INTERNET
SECURITY
SYSTEMS®

INTERNET|SECURITY|SYSTEMS®

proventia® network

Intrusion Detection System

A Appliance Upgrade Guide

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

December 1, 2006

Contents

Preface

Overview

Introduction

This guide is designed to help you install firmware update 1.4 on your Proventia Network IDS A appliance. It also describes configuring the Proventia Manager, the local management interface, and setting up SiteProtector management for the appliance. Finally, it offers a brief walk-through of some of the new features available in this firmware update.

Scope

This guide describes how to update and configure the appliance models A201, A604, and A1204. It also includes initial appliance setup procedures.

Additional documentation is located on the ISS Web site at http://www.iss.net/support/documentation.

Audience

This guide is intended for network security system administrators responsible for installing and configuring Proventia Network IDS A appliances. 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 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 A 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 and AX Appliance User Guide	Information about configuring policies and managing appliance settings.
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

Installing the Update

Overview

Introduction

This chapter explains how to install or upgrade the Proventia Network IDS A appliance firmware.

In this chapter

This chapter contains the following topics:

About the Firmware Update

Introduction

To update the Proventia A appliance, you must download Firmware Update 1.4 onto a CD from the Download Center on the ISS Web site at http://www.iss.net/download. Once you have downloaded the update, you can do one of the following:

- Perform a complete reinstallation.
- Upgrade the appliance locally by connecting the appliance directly to a monitor and keyboard (or to a computer through a serial connection).
- Upgrade the appliance remotely from a computer at another location.

Important: Before you update the firmware, you must unregister the appliance from the SiteProtector Console and remove the host.

Preserved settings

When you upgrade the appliance firmware, the following settings are preserved:

- Root and admin passwords
- Management port IP settings
- Host name and DNS settings
- Appliance name
- Time, date, and time zone settings
- Link speed and duplex settings for management, monitoring, and TCPReset (RSKill) ports
- TCPReset (RSKill) configuration

Important: If you choose to reinstall the image, rather than perform the upgrade, your current settings are deleted.

Prerequisites

Before you update the appliance to the latest firmware version, note the following prerequisites:

Prerequisite	Description
Java 1.5	You must have Java installed in order to run Proventia Manager, the local management interface for the appliance. If you have not installed Java, the first time you access Proventia Manager, it prompts you to install this program.
Internet Explorer 6.0 or later	You must have Internet Explorer 6.0 or later installed on any computer from which you plan to access Proventia Manager. **Note:** To access Proventia Manager, turn off all proxy settings in your browser and disable pop-up blockers.
Current network information	You must gather your current network settings if you plan to reinstall the appliance image. You must provide this information when you configure the appliance. The upgrade process preserves your network settings for the appliance, but ensure you have this information on hand in case you need it.
Correct TCP/IP settings	Ask your network administrator.

Table 6: *Prerequisites*

Prerequisite	Description
A valid license	You may use your current Proventia A license number to install the firmware update.

Table 6: *Prerequisites*

Setup overview

The Proventia A setup is a 10-step process, as follows:

Step	Description
1	Download the firmware update 1.4 from the ISS Download Center and copy it to a CD.
2	Install the update or upgrade the current firmware. **Reference**: Depending on how you choose to install the update, see one of the following: • "Performing a New Installation" on page 15 • "Applying the Update Locally" on page 16 • "Applying the Update Remotely" on page 17
3	Gather network information. **Reference**: "Information checklist" on page 20
4	Log in to Proventia Setup and configure the appliance settings. If you choose to upgrade the appliance, you only have to change the Proventia Manager password. **Reference**: "Completing the Initial Configuration" on page 20
5	Verify you have the following programs installed on any computer where you will access Proventia Manager: • Internet Explorer version 6.0 or later • Java Runtime Environment (JRE) version 1.5.
6	Log in to Proventia Manager as user name **admin** and the password you configured during Proventia Setup. **Reference**: "Accessing Proventia Manager" on page 29
7	Contact your Sales Representative for your license registration number. Do the following: 1. Register your customer license at the ISS License Registration center (https://www1.iss.net/cgi-bin/lrc). 2. Download the license key file from the ISS Registration Center to your computer. **Note:** ISS recommends that you upload the license key file to a designated directory so that the appliance can download and install the latest updates automatically. 3. Upload the license when you log in to Proventia Manager, when prompted.
8	Apply security updates. **Reference**: "Updating the Appliance Manually" on page 40
9	(Optional) If you plan to manage the appliance with SiteProtector, install the SiteProtector Database Service Pack (DBSP) associated with this release. **Reference**: SiteProtector DBSP Readme
10	(Optional) Register the appliance with SiteProtector. **Reference**: "Configuring SiteProtector Management" on page 46

Table 7: *Setup process*

Connecting to the Appliance

Introduction

If you are performing a new installation or upgrading the appliance firmware locally, you may need to establish a remote connection to the appliance to complete the installation and configuration steps. You can connect a computer directly to the appliance, or you can access the appliance through a computer on the network. The following procedure describes how to establish a remote connection to the appliance using Hyperterminal.

Procedure

To establish a remote connection 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.

Performing a New Installation

Introduction

When you reinstall the Proventia A firmware on the appliance, the installation program deletes current network information and settings on the appliance. ISS recommends that you perform a new installation to ensure complete transition to the new features included in the firmware update.

Important: Before you install the firmware update, you must unregister the appliance with the SiteProtector Console and remove the host.

Installing the update

To perform a new installation:

1. Download the firmware update from the ISS Download Center and copy it to a CD.
2. Remove the bezel cover on the front of the appliance.
3. Connect to the appliance one of the following ways:
   - Connect a keyboard and a monitor directly to the appliance.
   - Connect the appliance to a computer, and then use a terminal emulation program such as Hyperterminal to create a connection to the appliance. See "Connecting to the Appliance" on page 14 for more information.
4. Insert the CD in the appliance or computer, and then restart the appliance.

   Tip: If the appliance does not respond, you may need to shut off the appliance physically, and then turn it on again.
5. At the **`boot`** prompt, type `reinstall`, and then press ENTER.

   The appliance reloads the operating system, displays installation status messages, ejects the CD, and then restarts.
6. At the **`unconfigured login`** prompt, type the user name `admin`, and press `Enter`.
7. Type the default password `admin`, and then press ENTER.
8. You are ready to configure the appliance. Proceed to "Completing the Initial Configuration" on page 20.

Applying the Update Locally

Introduction

You can apply the update directly to the appliance by establishing a physical connection one of the following ways:

- Attaching a keyboard and monitor directly to the appliance
- Connecting a computer to the appliance through a serial connection

Procedure

To apply the update locally:

1. Download the Firmware Update from the ISS Download Center and copy it to a CD.
2. Attach a monitor and keyboard to the appliance or connect the appliance to a computer and establish a serial connection.
3. Remove the bezel cover.
4. Establish a remote connection with the appliance. See "Connecting to the Appliance" on page 14 for more information.
5. Insert the CD where you copied the update, and then start the appliance
6. At the prompt, type **`upgrade`**.

   The update program installs the new image, and then ejects the CD and restarts the appliance.

   Note: The update process verifies that the appliance qualifies for the upgrade. If it does not, an error message appears, and the appliance exits the process.
7. Establish a Proventia Manager password. Proventia Manager is the browser-based local management interface for the appliance that enables you to manage policies, view events, and configure appliance updates. You also use the Proventia Manager to register the appliance with SiteProtector.

   See "Completing the Initial Configuration" on page 20 for more information about setting a Proventia Manager password.

Applying the Update Remotely

Introduction

If you cannot gain physical access to the appliance, you can install the update from a remote computer by establishing a secure shell (SSH) connection to the appliance using a terminal emulation such as PuTTY.

Applying the update

To apply the firmware update remotely:

1. Download the Firmware Update from the ISS Download Center and copy it to a CD.
2. Insert the CD into the CD-ROM drive of a computer on your network and browse to the `\upgrade` directory on the CD.
3. Select and transfer the following files from the upgrade directory on the CD where you saved the update to the `/` directory on the appliance you want to upgrade:

   Tip: Use a transfer program such as SCP to facilitate the transfer. SCP is an open source Secure File Transfer Protocol (SFTP).

Use this file...	to upgrade...
upgrade_A201.tgz	Proventia A201 appliance
upgrade_A604.tgz	Proventia A604 appliance
upgrade_A1204.tgz	Proventia A1204 appliance

4. Establish a Secure Shell (SSH) connection to the appliance and login as the root user.
5. Type `cd /` to access the `/` directory, and then type one of the following commands to extract the update files:
   - Proventia A201 appliance: `tar -xzvpf upgrade_A210.tgz`
   - Proventia A604 appliance: `tar -xzvpf upgrade_A604.tgz`
   - Proventia A1204 appliance: `tar -xzvpf upgrade_A1204.tgz`
6. Type `./remote_upgrade.sh` to run the remote_upgrade.sh script.

   Note: The update process verifies that the appliance qualifies for the upgrade. If it does not, an error message appears, and the appliance exits the process.

   The update process proceeds through the following steps:
   - Verifies the checksum of the install files
   - Verifies the appliance model name matches the files

   The appliance restarts and the update process continues. This process takes about ten (10) minutes. You cannot access the appliance during this time.
7. When the appliance restarts for the second time, log in as user `admin`.
8. Establish a Proventia Manager password. Proventia Manager is the browser-based local management interface for the appliance that enables you to manage policies, view events, and configure appliance updates. You also use the Proventia Manager to register the appliance with SiteProtector.

   See “Completing the Initial Configuration” on page 20 for more information about setting a Proventia Manager password.

Chapter 2

Configuring the Appliance

Overview

Introduction

This chapter describes how to configure the Proventia A 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:

Completing the Initial Configuration

Introduction

If you reinstalled the appliance firmware, you must reconfigure the appliance settings.

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.

Information checklist

Use the checklist in Table 8 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 8: *Information checklist*

Procedure

To complete the initial configuration for the appliance:

1. At the unconfigured login prompt, type the user name **admin**, and then press ENTER.
2. At the password prompt, type one of the following:
   - If you reinstalled the appliance firmware, type the default password admin.
   - If you upgraded the appliance firmware, type the current appliance password.
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.

   Note: Use the TAB key to move between fields on the screen.

   The following table describes the required information.

Information	Description
Change Password	• **Admin Password**—To access the 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" in the *Proventia Network IDS A nd AX Appliance User Guide*.

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 9: *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 10: *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 10: *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 11: *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 12: *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 Proventia Network IPS 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” in the *Proventia Network IDS A and AX Appliance User Guide*.

Table 13: *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 14: *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" in the *Proventia Network IDS A and AX Appliance User Guide*.
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 15: *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 16: *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:

Before You Begin

Introduction

Once you have installed the update, you are ready to log in to the Proventia Manager to complete the final configuration steps and set up appliance management. The following table outlines these steps:

Step	Description
1	Contact your Sales Representative for the license registration number. Do the following: 1. Register your customer license at the ISS License Registration center (https://www1.iss.net/cgi-bin/lrc). 2. Download the license key file from the ISS Registration Center to your computer. **Note:** ISS recommends that you upload the license key file to a designated directory so the appliance can download and install the latest updates automatically. **Reference**: "Installing the license file" on page 32
2	Verify you have the following installed on the computer where you will run Proventia Manager: • Internet Explorer version 6.0 or later • Java Runtime Environment (JRE) version 1.5. The application prompts you with an installation link if you do not have it installed.
3	Log in to Proventia Manager. **Reference**: "Logging on to Proventia Manager" on page 29
4	Install license. **Reference**: "Installing the license file" on page 32
5	Apply updates. **Reference**: "Updating the Appliance" on page 35

Table 17: *Setting up Proventia Manager*

Verifying setup

Verify that you have logged on to Proventia Setup and configured (or confirmed) the following settings:

- admin, root, and Proventia Manager passwords
- network settings
- time and date

After you install the license file, ISS recommends that you perform the following tasks:

- view your component status on the Home page
- update the firmware
- configure update settings
- configure and update intrusion detection settings
- configure packet filters

Reference: You will find procedures for configuring intrusion detection settings and packet filters in the *Proventia Network IDS A and AX Appliance User Guide*.

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
- view events

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 do not have Java Runtime Environment (JRE) installed, 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 are planning 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 18: *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. See the *Proventia Network IDS A and AX Appliance User Guide* for more information about the features listed here.

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.
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 information and determine how the appliance should respond when it detects intrusions.
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.
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.
Statistics	The Statistics area lets you view important statistics about appliance activity, such as Protection, Packet, and Driver 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.
Support	The Support area provides contact information for Technical Support, as well as helpful links to provide you assistance with the appliance.

Table 19: *Left navigation pane*

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 will 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 20: *Proventia Manager policy icons*

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 will not be prompted to save before you click the new link.

Installing the License File

Introduction

Proventia A appliances require a properly configured license file. If you have not installed the appropriate license file, you will not be able to manage the appliance.

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

About the Licensing page

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.

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 current status of the appliance. This page includes the following navigation, information and reporting options:

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

Viewing protection status

The protection 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:

Icon	Description
	Indicates that the component is active.
	Indicates that the component is stopped.
	Indicates that the component is in an unknown state. This status may require immediate attention.

Table 21: *Protection status icons*

Viewing system status

On the Home page, the system status group box describes the current status of the system.

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 22: *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 22: *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 security 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 Network IPS and IDS Firmware 1.4 Feature Upgrade 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 security 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.

You enable updates through the X-Press Update Server through Update Advanced Parameters. For more information, see the *Proventia Network IDS A and AX Appliance User Guide*. See the SiteProtector documentation or online help for further information about configuring the X-Press Update Server. 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 detection 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 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

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 23: *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 40 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 has completed 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 Network IPS and IDS Firmware 1.4 Feature Upgrade 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 that was 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 security update version 1.81 but do not install version 1.82, and then you install version 1.83, version 1.82 is installed with version 1.83.

However, if you roll back from version 1.83, the appliance does not rollback to version 1.82. A rollback to the last applied update takes the appliance back to version 1.81.

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 38.

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.

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.

Caution: You must install the SiteProtector DBSP that accompanies this release before you register the appliance with SiteProtector.

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

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 become 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 filter rules enabled.

At the second heartbeat and each heartbeat thereafter, the Agent Manager "pushes" the group policy to the appliance. However, you can still change policy settings on local appliances. Any local policy settings you change on a specific appliance take precedence over the group policy settings *for that appliance only*; the group policy is unaffected by these changes, and its settings remain in effect for all other appliances in the group.

How appliance updates work with SiteProtector

After 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

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
- edit group policies
- edit policies for a single appliance within a group

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.

After you have registered your appliance, you must add the Proventia A license file in SiteProtector. This enables you to receive automatic updates. 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 or later.

Before registering the appliance

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

- If you have recently update the appliance firmware, ensure you have installed the latest SiteProtector DBSP.
- 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 59 for more information.

Configuring SiteProtector management

To configure SiteProtector management:

Caution: You must install the SiteProtector DBSP that accompanies this release before you register the appliance with SiteProtector.

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.
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-Series 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.

Setting	Description
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 the appliance, it appears in the default group "A-Series." If you cleared the default group and did not specify a new one, 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. For information about the polices and settings listed below, see the *Proventia Network IDS A and AX Appliance User Guide*.

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 network intrusions. You can also view important security alerts and determine how the appliance should respond to detected intrusions.
Packet Filters	Create and edit packet filter rules to filter out packets you do not want the appliance to monitor.
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
Statistics	View important statistics about appliance activity, such as Protection, Packet, and Driver information.
Updates	Configure and manage updates for a single appliance, so that you have the latest protection available for the network.

Table 24: *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.
	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 will each have their own group, making it easier for you to search for events.

Table 25: *Policy editor icons in SiteProtector*

Icon	Description
	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 25: *Policy editor icons in SiteProtector*

About saving changes

You should save your changes before you navigate to another policy. Click Save All on the Console toolbar to save your changes before navigating to a new policy.

Opening a policy in SiteProtector

To open a policy in SiteProtector:

1. In the SiteProtector Console, select a Site.
2. Do one of the following:
   - To edit a group level policy, right-click the group in the left pane of the main Console window, 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.
3. On the Policy tab, select Network IDS from the **Agent Type** drop-down menu.
4. 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.
5. Edit the policy as necessary.
6. Click **Save All** on the toolbar to save your changes.

Chapter 6

Working with Security Events: A Walk-Through

Overview

Introduction

This chapter describes some of the new features in the 1.4 release and explains how to create a security events policy using the new features. Detailed descriptions and procedures of the tasks listed in this chapter are available in the *Proventia Network IDS A and AX Appliance User Guide*.

In this chapter

This chapter contains the following topics:

About Intrusion Detection

Introduction

After you have installed the new features in the 1.4 release, you will find substantial differences in the way you create and edit your security policies. ISS strongly recommends that you adopt the new features for creating and managing your appliance policies, as these features ensure your network is monitored appropriately.

Intrusion detection

In the Proventia Network IDS Appliance 1.4 release, you will find the following new features:

- **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 and user-defined 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 monitor your network. You can define protection domains by ports, VLANs, or IP address ranges.

- **Security Events and Response Filters**

  The Security Events page in the Policy Editor lists hundreds of known attacks and security events against which you want to protect your network. 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 your active security policy, which you can edit to meet your network's needs.

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

Step 1: Creating an Email Response

Introduction

Creating responses is a logical first step in managing your security policy. Responses determine how the appliance reacts when it detects an event. You can configure different response types for different groups of events. Perhaps you want your Web Administrator to be aware of certain HTTP events that take place on your network. You set up an email response that automatically notifies your Web Administrator when HTTP events you have specified occur on your network.

Procedure

You want to create an email response for your Web Administrator, John Smith.

1. In the Proventia Manager, select **Intrusion Detection→Responses** in the left pane.

   Tip: In the SiteProtector Policy Editor, you select the appliance, and then select Response Objects.

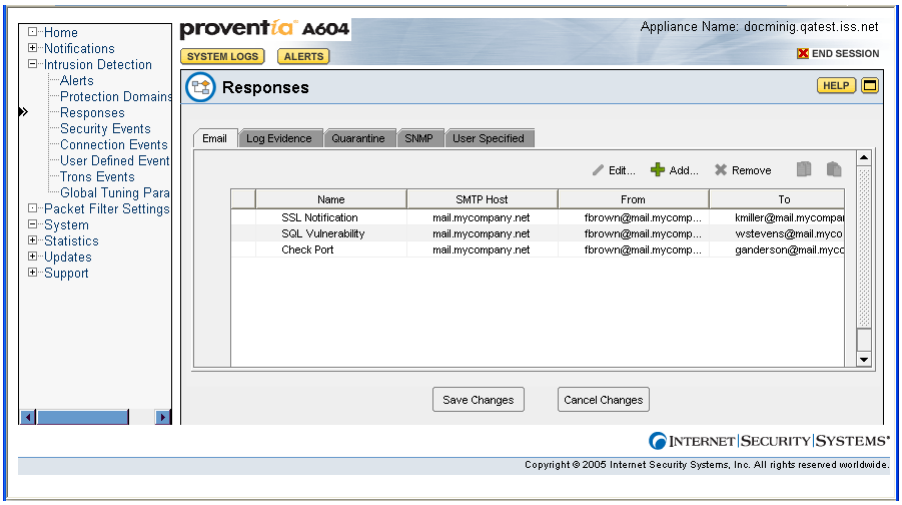

Figure 1: *Email Response tab*

2. Select the **Email** tab, and then click **Add**.

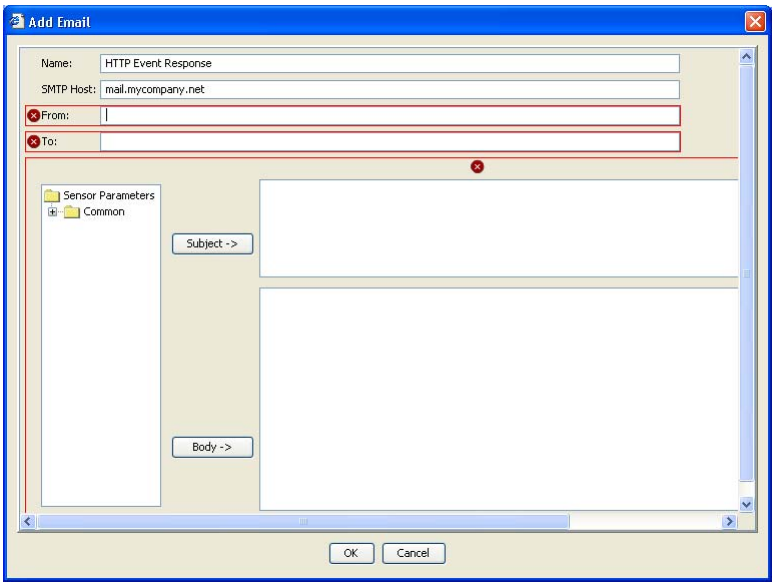

Figure 2: *Add Email dialog box*

3. In the Add Email dialog box, provide the following information:

Setting	Description
Name	You type a meaningful name for the response, such as “HTTP Event Response.”
SMTP Host	You type the fully qualified domain name (mail.mycompany.net) or IP address of the mail server.
From	You enter the email address for the person assigning this responsibility to John, the Web Administrator. You want his boss, Frank Brown, to appear as the sender, so you type “fbrown@mail.mycompany.net”
To	You enter the email address for the responsible party or parties. You want to send it to the Web Administrator, but also to his assistant, Susie Ellis. You type: “jsmith@mail.mycompany.net; sellis@mail.mycompany.net”
Sensor Parameters	You type a **Subject** and **Body** for the message. You can also select parameters to add to the message. You type the subject, “Suspicious HTTP event has occurred,” and then type a message. You add the date and time parameters, so John knows exactly when the event took place.

Step 2: Creating a Protection Domain

Introduction

After you create your email response, you want to create a protection domain. Maybe John is only concerned about HTTP events that take place on a certain part of the network. Protection domains act like virtual sensors, letting you create specific security event policies for specific network segments that you want to monitor more closely than others.

Procedure

1. In the Proventia Manager, select **Intrusion Detection→Protection Domains**.

   Tip: In the SiteProtector Policy Editor, you select the appliance, and then select **Protection Domains**.

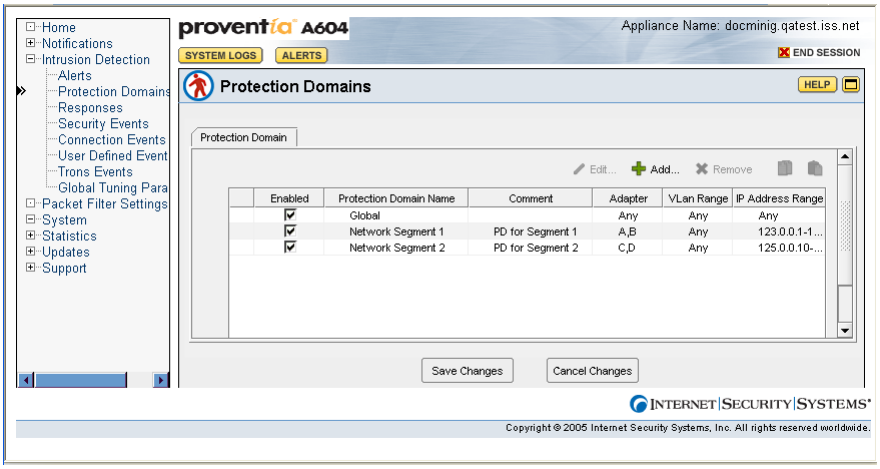

Figure 3: *Protection Domains tab*

1. On the Protection Domains page, click **Add**.

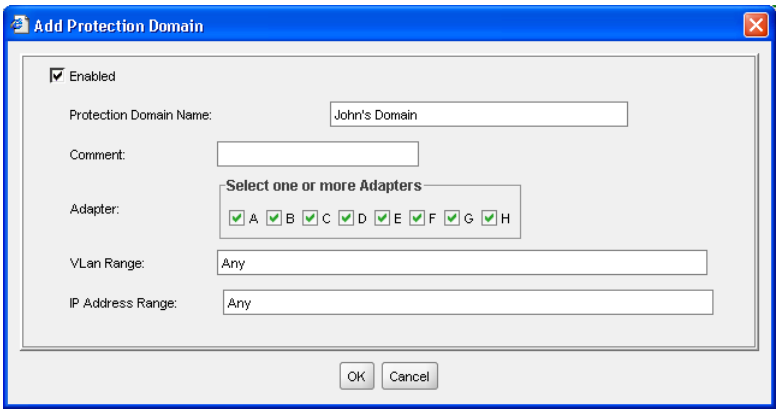

Figure 4: *Add Protection Domain dialog box*

2. In the Add Protection Domain dialog box, specify the following information:

Setting	Description
Enabled	You select this check box to enable the protection domain.
Protection Domain Name	You type a descriptive name for the domain. Call it “John’s Domain.”

Setting	Description
Comment	You type a unique description for the domain. You could type “John Smith’s network segment.”
Adapter	You select the appliance monitoring adapter or list of monitoring adapters for John’s domain.
VLAN Range	Here, you type the range of virtual LAN tags, but this setting does not apply to John’s domain.
IP Address Range	Instead you type the range of source and destination IP addresses for John’s domain: 127.0.0.1-127.0.0.10

3. When you have finished, your protection domain appears in the list.

Step 3: Selecting Security Events to Monitor

Introduction

After you define responses and protection domains, you are ready to select the security events you want to manage in this particular policy. You could scroll through the list and select each event you want to add to your policy—a time consuming operation. The best way to select events to add to your policy is to use the Select Columns, Group By, and Filter features. This allows you to create and manage smaller groups for which you want to define custom policies.

Procedure

1. In the Proventia Manager, select **Intrusion Detection→Security Events**.

   Tip: In the SiteProtector Policy Editor, select **Security Events**. Notice that the Security Events window lists thousands of events.

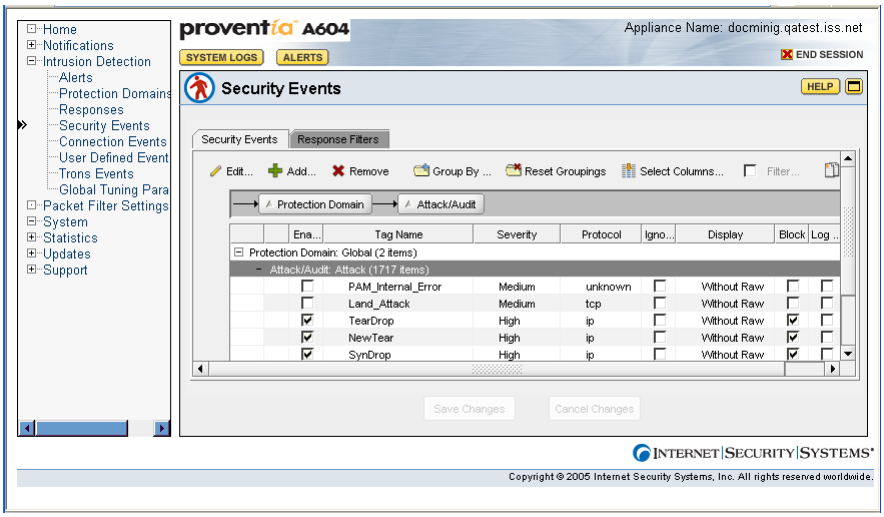

Figure 5: *Security Events list*

2. You can select security events several ways, but these are the best methods:

   - **Select Columns**

     You use this option to select the columns you want to appear on the Security Events page when you are managing security events.

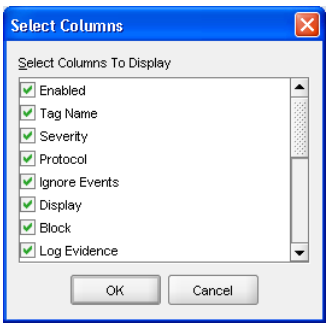

Figure 6: *Select columns dialog box*

- **Group By**

  After you have selected the columns you want to display, you can select this option to group events by column. For example, you may select the Severity column. This groups your events by severity level.

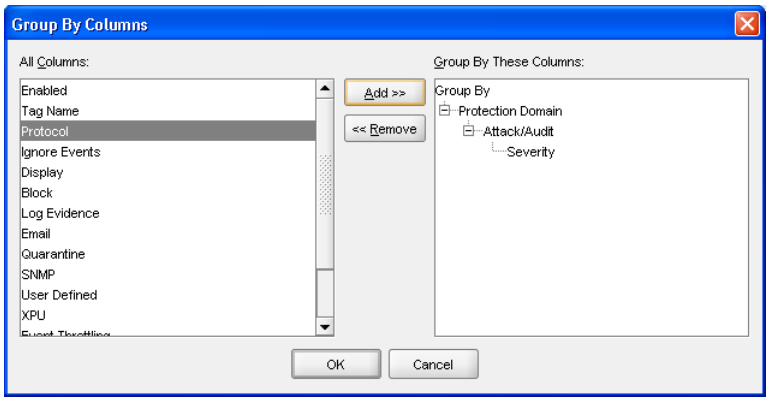

Figure 7: *Group By Columns dialog box*

- **Filters**

  You select this option to create an even more granular view of the events list. If you selected to group your events by severity level, you could filter the list even further by filtering the list so only High events appear.

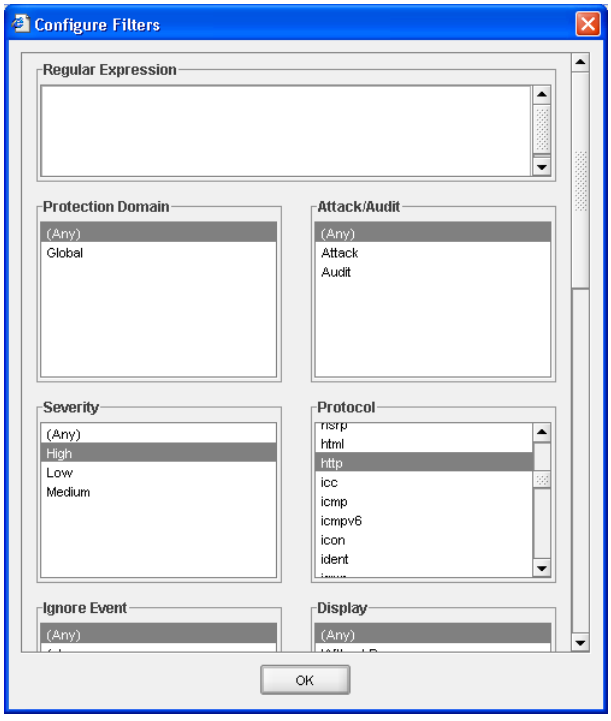

Figure 8: *Configure Filters dialog box*

Step 4: Editing Security Events

Introduction

After you customize your security events list, you are ready to edit the events most important to your policy. The first thing you want to do is add events to the protection domain you created in Step 2.

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 that 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 events 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.

In this example, you assign several HTTP events to the protection domain John's Domain. These HTTP events may also be enabled for the global domain. When the appliance detects an HTTP event occurring in John's Domain, it uses the setting for the event assigned to his domain. If the appliance detects the same HTTP event *outside* John's domain, the appliance uses the settings in the global policy.

Procedure

1. On the **Security Events** page, select the group of events you want to edit by selecting the parent row for the event list you want to edit. You selected to group and filter the list for high severity events only, so you select the Severity: High parent row, which automatically selects all the events in that list.

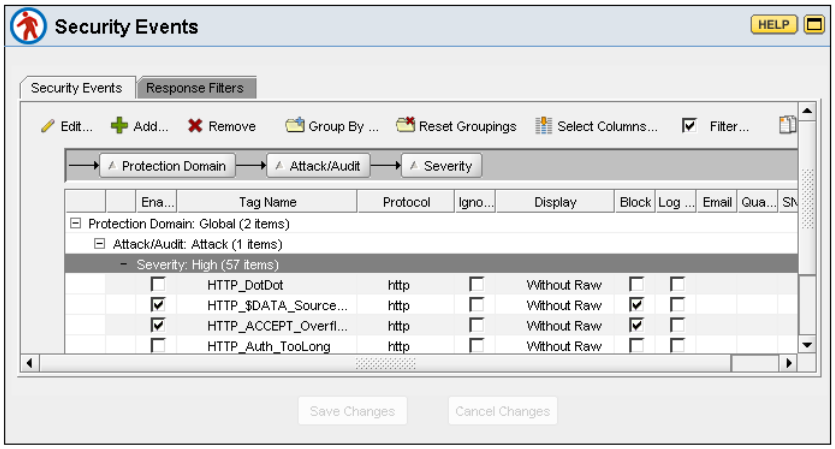

Figure 9: *Security Events page*

2. Click **Copy**, and then click **Paste**. This adds the filtered events to the list outside of the global protection domain.

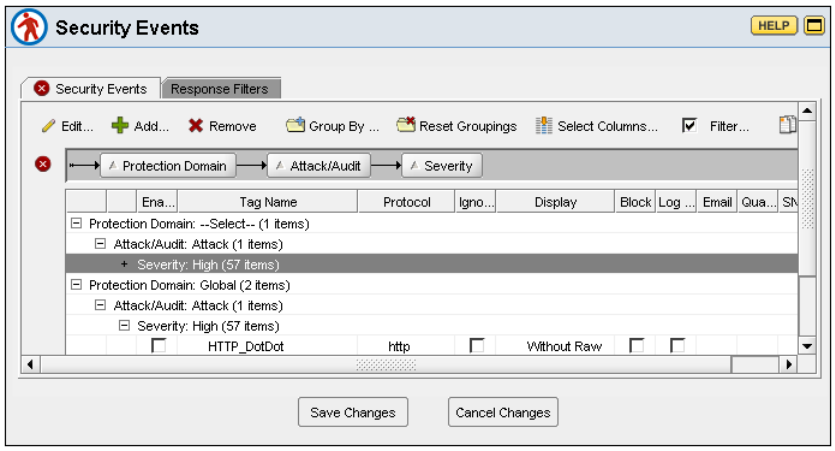

Figure 10: *Pasted security events*

3. Select the row you just pasted, and then click **Edit** to edit the event properties.

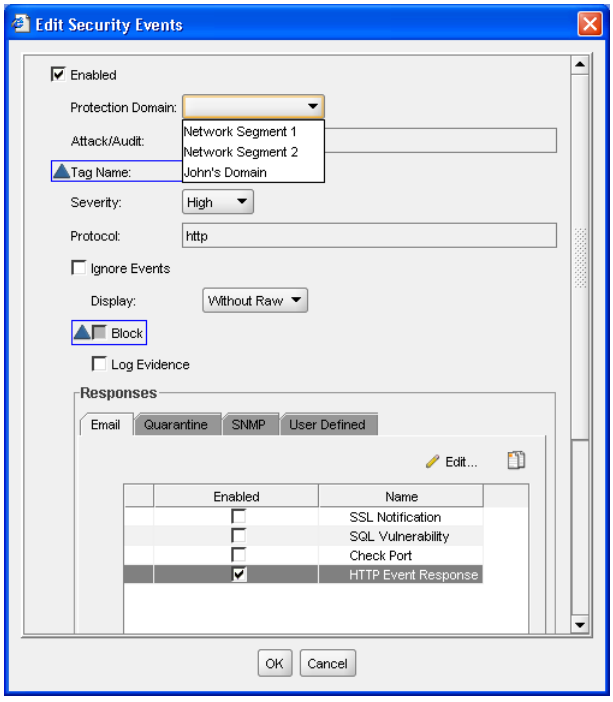

Figure 11: *Edit Security Events dialog box*

A blue triangle icon appears next to any item that has a different value in the selected events list. 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.

4. Select **Enabled** to enable the events in the list, and then select the **Protection Domain** "John's Domain" from the list.

   You can also edit or review the following event properties:

Setting	Description
Attack/Audit	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 your network. • Attack events match network traffic that seeks to harm your network. For security events you have edited, this area is read-only.
Tag Name	A unique descriptive name for the event. If you are editing an existing event, this field displays the event name, which is uneditable.
Severity	The severity level for the event: Low, Medium, or High.
Protocol	The event protocol. For existing events, this setting displays the protocol type and is read-only.
Ignore Events	Enables the appliance to ignore events that match the criteria set for this event.
Display	Determines how the event appears 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	Blocks TCP attacks only by sending a TCPReset (kill). All other event types are unaffected by the Block setting.
Log Evidence	Logs the packet that triggered the event to the /var/iss/ directory.
Responses	Lets you select responses for the event.
XPU	For existing events only, displays the XPU in which the vulnerability check was released. This setting is read-only.
Event Throttling	Event throttling enables you to reduce the number of events that match an attack are reported to the management console. Shows the event throttling interval (in seconds) enabled to reduce the number of events received. 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	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.

5. When you click **OK**, the security event policy you just created becomes active, as long as the events are enabled. Notice that the Security Events window is filtered by

Protection Domain, and John's Domain appears in the list with the other settings you applied.

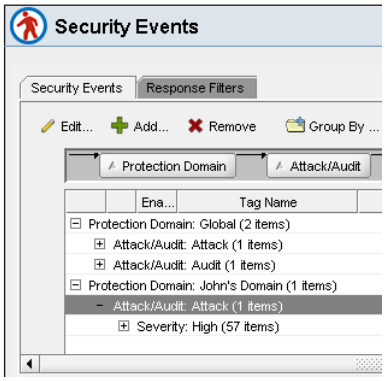

Figure 12: *Close-up of John's domain in Security Events list*

Step 5: Creating a Response Filter

Introduction

At some point, you may need to refine the security policy. Perhaps an FTP event has been occurring across a certain VLAN on John's domain, and you decide to track this activity for a few weeks. Rather than editing the entire security policy for all of John's domain, you can set up a response filter to monitor the event. When you are sure the event is no longer a problem, you can simply remove the filter.

Procedure

1. Select the **Response Filters** tab.

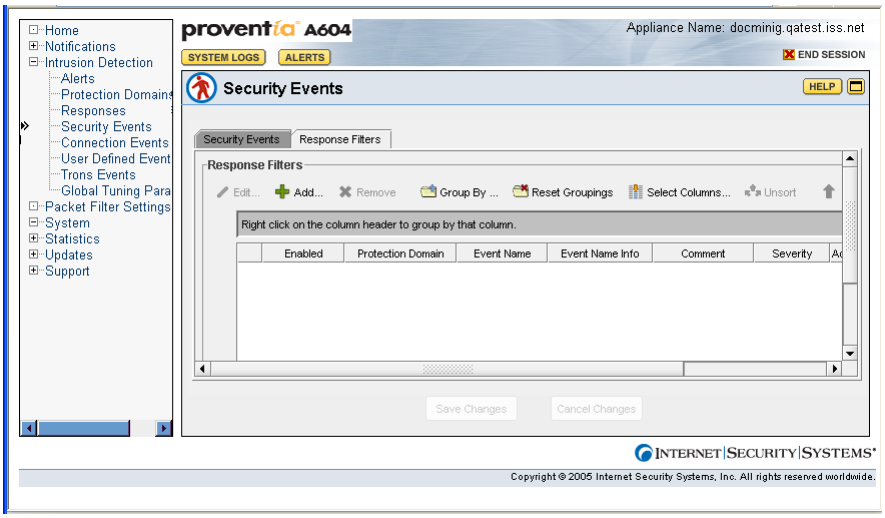

Figure 13: *Response Filters page*

2. Click **Add** to add the response filter.

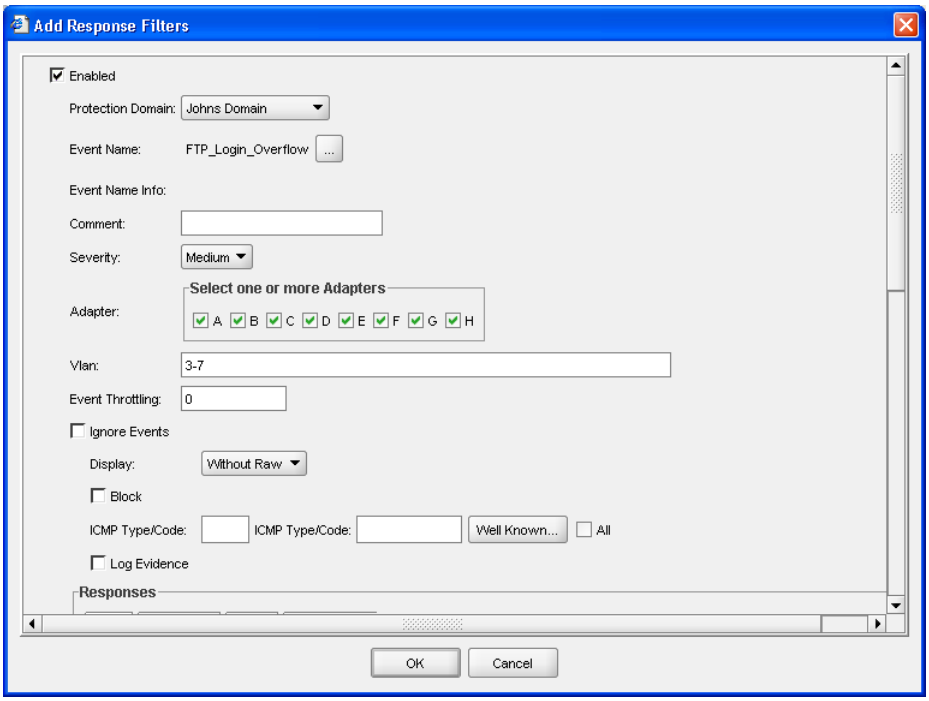

Figure 14: *Add Response Filters dialog box*

3. In the Add Response Filters dialog box, do the following:
   - Select John's domain as the **Protection Domain**.
   - Click the button to select an **Event Name**, and then select FTP_Login_Overflow from the list.
   - In the **VLAN** box, type 3-7. This tells the appliance which VLAN segments on the domain to monitor specifically for the event.

   You can also define the following response filter settings for events in your security policy:

Setting	Description
Enabled	The filter is enabled by default. You clear the check box to disable the filter.
Protection Domain	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	The event for which you want to filter responses. You can only select one event per filter.
Event Name Info	Additional information about the event, if any. This setting is read-only.
Comment	A unique description for the event filter.
Severity	The event's severity level: high, medium, or low.
Adapter	The appliance port(s) on which to apply the response filter.
VLAN	The range of virtual LAN tags where you can apply the response filter.
Event Throttling	Shows the event throttling interval (in seconds) enabled to reduce the number of events received.
Ignore Events	Enables the appliance to ignore events that match the criteria set for this event.
Display	Determines how events appear 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	Blocks TCP attacks only by sending a TCPReset (kill). All other event types are unaffected by the Block setting.
ICMP Type/Code	Specifies ICMP types or codes for either side of the packet, or click **Well Known** to select often-used types and codes.
Log Evidence	Logs the packet that triggered the event to the /var/iss/ directory.
Responses	Lets you select responses for the event.
IP Address and Port	Determines the Source and/or Target IP addresses or ports by which you want to filter.

4. The response filter you have set appears in the list. Notice that the event name appears as a link. If you click this link, a description of the event from the X-Force

Database appears that describes the signature or vulnerability, along with a default risk level, sensors that have the signature, affected systems, and the event type.

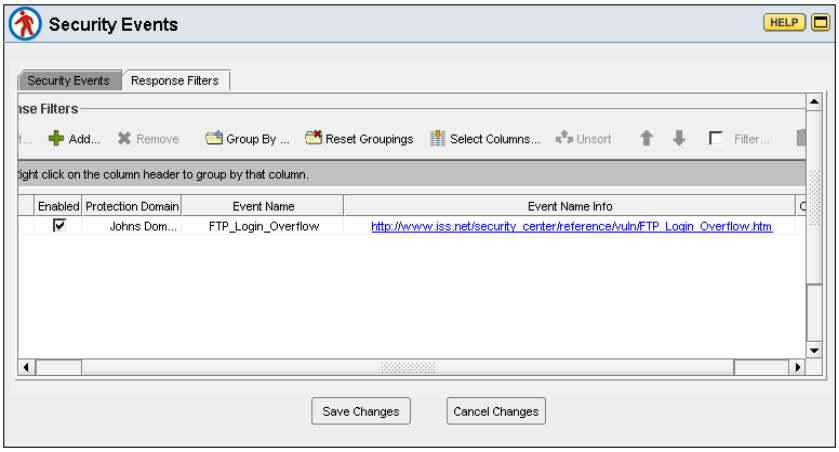

Figure 15: *Response Filters list*