to establish a link.
10 MB Half Duplex	Device either transmits or receives information at 10 megabits per second, but not at the same time.
10 MB Full Duplex	Device transmits information at 10 megabits per second in both directions at the same time.
100 MB Half Duplex	Device either transmits or receives information at 100 megabits per second, but not both at the same time.
100 MB Full Duplex	Device transmits information at 100 megabits per second in both directions at the same time.
1000 MB Full Duplex	Device transmits information at 1000 megabits per second in both directions at the same time.

6. Click **OK**.
7. Save your changes.

Managing the Alert Queue

Introduction

The appliance uses a queue file named SensorEventQueue.adf to store event alerts. Use the Alert Queue page to determine how large this file can become before alerts are lost and how the queue file handles alerts after the maximum file size is reached.

Alert queue and SiteProtector

The options you select on this page only change settings for the Proventia Manager queue file. When you are managing the appliance through SiteProtector, event data flows directly through the queue to the Event Collector and into the Site Database. However, if communication goes down between the appliance and the Event Collector, or between the Event Collector and the Site Database, the event data is stored in the queue file. When normal communication resumes, the queued data is committed through the Event Collector to the Site Database.

Procedure

To manage the alert queue size:

1. Select **Local Tuning Parameters**.
2. Select the **Alert Queue** tab.
3. Complete or change the settings as indicated in the following table.

Setting	Description
Proventia Manager Alert Queue Max Size	Type the maximum size of the alert queue file.
Proventia Manager Alert Queue Full Policy	Select the method the appliance should use once the queue reaches its maximum size, as follows: • **Stop Logging**. The queue file stops logging alerts when the maximum file size is reached. • **Wrap Around**. The queue file overwrites the oldest alert in order to create space for the new alert, when the maximum file size is reached.

4. Save your changes.

   Important: When you save changes on this page, the agent must restart. This may briefly impact the network and security, as the agent goes into bypass for a short time.

Configuring Advanced Parameters

Introduction

You can use the Advanced Parameters tab to configure (or tune) certain parameters for a specific appliance to better meet your security needs or enhance the performance of the hardware.

You can tune the following components for each appliance:

- intrusion detection responses
- intrusion detection security risks
- automatic updates

About advanced parameters

Advanced parameters are composed of name/value pairs. Each name/value pair has a default value. For example, the parameter np.packet filter.log is a parameter that determines whether to log the details of packets that match packet filter rules you have enabled. The default value for this parameter is on.

You can edit the value of any parameter that appears in the list on the Advanced Parameters tab. If the parameter does not appear in the list, it does not mean the parameter has no default value. You simply need to add the parameter to the list with the new value.

For information about update advanced parameters, see. For information about packet filter logging parameters, see "Tuning Packet Filter Logging" on page 93.

Common advanced tuning parameters

The following table describes common advanced tuning parameters:

Name	Type	Default Value	Description
crm.history.enabled	boolean	true	Determines whether to log administrative history.
crm.history.file	string	/var/iss/ crmhistory.log	The administrative history file name.
crm.policy.numbackups	number	4	The number of previous policy files to save.
engine.adapter.high-water.default	number	5	The number of packets per traffic sampling interval that are expected to flow on each adapter. The high-water mark is used to prevent multiple low traffic warnings from being issued when the traffic is hovering around low-water mark.

Table 27: *Common advanced tuning parameters*

Name	Type	Default Value	Description
engine.adapter.low-water.default	number	1	The minimum number of packets per traffic sampling interval that are expected to flow on each adapter. The low-water mark is used as the threshold to issue Network_Quiet and Network_Normal audit events.
engine.droplog.enabled	boolean	false	Determines whether logging of dropped packets is enabled.
engine.droplog.fileprefix	string	/var/iss/drop	The drop log file name prefix.
engine.droplog.filesuffix	string	.enc	The drop log file name suffix.
engine.droplog.flush	boolean	false	Disables buffering of dropped packets. Enabling this adversely affects performance.
engine.droplog.maxfiles	number	10	The number of drop log files to save.
engine.droplog.maxkbytes	number	10000 (kb)	The maximum size of a drop log file.
engine.evidencelog.fileprefix	string	/var/iss/ evidence	The evidence file name prefix.
engine.evidencelog.filesufffix	string	.enc	The evidence file name suffix.
engine.evidencelog.maxfiles	number	10	The number of evidence files to save.
engine.evidencelog.maxkbytes	number	10000 (kb)	The maximum size of an evidence file.
engine.log.file	string	/var/iss/ engine#.log	The engine log file name.
engine.pam.logfile	string	/var/iss/ pam#.log	The PAM log file name.
engine.statistics.interval	number	120	The number of seconds between statistics gathering.
np.packet filter.log	string	on	Determines whether to log the details of packets that match packet filter rules that are enabled.
np.statistics	string	on	Determines whether logging of PAM statistics is enabled.
np.statistics.file	on	/var/iss/ pamstats.dat	The PAM statistics file name.

Table 27: *Common advanced tuning parameters (Continued)*

Name	Type	Default Value	Description
pam.traffic.sample	boolean	true	Enables traffic sampling for the purpose of detecting abnormal levels of network activity. This parameter affects the Network_Quiet and Network_Normal audit events.
pam.traffic.sample.interval	number	300	The interval, expressed in seconds, at which traffic flow should be sampled for the purpose of detecting abnormal levels of network activity. This parameter affects the Network_Quiet and Network_Normal audit event.
sensor.trace.level	number	3	The Proventia IDS log level.

Table 27: *Common advanced tuning parameters (Continued)*

Adding advanced parameters

To add advanced parameters:

1. Select **Local Tuning Parameters**.
2. Select the **Advanced Parameters** tab.
3. Click **Add**.
4. Complete the settings as indicated in the following table.

Setting	Description
Enabled	Select this check box to enable the parameter.
Name	Type a name for the parameter. **Example**: engine.log.file
Comment	Type a unique description for the parameter. **Example**: The engine log file.
Value	Select one of the following options: • **Boolean**. Select a value of True or False. • **Number**. Enter the appropriate number for the parameter. • **String**. Type the value for the parameter, such a log file location. Example: /var/iss/engine#.log

5. Click **OK**.
6. Save your changes.

Working with advanced parameters

To edit, copy, or remove advanced parameters:

1. Select **Local Tuning Parameters**.
2. Select the **Advanced Parameters** tab, and then do one of the following:

If you want to...	Then...
Edit	**Tip**: You can edit some properties directly on the Advanced Parameters tab by double-clicking the item you want to configure. 1. Select the parameter, and then click the **Edit** icon. 2. Select or clear the **Enabled** check box. 3. Edit the parameter, and then click **OK**.
Copy	1. Select the parameter, and then click the **Copy** icon. 2. Click the **Paste** icon. 3. Edit the parameter as needed, and then click **OK**.
Remove	1. Select the parameter. 2. Click the **Remove** icon.

3. Save your changes.

Configuring TCPReset

Introduction

You can use the appliance to monitor (read-only) SPAN ports on network equipment. To monitor (read-only) SPAN ports, you must configure the appliance's TCPReset (kill) port. If using (read-only) monitoring ports, the appliance must send kills on another interface.

TCPReset is not available for Proventia A201 appliances.

Note: The appliance is configured by default to send kills through the monitoring ports even in passive monitoring mode. For example, if you are monitoring through a hub, you do not need to configure the external kill port.

Procedure

To configure TCPReset:

1. Connect the kill port to the network.
2. To determine the MAC address of the router of the kill port (eth0), do one of the following:
   - Contact your system administrator to get the MAC address of the router. Once you have received the MAC address, go to Step 4.
   - Run the get-reset-config script on the appliance to get the MAC address. Go to Step 3.
3. Login to the appliance as root and run `get-reset-config`.

   Note the following:
   - If you run the script without parameters, it displays usage information.
   - If you run the script with required parameters, it displays the MAC address.

   Note: The `get-reset-config` utility requires a temporary IP address to connect to the network in order to detect the router's MAC address. During normal operation, the kill port is in stealth mode and does not require an IP address
4. In Proventia Manager, select **System→Local Tuning Parameters**.
5. Select the **Advanced Parameters** tab.
6. Add the local tuning parameter `np.macaddress.destination` to configure the MAC address of the router:

   ```
   np.macaddress.destination = XX:XX:XX:XX:XX:XX
   ```

   Note: See "Adding advanced parameters" on page 103 for more information about adding a local parameter.
7. Select the **Adapter Management** tab.
8. Select the adapter for which you want to enable the External Kill port, and then click **Edit**.
9. On each port where you want to enable the External Kill port, change **TCP Resets** from "This Port" to "TCP Reset Port", and then click **OK**.
10. To enable External Kill ports on other adapters, repeat Steps 8 and 9.

    Example: You can enable the External Kill port to send TCP Resets for events received on ports A, B, C, and D, but you can also choose to send TCP resets for events received on ports E and F through E and F.
11. Click **Save Changes**.

Chapter 11

Managing System Settings

Overview

Introduction

This chapter explains how to view system status and how to change system settings and properties. For the procedures in this chapter, you will use the Proventia Manager. Even if you are managing the appliance through SiteProtector, you must use Proventia Manager to configure these local settings.

In this chapter

This chapter contains the following topics:

Viewing System Status

Introduction

Review system status information occasionally to ensure the appliance is not overwhelmed by network traffic. System settings can also help you detect any sudden changes in memory or CPU usage.

Procedure

To view system status:

1. In the navigation pane, select **System**.

   The following system information appears:

Table	Statistic	Description
Memory Usage	Total Memory	Amount of memory installed on the appliance.
	Used Memory	Amount of memory currently used by running processes.
	Free Memory	Amount of unused memory on the appliance.
CPU Usage	User	Percentage of CPU resources used by user-level processes.
	System	Percentage of system resources used by the kernel.
	Idle	Percentage of CPU resources currently not used.

2. To refresh the information, select a value from the **Refresh Data** list.

   Tip: Select **Refresh Now** to manually refresh the page.

Managing Log Files

Introduction

The Log Files page in Proventia Manager displays all the log files associated with the appliance. Use this page to view, download, or delete system logs.

About timestamps in log files

Timestamps in log files are stored in Unix time (the number of seconds elapsed since 00:00:00 on January 1, 1970 UTC).

You can use a tool called logtime to translate these timestamps to local time.

Important: You must perform this operation on the appliance itself.

Downloading log files

To download log files:

1. In the navigation pane, select **System→Log Files**.
2. Select a file to download, and then click **Download**.
3. Select **Save the file to disk**, and then click **OK**.
4. Type a **File Name**, and then click **Save**.

   Note: After the download, the saved log file still exists on the appliance.

Deleting log files

To delete log files:

1. In the navigation pane, select **System→Log Files**.
2. Do one of the following:
   - Select a file to delete, and then click **Delete**.
   - Click **Delete All**.
3. Click **OK**.

Translating log file timestamps

To translate the log file timestamps:

1. Log on to the appliance as root.
2. Run logtime with the required parameters. If you run logtime without the arguments, logtime will display usage information.

   Example: To translate timestamps in the packet filter log file frw000.log, run the following command:

   ```
   logtime /var/iss/frw000.log /var/iss/newfrw000.log
   ```

   This command creates a new file called newfrw000.log based on the frw000.log file, but the timestamps in the new file are in local time. The original log file is not modified.

   If you create the new translated log file in /var/iss directory, you can download it from Proventia Manager.

Working with System Tools

Introduction

Use the System Tools page to perform basic system tasks, such as the following:

- handling problems with the appliance management port
- testing whether the appliance is communicating correctly with SiteProtector
- testing whether the appliance can communicate with configured SNMP trap receivers, email servers, or NTP servers

Important: You can only perform these tasks in Proventia Manager.

Rebooting the appliance

To reboot the appliance:

1. In Proventia Manager, select **System→Tools**.
2. Click **Reboot**.
3. Click **OK** to reboot the appliance.

Shutting down the appliance

To shut down the appliance:

1. In Proventia Manager, select **System→Tools**.
2. Click **Shut Down**.
3. Click **OK** to shut down the appliance.

Pinging a computer

To ping a computer:

1. In Proventia Manager, select **System→Tools**.
2. In the Diagnostics area, type the IP address of the computer you want to test in the **Ping** box.
3. Click **Submit**.

Using the traceroute utility

To use the traceroute utility:

1. Select **System→Tools**.
2. In the Diagnostics area, type the IP address you want to trace in the **Traceroute** box.
3. Select a **Protocol**, as follows:

Protocol	Description
UDP	When you select a UDP traceroute protocol (UNIX "traceroute" command), the appliance sends a UDP packet to a random port on the target host. The TTL (Time to Live) field and the destination port field are incremented for each "ICMP Port Unreachable" message that is returned, or 30 hops are reached.
ICMP	When you select a ICMP traceroute protocol (Windows "tracert" command), the TTL (Time to Live) field and the destination port field are incremented for each "ICMP Echo Request" message that is returned, or 30 hops are reached.

4. Click **Submit**.

Configuring User Access

Introduction

You can change the following passwords in the Proventia Manager interface:

- root password for the command line
- administrative password for the Proventia appliance
- Web administrative password for the Proventia Manager

Important: Record and protect your passwords. If you lose a password, you must reinstall the appliance and reconfigure the network settings.

You can also enable or disable the bootloader (root) password. The bootloader password protects the appliance from unauthorized users during the boot process. When you enable the bootloader password, then you must enter the root password to use a boot option other than the default.

Changing passwords

To change passwords:

1. In Proventia Manager, select **System→ Access**.
2. In the area for the password you want to change, type the **Current Password**.
3. Click **Set Password**.
4. Type the new password twice to confirm it, and then click **OK**.
5. Click **Save Changes**.

Enabling or disabling the boot loader password

To enable the boot loader password:

1. In the navigation pane, select **System→ Access**.
2. Select or clear the **Enable bootloader password** check box, depending on whether you want to enable or disable the password.
3. Click **Save Changes**.

Installing and Viewing Current Licenses

Introduction

Use the Licensing page to view important information about the current status of the license file, including expiration dates, and to enter new license key files to activate Proventia Manager. Each license key file you install is unique to the product license and may require that you provide IP address range information specific to the network. You can also access the License Information page, which tells you how to acquire a current license.

Important: ISS is bound by its confidentiality policy not to share the network information with any other organization, except as required by law.

Installing a license key file

To install a license key file:

1. In Proventia Manager, select **System→Licensing**.
2. Click **Browse** in the Upload a new License Key box.
3. Locate the license key file that you downloaded.
4. Click **OK**.
5. Click **Upload**.

Viewing current license settings

To view current license settings:

1. In Proventia Manager, select **System→Licensing**.
2. Review the following **Status** information:

Status	Description
Serial Number	The serial number of the license key. **Note**: Each license key has its own serial number, unique to the Identity and the OCN.
OCN	The Order Confirmation Number (OCN) or your customer number with ISS.
Expiration	The date the license expires, in yyyy-mm-dd format.
Maintenance Expiration	The date the maintenance agreement expires, in yyyy-mm-dd format.

3. To access information about acquiring or maintaining licenses, click **License Renewal Information**.

   The License Information page appears and tells you how to contact an ISS representative.

Chapter 12

Viewing Alerts and System Information

Introduction

This chapter describes how to view system alerts, events, logs, and statistics in the Proventia Manager.

This chapter contains the following topics:

Viewing Alerts

Introduction

Use the Alerts page in the Proventia Manager to view and manage system- and security-related alerts. The alerts list contains the following alert types:

- intrusion detection alerts are related to attempted attacks that occur in the network
- system alerts are related the appliance and its operation

Reference: See "Configuring Alerts" on page 96 for more information about creating alerts to display in the management console.

How the appliance saves the alert list

The current list is saved as three comma separated values (.csv) files. The three files are used to cross-reference the data that appears in the Alerts page. The files are as follows:

This file...	Contains...
filename_eventdata.csv	the distinct records that match the alert record number. This file also lists the alert name and the risk level.
filename_eventinfo.csv	the data listed in the alert specific information section of the alert.
filename_eventresp.csv	the data from the responses executed section of the alert.

Table 28: *Alert list files*

Viewing alert information

To view alert information:

1. Do one of the following:
   - Click the **Alerts** button.
   - Select one of the following:

     Notifications→Alerts

     Intrusion Detection→Alerts

     System→Alerts

   The Alerts tab displays the following information about each alert:

Column	Description
Rec.#	Record number of the alert.
Risk Level	Risk level icon for the alert.
Alert Name	The alert name.
Source IP	The source IP address for the alert.
Source Port	The source port and port name for the alert.
Destination IP	The destination (or target) IP address of the alert.
Destination Port	The destination (or target) port and port name of the alert.
Protocol	The alert's protocol and protocol number.
Vuln Status	The vulnerability status.
Alert Date & Time	The date and time the alert occurred.

2. To view an alert's details, click the **Alert Name**.

   Tip: To view the previous or next alert's details, click the UP or DOWN arrows.

3. To refresh the view, from the **Refresh Data** list, select one of the following:
   - To refresh the list immediately, select **Refresh Now**.
   - To refresh the list automatically, select the time interval.

   Tip: Select **Auto Off** to turn off automatic refresh. If you select this option, you must manually refresh the page to view the latest alerts.

Filtering alerts

To filter alerts:

1. Do one of the following:
   - Click the **Alerts** button.
   - Select one of the following:

     Notifications→Alerts

     Intrusion Detection→Alerts

     System→Alerts

2. On the Alerts tab, select one of the **Filter Options** listed in the following table:

Option	Description
Risk Level	Displays alerts by the level you select from the **Risk Level** list.
Alert Name	Type the **Alert Name** for which you want to search. You can use wildcard characters to search for alert names.
Alert Type	Select an **Alert Type**, Intrusion Detection or System.
Date and Time	Enter a specific **Start Date and Time** or **End Date and Time** to search for alerts.
Source IP	Search for alerts for the **Source IP** address you specify.
Target IP	Search for alerts for the **Target IP** address you specify.
Source and Target IP	Search for alerts for both the **Source and Target IP** addresses you specify.
Source Port Number	Search for alerts for the **Source Port Number** you specify.
Target Port Number	Search for alerts for the **Target Port Number** you specify.
Protocol Number	Search for alerts by the **Protocol Number** you specify.
Multiple Values	Enter a combination of filters to search for alerts. For example, you could enter values for Date and Time, Source IP, and Protocol Type to narrow the search.

Saving the alerts list

To save the alerts list:

1. Do one of the following:
   - Click the **Alerts** button.
   - Select one of the following:

     Notifications→Alerts

     Intrusion Detection→Alerts

     System→Alerts
2. On the Alerts tab, click **Save alerts list to file**.
3. Select the log where you want to save the information, and then click **Download**.
4. On the File Download dialog box, click **Save**.
5. Do one of the following:
   - To save this information in a new file, type the new file name and click **Save**.
   - To save this information in an existing file, click **Save**.

Clearing alerts from the list

To clear alerts from the list:

1. Do one of the following:
   - Click the **Alerts** button.
   - Select one of the following:

     Notifications→Alerts

     Intrusion Detection→Alerts

     System→Alerts
2. On the Alerts tab, click **Clear alerts list**.
3. Click **OK**.

Managing Saved Alert Files

Introduction

Use the Log File Management page in Proventia Manager to view and manage saved alerts files by either downloading the files to another system, deleting the files, or by doing both. After you download files to another system, the saved file still exists on the appliance.

Downloading alert files

To download alert files:

1. Do one of the following:
   - Click the **Alerts** button.
   - Select one of the following:

     Notifications→Alerts

     Intrusion Detection→Alerts

     System→Alerts
2. On the Alerts page, click **View/manage alerts files**.
3. Select a file to download, and then click **Download**.
4. Select **Save the file to disk**, and then click **OK**.
5. Type a **File Name**, and then click **Save**.

Deleting alert files

To delete alert files:

1. Do one of the following:
   - Click the **Alerts** button.
   - Select one of the following:

     Notifications→Alerts

     Intrusion Detection→Alerts

     System→Alerts
2. On the Alerts page, click **View/manage alerts files**.
3. Do one of the following:
   - Select a file to delete, and then click **Delete**.
   - Click **Delete All**.
4. Click **OK**.

Viewing Notifications Status

Introduction

The Notifications Status area provides valuable information about actions taking place on the appliance.

You can view or change the following:

- Alert log event data
- System logs

Viewing alert log event data

Use the Alert Event Log information on the Notifications Status page to monitor the size and number of your event logs. Monitoring this information will help you effectively manage system and event data. If a serious event occurs, you will be able to find the information and solve the problem quickly.

The Alert Event Log table provides the following information:

Item	Description
Number of Logged Alerts	The number of alerts written to the log file.
Percentage Full	The percentage of allocated space that contains alerts log entries.
Time of Last Alert	The date and time of the last alert written to the log file.

Table 29: *Alert log event data*

Viewing system logs

Use the System Logs page to view the system log. System logs contain important information about actions the application has taken, either because a user performed the action (system restart or manual feature configuration), or the appliance has performed the action itself (such as an automatic update).

Refreshing notification status data

You can refresh the page manually or automatically at certain intervals.

To refresh the data:

- Select an option from the **Refresh Data** list:
  - Refresh Now (Use this option to manually refresh the page.)
  - every 10 seconds
  - every 20 seconds
  - every 30 seconds
  - every 1 minute
  - every 2 minutes
  - Auto Off (Use this option to disable automatic refresh.)

  The appliance refreshes the page to display the latest events.

Viewing Statistics

Introduction

Use the Statistics page to view the statistics of network traffic processed by the appliance. You can use these statistics for testing purposes, troubleshooting, or some type of auditing to discover network data and attack trends.

Viewing statistics

To view the statistics:

1. On the Proventia Manager navigation pane, select **Statistics**.
2. Select one of the following statistics pages to view:

Statistic	Description
Protection Statistics	Use the Protection Statistics page to view information about the current appliance configuration and behavior that occurred as a result of the configuration. This information includes statistics about enabled event checks, as well as details about attack and blocking actions the appliance has taken.
Packet Analysis Statistics	Use the Packet Analysis Statistics page to view all the statistics output by the Protocol Analysis Module (PAM). You can use this information to track protocol counts and protocol processing.
Driver Statistics	Use the Driver Statistics page to view network activity on each adapter used on the appliance, as well as information about packet counts (such as packets injected, rejected, or dropped), or any unanalyzed packets that have passed through the network. Unanalyzed packets can pass through when the appliance is overloaded, or because of routine events such as policy "push" through groups.

Types of driver packets

The following table describes the driver packets:

Packets	Description
Received Packets	The number of packets received since the adapter instance was created.
Transmitted Packets	The number of packets transmitted since the adapter instance was created. This number includes packets forwarded, injected, or unanalyzed.
Forwarded Packets	The number of packets forwarded to a twinned or mirror interface since the adapter instance was created. This number does not include injected packets, but does include packets forwarded without analysis.
Dropped Packets	The number of packets not forwarded (dropped) since the adapter instance was created. (Includes those dropped without analysis.)
Injected Packets	The number of packets injected (i.e. transmitted packets constructed by the application) since the adapter instance was created.

Table 30: *Driver packets*

Packets	Description
Unanalyzed Packets	The number of packets forwarded or dropped without analysis since the adapter instance was created. Unanalyzed packets are processed by the driver whenever the application cannot process them as quickly as they are being received. Whether unanalyzed packets are forwarded or dropped as well as the threshold at which the driver determines that the application is not keeping up is determined by configuration parameters.

Table 30: *Driver packets*

Index

a

b

c

d

e

f

g

h

i

k

l

m

n

o

p

r

s

t

u

v

w

X

Internet Security Systems, Inc. Software License Agreement

THIS SOFTWARE PRODUCT IS PROVIDED IN OBJECT CODE AND IS LICENSED, NOT SOLD. BY INSTALLING, ACTIVATING, COPYING OR OTHERWISE USING THIS SOFTWARE PRODUCT, YOU AGREE TO ALL OF THE PROVISIONS OF THIS SOFTWARE LICENSE AGREEMENT ("LICENSE"). EXCEPT AS MAY BE MODIFIED BY AN APPLICABLE ISS LICENSE NOTIFICATION THAT ACCOMPANIES, PRECEDES, OR FOLLOWS THIS LICENSE, AND AS MAY FURTHER BE DEFINED IN THE USER DOCUMENTATION ACCOMPANYING THE SOFTWARE PRODUCT, YOUR RIGHTS AND OBLIGATIONS WITH RESPECT TO THE USE OF THIS SOFTWARE PRODUCT ARE AS SET FORTH BELOW. IF YOU ARE NOT WILLING TO BE BOUND BY THIS LICENSE, RETURN ALL COPIES OF THE SOFTWARE PRODUCT, INCLUDING ANY LICENSE KEYS, TO ISS WITHIN FIFTEEN (15) DAYS OF RECEIPT FOR A FULL REFUND OF ANY PAID LICENSE FEE. IF THE SOFTWARE PRODUCT WAS OBTAINED BY DOWNLOAD, YOU MAY CERTIFY DESTRUCTION OF ALL COPIES AND ANY LICENSE KEYS IN LIEU OF RETURN.

1. License - Upon your payment of the applicable fees and ISS delivery to you of the applicable license notification, Internet Security Systems, Inc. ("ISS") grants to you as the only end user ("Licensee") a nonexclusive and nontransferable, limited license for the accompanying ISS software product, the related documentation, and any associated license key(s) (Software), for use only on the specific network configuration, for the number and type of devices, and for the time period ("Term") that are specified in ISS quotation and Licensees purchase order, as accepted by ISS. ISS limits use of Software based upon the number of nodes, users and/or the number and type of devices upon which it may be installed, used, gather data from, or report on, depending upon the specific Software licensed. A device includes any network addressable device connected to Licensees network, including remotely, including but not limited to personal computers, workstations, servers, routers, hubs and printers. A device may also include ISS hardware (each an Appliance) delivered with pre-installed Software and the license associated with such shall be a non-exclusive, nontransferable, limited license to use such pre-installed Software only in conjunction with the ISS hardware with which it is originally supplied and only during the usable life of such hardware. Except as provided in the immediately preceding sentence, Licensee may reproduce, install and use the Software on multiple devices, provided that the total number and type are authorized by ISS. Licensee may make a reasonable number of backup copies of the Software solely for archival and disaster recovery purposes. In connection with certain Software products, ISS licenses security content on a subscription basis for a Term. Content subscriptions are licensed pursuant to this License based upon the number of protected nodes or number of users. Security content is regularly updated and includes, but is not limited to, Internet content (URLs) and spam signatures that ISS classifies, security algorithms, checks, decodes, and ISS related analysis of such information, all of which ISS regards as its confidential information and intellectual property. Security content may only be used in conjunction with the applicable Software in accordance with this License. The use or re-use of such content for commercial purposes is prohibited. Licensees access to the security content is through an Internet update using the Software. In addition, unknown URLs may be automatically forwarded to ISS through the Software, analyzed, classified, entered into ISS URL database and provided to Licensee as security content updates at regular intervals. ISS URL database is located at an ISS facility or as a mirrored version on Licensees premises. Any access by Licensee to the URL database that is not in conformance with this License is prohibited. Upon expiration of the security content subscription Term, unless Licensee renews such content subscription, Licensee shall implement appropriate system configuration modifications to terminate its use of the content subscription. Upon expiration of the license Term, Licensee shall cease using the Software and certify return or destruction of it upon request.
2. Migration Utilities - For Software ISS markets or sells as a Migration Utility, the following shall apply. Provided Licensee holds a valid license to the ISS Software to which the Migration Utility relates (the Original Software), ISS grants to Licensee as the only end user a nonexclusive and nontransferable, limited license to the Migration Utility and the related documentation ("Migration Utility") for use only in connection with Licensees migration of the Original Software to the replacement software, as recommended by ISS in the related documentation. The Term of this License is for as long as Licensee holds a valid license to the applicable Original Software. Licensee may reproduce, install and use the Migration Utility on multiple devices in connection with its migration from the Original Software to the replacement software. Licensee shall implement appropriate safeguards and controls to prevent unlicensed use of the Migration Utility. Licensee may make a reasonable number of backup copies of the Migration Utility solely for archival and disaster recovery purposes.
3. Third-party Products - Use of third party product(s) supplied hereunder, if any, will be subject solely to the manufacturers terms and conditions that will be provided to Licensee upon delivery. ISS will pass any third party product warranties through to Licensee to the extent authorized. If ISS supplies Licensee with Crystal Decisions Runtime Software, then the following additional terms apply: Licensee agrees not to alter, disassemble, decompile, translate, adapt or reverse-engineer the Runtime Software or the report file (.RPT) format, or to use, distribute or integrate the Runtime Software with any general-purpose report writing, data analysis or report delivery product or any other product that performs the same or similar functions as Crystal Decisions product offerings; Licensee agrees not to use the Software to create for distribution a product that converts the report file (.RPT) format to an alternative report file format used by any general-purpose report writing, data analysis or report delivery product that is not the property of Crystal Decisions; Licensee agrees not to use the Runtime Software on a rental or timesharing basis or to operate a service bureau facility for the benefit of third parties unless Licensee first acquires an Application Service Provider License from Crystal Decisions; **CRYSTAL DECISIONS AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS, OR IMPLIED, INCLUDING WITHOUT LIMITATION THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. CRYSTAL DECISIONS AND ITS SUPPLIERS SHALL HAVE NO LIABILITY WHATSOEVER UNDER THIS AGREEMENT OR IN CONNECTION WITH THE SOFTWARE.** In this section 3 Software means the Crystal Reports software and associated documentation supplied by ISS and any updates, additional modules, or additional software provided by Crystal Decisions in connection therewith; it includes Crystal Decisions Design Tools, Report Application Server and Runtime Software, but does not include any promotional software or other software products provided in the same package, which shall be governed by the online software license agreements included with such promotional software or software product.
4. Beta License - If ISS is providing Licensee with the Software, security content and related documentation, and/or an Appliance as a part of an alpha or beta test, the following terms of this Section 4 additionally apply and supersede any conflicting provisions herein or any other license agreement accompanying, contained or embedded in the subject prototype product or any associated documentation. ISS grants to Licensee a nonexclusive, nontransferable, limited license to use the ISS alpha/beta software program, security content, if any, Appliance and any related documentation furnished by ISS (Beta Products) for Licensees evaluation and comment (the "Beta License") during the Test Period. ISS standard test cycle, which may be extended at ISS discretion, extends for sixty (60) days, commencing on the date of delivery of the Beta Products (the "Test Period"). Upon expiration of the Test Period or termination of the Beta License, Licensee shall, within thirty (30) days, return to ISS or destroy all copies of the beta Software, and shall furnish ISS written confirmation of such return or destruction upon request. If ISS provides Licensee a beta Appliance, Licensee agrees to discontinue use of and return such Appliance to ISS upon ISS request and direction. If Licensee does not promptly comply with this request, ISS may, in its sole discretion, invoice Licensee in accordance with ISS current policies. Licensee will provide ISS information reasonably requested by ISS regarding Licensee's experiences with the installation and operation of the Beta Products. Licensee agrees that ISS shall have the right to use, in any manner and for any purpose, any information gained as a result of Licensees use and evaluation of the Beta Products. Such information shall include but not be limited to changes, modifications and corrections to the Beta Products. Licensee grants to ISS a perpetual, royalty-free, non-exclusive, transferable, sublicensable right and license to use, copy, make derivative works of and distribute any report, test result, suggestion or other item resulting from Licensee's evaluation of its installation and operation of the Beta Products. **LICENSEE AGREES NOT TO EXPORT BETA PRODUCTS DESIGNATED BY ISS IN ITS BETA PRODUCT DOCUMENTATION AS NOT YET CLASSIFIED FOR EXPORT TO ANY DESTINATION OTHER THAN THE U.S. AND THOSE COUNTRIES ELIGIBLE FOR EXPORT UNDER THE PROVISIONS OF 15 CFR 740.17(A) (SUPPLEMENT 3), CURRENTLY CANADA, THE EUROPEAN UNION, AUSTRALIA, JAPAN, NEW ZEALAND, NORWAY, AND SWITZERLAND.** If Licensee is ever held or deemed to be the owner of any copyright rights in the Beta Products or any changes, modifications or corrections to the Beta Products, then Licensee hereby irrevocably assigns to ISS all such rights, title and interest and agrees to execute all documents necessary to implement and confirm the letter and intent of this Section. Licensee acknowledges and agrees that the Beta Products (including its existence, nature and specific features) constitute Confidential Information as defined in Section 18. Licensee further agrees to treat as Confidential Information all feedback, reports, test results, suggestions, and other items resulting from Licensee's evaluation and testing of the Beta Products as contemplated in this Agreement. With regard to the Beta Products, ISS has no obligation to provide support, maintenance, upgrades, modifications, or new releases. However, ISS agrees to use its reasonable efforts to correct errors in the Beta Products and related documentation within a reasonable time, and will provide Licensee with any corrections it makes available to other evaluation participants. The documentation relating to the Beta Products may be in draft form and will, in many cases, be incomplete. Owing to the experimental nature of the Beta Products, Licensee is advised not to rely exclusively on the Beta Products for any reason. **LICENSEE AGREES THAT THE BETA PRODUCTS AND RELATED DOCUMENTATION ARE BEING DELIVERED "AS IS" FOR TEST AND EVALUATION PURPOSES ONLY WITHOUT WARRANTIES OF ANY KIND, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OF NONINFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. LICENSEE ACKNOWLEDGES AND AGREES THAT THE BETA PRODUCT MAY CONTAIN DEFECTS, PRODUCE ERRONEOUS AND UNINTENDED RESULTS AND MAY AFFECT DATA NETWORK SERVICES AND OTHER MATERIALS OF LICENSEE. LICENSEES USE OF THE BETA PRODUCT IS AT THE SOLE RISK OF LICENSEE. IN NO EVENT WILL ISS BE LIABLE TO LICENSEE OR ANY OTHER PERSON FOR DAMAGES, DIRECT OR INDIRECT, OF ANY NATURE, OR EXPENSES INCURRED BY LICENSEE. LICENSEE'S SOLE AND EXCLUSIVE REMEDY SHALL BE TO TERMINATE THE BETA PRODUCT LICENSE BY WRITTEN NOTICE TO ISS.**
5. Evaluation License - If ISS is providing Licensee with the Software, security content and related documentation on an evaluation trial basis at no cost, such license Term is 30 days from installation, unless a longer period is agreed to in writing by ISS. ISS recommends using Software and security content for evaluation in a non-production, test environment. The following terms of this Section 5 additionally apply and supercede any conflicting provisions herein. Licensee agrees to remove or disable the Software and security content from the authorized platform and return the Software, security content and documentation to ISS upon expiration of the evaluation Term unless otherwise agreed by the parties in writing. ISS has no obligation to provide support, maintenance, upgrades, modifications, or new releases to the Software or security content under evaluation. **LICENSEE AGREES THAT THE EVALUATION SOFTWARE, SECURITY CONTENT AND RELATED DOCUMENTATION ARE BEING DELIVERED AS IS FOR TEST AND EVALUATION PURPOSES ONLY WITHOUT WARRANTIES OF ANY KIND, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OF NONINFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT WILL ISS BE LIABLE TO LICENSEE OR ANY OTHER PERSON FOR DAMAGES, DIRECT**

OR INDIRECT, OF ANY NATURE, OR EXPENSES INCURRED BY LICENSEE. LICENSEES SOLE AND EXCLUSIVE REMEDY SHALL BE TO TERMINATE THE EVALUATION LICENSE BY WRITTEN NOTICE TO ISS.

6. Covenants - ISS reserves all intellectual property rights in the Software, security content and Beta Products. Licensee agrees: (i) the Software, security content or Beta Products is owned by ISS and/or its licensors, is a valuable trade secret of ISS, and is protected by copyright laws and international treaty provisions; (ii) to take all reasonable precautions to protect the Software, security content or Beta Product from unauthorized access, disclosure, copying or use; (iii) not to modify, adapt, translate, reverse engineer, decompile, disassemble, or otherwise attempt to discover the source code of the Software, security content or Beta Product; (iv) not to use ISS trademarks; (v) to reproduce all of ISS and its licensors copyright notices on any copies of the Software, security content or Beta Product; and (vi) not to transfer, lease, assign, sublicense, or distribute the Software, security content or Beta Product or make it available for time-sharing, service bureau, managed services offering, or on-line use.
7. Support and Maintenance - Depending upon what maintenance programs Licensee has purchased, ISS will provide maintenance, during the period for which Licensee has paid the applicable maintenance fees, in accordance with its prevailing Maintenance and Support Policy that is available at http://documents.iss.net/maintenance_policy.pdf. Any supplemental Software code or related materials that ISS provides to Licensee as part of any support and maintenance service are to be considered part of the Software and are subject to the terms and conditions of this License, unless otherwise specified.
8. Limited Warranty - The commencement date of this limited warranty is the date on which ISS provides Licensee with access to the Software. For a period of ninety (90) days after the commencement date or for the Term (whichever is less), ISS warrants that the Software or security content will conform to material operational specifications described in its then current documentation. However, this limited warranty shall not apply unless (i) the Software or security content is installed, implemented, and operated in accordance with all written instructions and documentation supplied by ISS, (ii) Licensee notifies ISS in writing of any nonconformity within the warranty period, and (iii) Licensee has promptly and properly installed all corrections, new versions, and updates made available by ISS to Licensee. Furthermore, this limited warranty shall not apply to nonconformities arising from any of the following: (i) misuse of the Software or security content, (ii) modification of the Software or security content, (iii) failure by Licensee to utilize compatible computer and networking hardware and software, or (iv) interaction with software or firmware not provided by ISS. If Licensee timely notifies ISS in writing of any such nonconformity, then ISS shall repair or replace the Software or security content or, if ISS determines that repair or replacement is impractical, ISS may terminate the applicable licenses and refund the applicable license fees, as the sole and exclusive remedies of Licensee for such nonconformity. **THIS WARRANTY GIVES LICENSEE SPECIFIC LEGAL RIGHTS, AND LICENSEE MAY ALSO HAVE OTHER RIGHTS THAT VARY FROM JURISDICTION TO JURISDICTION. ISS DOES NOT WARRANT THAT THE SOFTWARE OR THE SECURITY CONTENT WILL MEET LICENSEE'S REQUIREMENTS, THAT THE OPERATION OF THE SOFTWARE OR SECURITY CONTENT WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT ALL SOFTWARE OR SECURITY CONTENT ERRORS WILL BE CORRECTED. LICENSEE UNDERSTANDS AND AGREES THAT THE SOFTWARE AND THE SECURITY CONTENT ARE NO GUARANTEE AGAINST UNSOLICITED E-MAILS, UNDESIRABLE INTERNET CONTENT, INTRUSIONS, VIRUSES, TROJAN HORSES, WORMS, TIME BOMBS, CANCELBOTS OR OTHER SIMILAR HARMFUL OR DELETERIOUS PROGRAMMING ROUTINES AFFECTING LICENSEE'S NETWORK, OR THAT ALL SECURITY THREATS AND VULNERABILITIES, UNSOLICITED E-MAILS OR UNDESIRABLE INTERNET CONTENT WILL BE DETECTED OR THAT THE PERFORMANCE OF THE SOFTWARE AND SECURITY CONTENT WILL RENDER LICENSEES SYSTEMS INVULNERABLE TO SECURITY BREACHES. THE REMEDIES SET OUT IN THIS SECTION 8 ARE THE SOLE AND EXCLUSIVE REMEDIES FOR BREACH OF THIS LIMITED WARRANTY.**
9. Warranty Disclaimer - **EXCEPT FOR THE LIMITED WARRANTY PROVIDED ABOVE, THE SOFTWARE AND SECURITY CONTENT ARE EACH PROVIDED AS IS AND ISS HEREBY DISCLAIMS ALL WARRANTIES, BOTH EXPRESS AND IMPLIED, INCLUDING IMPLIED WARRANTIES RESPECTING MERCHANTABILITY, TITLE, NONINFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE. LICENSEE EXPRESSLY ACKNOWLEDGES THAT NO REPRESENTATIONS OTHER THAN THOSE CONTAINED IN THIS LICENSE HAVE BEEN MADE REGARDING THE GOODS OR SERVICES TO BE PROVIDED HEREUNDER, AND THAT LICENSEE HAS NOT RELIED ON ANY REPRESENTATION NOT EXPRESSLY SET OUT IN THIS LICENSE.**
10. Proprietary Rights - ISS represents and warrants that ISS has the authority to license the rights to the Software and security content that are granted herein. ISS shall defend and indemnify Licensee from any final award of costs and damages against Licensee for any actions based on infringement of any U.S. copyright, trade secret, or patent as a result of the use or distribution of a current, unmodified version of the Software and security content, but only if ISS is promptly notified in writing of any such suit or claim, and only if Licensee permits ISS to defend, compromise, or settle same, and only if Licensee provides all available information and reasonable assistance. In any such suit, if the use of the alleged infringing intellectual property is held to constitute an infringement and is enjoined, or if in light of any claim, ISS deems it reasonably advisable to do so, ISS may at ISS sole option: (i) procure the right to continue the use of such Software and security content for Licensee; (ii) replace or modify such Software and security content in a manner such that such Software and security content are free of the infringement claim; or (iii) require Licensee to return the same to ISS and ISS shall refund the fees paid for the affected Software, security content or portion thereof, less amortization for use (A) on a straight line basis over a period of three (3) years from the effective date of the applicable order for a perpetual license, or (B) on a straight line basis over the subscription term for a term license. The foregoing is the exclusive remedy of Licensee and states the entire liability of ISS with respect to claims of infringement or misappropriation relating to the Software and security content.
11. Limitation of Liability - **ISS' ENTIRE LIABILITY FOR MONETARY DAMAGES ARISING OUT OF THIS LICENSE SHALL BE LIMITED TO THE AMOUNT OF THE LICENSE FEES ACTUALLY PAID BY LICENSEE UNDER THIS LICENSE, PRORATED OVER A THREE-YEAR TERM FROM THE DATE LICENSEE RECEIVED THE SOFTWARE. OR SECURITY CONTENT, AS APPLICABLE, IN NO EVENT SHALL ISS BE LIABLE TO LICENSEE UNDER ANY THEORY INCLUDING CONTRACT AND TORT (INCLUDING NEGLIGENCE AND STRICT PRODUCTS LIABILITY) FOR ANY SPECIAL, PUNITIVE, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING, BUT NOT LIMITED TO, COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, DAMAGES FOR LOST PROFITS, LOSS OF DATA, LOSS OF USE, OR COMPUTER HARDWARE MALFUNCTION, EVEN IF ISS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.**
12. Termination - Licensee may terminate this License at any time by notifying ISS in writing. All rights granted under this License will terminate immediately, without prior written notice from ISS, at the end of the term of the License, if not perpetual. If Licensee fails to comply with any provisions of this License, ISS may immediately terminate this License if such default has not been cured within ten (10) days following written notice of default to Licensee. Upon termination or expiration of a license for Software, Licensee shall cease all use of such Software, including Software pre-installed on ISS hardware, and destroy all copies of the Software and associated documentation. Termination of this License shall not relieve Licensee of its obligation to pay all fees incurred prior to such termination and shall not limit either party from pursuing any other remedies available to it.
13. General Provisions - This License, together with the identification of the Software and/or security content, pricing and payment terms stated in the applicable ISS quotation and Licensee purchase order (if applicable) as accepted by ISS, constitute the entire agreement between the parties respecting its subject matter. Standard and other additional terms or conditions contained in any purchase order or similar document are hereby expressly rejected and shall have no force or effect. If Licensee has not already downloaded the Software, security content and documentation, then it is available for download at http://www.iss.net/download/. All ISS hardware with pre-installed Software and any other products not delivered by download are delivered f.o.b. origin. This License will be governed by the substantive laws of the State of Georgia, USA, excluding the application of its conflicts of law rules. This License will not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded. If any part of this License is found void or unenforceable, it will not affect the validity of the balance of the License, which shall remain valid and enforceable according to its terms. This License may only be modified in writing signed by an authorized officer of ISS.
14. Notice to United States Government End Users - Licensee acknowledges that any Software and security content furnished under this License is commercial computer software and any documentation is commercial technical data developed at private expense and is provided with **RESTRICTED RIGHTS**. Any use, modification, reproduction, display, release, duplication or disclosure of this commercial computer software by the United States Government or its agencies is subject to the terms, conditions and restrictions of this License in accordance with the United States Federal Acquisition Regulations at 48 C.F.R. Section 12.212 and DFAR Subsection 227.7202-3 and Clause 252.227-7015 or applicable subsequent regulations. Contractor/manufacturer is Internet Security Systems, Inc., 6303 Barfield Road, Atlanta, GA 30328, USA.
15. Export and Import Controls; Use Restrictions - Licensee will not transfer, export, or reexport the Software, security content, Beta Products, any related technology, or any direct product of either except in full compliance with the export controls administered by the United States and other countries and any applicable import and use restrictions. Licensee agrees that it will not export or reexport such items to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Commerce Department's Denied Persons List or Entity List or such additional lists as may be issued by the U.S. Government from time to time, or to any country to which the United States has embargoed the export of goods or for use with chemical or biological weapons, sensitive nuclear end-uses, or missiles. Licensee represents and warrants that it is not located in, under control of, or a national or resident of any such country or on any such list. Many ISS software products include encryption and export outside of the United States or Canada is strictly controlled by U.S. laws and regulations. ISS makes its current export classification information available at http://www.iss.net/export. Please contact ISS' Sourcing and Fulfillment for export questions relating to the Software or security content (fulfillment@iss.net). Licensee understands that the foregoing obligations are U.S. legal requirements and agrees that they shall survive any term or termination of this License.
16. Authority - Because the Software is designed to test or monitor the security of computer network systems and may disclose or create problems in the operation of the systems tested, Licensee and the persons acting for Licensee represent and warrant that: (a) they are fully authorized by the Licensee and the owners of the computer network for which the Software is licensed to enter into this License and to obtain and operate the Software in order to test and monitor that computer network; (b) the Licensee and the owners of that computer network understand and accept the risks involved; and (c) the Licensee shall procure and use the Software in accordance with all applicable laws, regulations and rules.
17. Disclaimers - Licensee acknowledges that some of the Software and security content is designed to test the security of computer networks and may disclose or create problems in the operation of the systems tested. Licensee further acknowledges that neither the Software nor security content is fault tolerant or designed or intended for use in hazardous environments requiring fail-safe operation, including, but not limited to, aircraft navigation, air traffic control systems, weapon systems, life-support systems, nuclear facilities, or any other applications in which the failure of the Software and security content could lead to death or personal injury, or severe physical or property damage. ISS disclaims any implied warranty of fitness for High Risk Use. Licensee accepts the risk associated with the foregoing disclaimers and hereby waives all rights, remedies, and causes of action against ISS and releases ISS from all liabilities arising therefrom.

18. Confidentiality - “Confidential Information” means all information proprietary to a party or its suppliers that is marked as confidential. Each party acknowledges that during the term of this Agreement, it will be exposed to Confidential Information of the other party. The obligations of the party (“Receiving Party”) which receives Confidential Information of the other party (“Disclosing Party”) with respect to any particular portion of the Disclosing Party’s Confidential Information shall not attach or shall terminate when any of the following occurs: (i) it was in the public domain or generally available to the public at the time of disclosure to the Receiving Party, (ii) it entered the public domain or became generally available to the public through no fault of the Receiving Party subsequent to the time of disclosure to the Receiving Party, (iii) it was or is furnished to the Receiving Party by a third parting having the right to furnish it with no obligation of confidentiality to the Disclosing Party, or (iv) it was independently developed by the Receiving Party by individuals not having access to the Confidential Information of the Disclosing Party. Each party acknowledges that the use or disclosure of Confidential Information of the Disclosing Party in violation of this License could severely and irreparably damage the economic interests of the Disclosing Party. The Receiving Party agrees not to disclose or use any Confidential Information of the Disclosing Party in violation of this License and to use Confidential Information of the Disclosing Party solely for the purposes of this License. Upon demand by the Disclosing Party and, in any event, upon expiration or termination of this License, the Receiving Party shall return to the Disclosing Party all copies of the Disclosing Party’s Confidential Information in the Receiving Party’s possession or control and destroy all derivatives and other vestiges of the Disclosing Party’s Confidential Information obtained or created by the Disclosing Party. All Confidential Information of the Disclosing Party shall remain the exclusive property of the Disclosing Party.
19. Compliance - From time to time, ISS may request Licensee to provide a certification that the Software and security content is being used in accordance with the terms of this License. If so requested, Licensee shall verify its compliance and deliver its certification within forty-five (45) days of the request. The certification shall state Licensees compliance or non-compliance, including the extent of any non-compliance. ISS may also, at any time, upon thirty (30) days prior written notice, at its own expense appoint a nationally recognized software use auditor, to whom Licensee has no reasonable objection, to audit and examine use and records at Licensee offices during normal business hours, solely for the purpose of confirming that Licensees use of the Software and security content is in compliance with the terms of this License. ISS will use commercially reasonable efforts to have such audit conducted in a manner such that it will not unreasonably interfere with the normal business operations of Licensee. If such audit should reveal that use of the Software or security content has been expanded beyond the scope of use and/or the number of authorized devices or Licensee certifies such non-compliance, ISS shall have the right to charge Licensee the applicable current list prices required to bring Licensee in compliance with its obligations hereunder with respect to its current use of the Software and security content. In addition to the foregoing, ISS may pursue any other rights and remedies it may have at law, in equity or under this License.
20. Data Protection - The data needed to process this transaction will be stored by ISS and may be forwarded to companies affiliated with ISS and possibly to Licensees vendor within the framework of processing Licensees order. All personal data will be treated confidentially.

Revised October 7, 2005.