INTERNET|SECURITY|SYSTEMS®

proventia®
intrusion prevention appliance

G Next Generation Installation and Upgrade Procedures

October 28, 2005

Overview

Introduction

This guide explains how to upgrade existing G Series model appliances to the Next Generation 1.2 release features. Use the procedures in this document to upgrade the following appliance models:

- Proventia G100
- Proventia G200
- Proventia G1000
- Proventia G1200

In this guide

This guide contains the following topics:

Related documentation

Refer to the *Proventia G Quick Start Card* or *Guide* that came with your appliance for hardware and cabling information specific to your appliance model. Refer to the *Proventia G Intrusion Prevention User Guide* or the Help for information about using the new features associated with this release.

Additional information about the Proventia G Intrusion Prevention Appliances is available on the ISS Web site at the following location: **Support→ Product Documentation→ Proventia G Intrusion Prevention Appliance** (http://www.iss.net/support/documentation) .

New G Intrusion Prevention Appliance Features

What's new in this release

This release offers enhanced functionality for older G Series appliances. This upgrade offers the following capabilities:

- Proventia Manager, a web-based local management interface
- Proventia Setup Assistant, an administrative configuration tool
- three adapter modes, configured at the adapter level
  - inline protection
  - inline simulation
  - passive monitoring
- enhanced firewall rules management
- improved granular policy implementation
- ability to view triggered events
- dynamic blocking is now quarantine response
- simplified blocking configuration
- TCP dump
- agent settings for processing traffic
- SNMP configuration (Simple Network Management Protocol)
- X-Force recommended blocking responses using Virtual Patch™ technology
- Network Time Protocol (NTP)
- perform diagnostics and gather statistics

Before you perform the upgrade

Note the following prerequisites:

Prerequisite	Where to find information
Backup your existing appliance	See "Creating a system backup" on page 13.
Verify that you have Java 1.4.2 installed on your computer	Proventia Manager will prompt you to install this required plug-in. See "Logging on to Proventia Manager" on page 20.
Verify that you have Internet Explorer 6.0 or later on your computer	Check your computer. In Internet Explorer, click **Help→About Internet Explorer**. **Note:** In order to access Proventia Manager, all proxy settings in your browser should be turned off and pop-up blockers disabled.
Obtain your network settings information	Ask your Network Administrator. Use the "Information checklist" on page 5.
Verify that your computer's TCP/IP settings are correct, depending on your network configuration.	Ask your network administrator.

Table 1: *Prerequisite to upgrading a G appliance*

Prerequisite	Where to find information
Obtain a license	Obtain a license registration number from your Sales representative and see “Logging on to Proventia Manager” on page 11.
Unregister the appliance from the SiteProtector console and remove the host	You must unregister the appliance before you upgrade. See your SiteProtector documentation.
Install the Agent Manager	See “What is the Agent Manager?” on page 4.

Table 1: *Prerequisite to upgrading a G appliance*

What is Proventia Setup?

The Proventia Setup is an administrator utility used to:

- configure the hostname
- configure network interfaces
- configure domain name system (DNS)
- set the time and date
- set the passwords for users:
  - root user (command line access)
default user name: root
default password: admin
  - administrative user appliance access (Proventia Setup)
default user name: admin
default password: admin
  - Proventia Manager user (web-based management interface access)
default user name: admin
default password: admin
- set port speeds and duplex settings
- set adapter mode (operation mode)

What is Proventia Manager?

Proventia Manager is the web-based local management interface. Use Proventia Manager to:

- monitor the status of the appliance
- automatically download and install updates
- change appliance settings
- configure firewall settings
- configure intrusion prevention settings
- configure system settings
- configure high availability (optional)
- manage appliance activities
- configure local and advanced parameters

What is the Agent Manager?

The Agent Manager (formerly Desktop Controller) allows SiteProtector to collect and manage data from agents and components. An Agent Manager is installed with all SiteProtector installation options.

Note: If you plan to use multiple Agent Managers, you must install each Agent Manager on a separate computer.

Why do I have to install Agent Manager?

The Agent Manager is now required to monitor all Proventia G appliance with Site Protector. If you do not upgrade to the new code base, an Agent Manager is not required.

Where do I install the Agent Manager?

The Agent Manager can be installed on Database Server or the SiteProtector console system. If you need to install more than one Agent Manager, you will need to install them on separate computers.

What is a protection domain?

A protection domain is a type of virtual sensor that is made up of a group of network assets or security events that monitor IP address, port paging, or VLAN. You use protection domains when you want to monitor groups of different network segments from a single appliance using global policies that centralize intrusion prevention.

You can also use protection domains to define and apply multiple protection domains to a single appliance, to apply multiple policies to a single appliance, which lets you tune the responses to specific network traffic on one or more networks (ports or segments).

Reference: See your SiteProtector documentation and the *Proventia G Intrusion Prevention User Guide* or the Proventia Manager Help for more information.

Information checklist

Use the checklist in Table 2 to obtain the information you need to configure your Proventia G 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:	
□	Adapter mode	The adapter (operation) mode to use for the appliance. The adapter mode you plan to use should correspond to the way you connected the network cables.
	Your setting:	

Table 2: *Checklist and worksheet for configuration information*

Performing a New Installation

Introduction

Use the following procedure if you wish to perform a complete new installation of the 1.2 firmware release on a Proventia G Intrusion Prevention appliance.

Important: BEFORE YOU PERFORM THE INSTALLATION OR UPGRADE PROCEDURES, YOU MUST UNREGISTER THE SENSOR FROM THE SITEPROTECTOR CONSOLE AND REMOVE THE HOST.

ISS recommends that you perform a new installation to insure a complete transition to new features. Performing a new installation removes all of your current settings. You cannot perform a new installation remotely.

Installing the new software

To install the new software:

1. If there is a bezel cover on the front of the appliance, remove it.
2. Connect to the appliance in one of the following ways:
   - connect directly to the appliance using the video and keyboard ports.
   - connect the appliance to a computer using the serial cable and then use a terminal emulation program, such as Hyperterminal, to create a connection to the appliance. Set the terminal emulation session to **Auto Detect**.
3. Restart the appliance.

   Tip: You can manually turn the power off and on if the appliance is not responding.
4. Type `reinstall`, and then press ENTER.

   The appliance reloads the operating system, displays status messages, ejects the CD, and then restarts.
5. At the unconfigured login prompt, log in as username `admin`, and then the default password `admin` to access the Proventia Setup Utility.

   Important: The new software has three required usernames and passwords as follows:
   - **root**: Used for command line access to the appliance. Default is `root/admin.`
   - **administrative**: Used for accessing the Proventia Setup Utility. Default is `admin/admin.`
   - **Proventia Manager**: Used to access the new Proventia Manager, web-based local management interface. Default is `admin/admin.`

   Note: Use your existing SiteProtector username and password for SiteProtector console access.
6. Press ENTER.
7. Proceed to "Logging on and changing the default administrative password" on page 7.

   Important: The appliance applies new settings. A new installation does not save any of your previous settings.

Logging on and changing the default administrative password

To log on to the appliance and set your new administrative password:

Note: Use the administrative password to access the Proventia Setup utility.

1. Turn on the appliance.
2. Start your terminal emulator, if using the serial setup.
3. At the uncongured log in prompt, type **`admin`** for the user name, and then press ENTER.
4. Type **`admin`** for the password, and then press ENTER.

   The Proventia G Setup Utility screen appears.
5. Select **Start**, and then press ENTER.
6. Read the Software License Agreement, and then select **Accept** to continue.

   The Change Admin Password screen appears.
7. Type the default password **`admin`**, and then a new password.

   Note: You must use a minimum of six characters.
8. Re-type the new password to confirm it, select **OK**, and then press ENTER.

   Note: Record and protect this password. If you lose or forget this password, you must reinstall the appliance.

Setting the root and Proventia Manager passwords

To set the root and Proventia Manager passwords:

1. From the Setup Root Password screen, type the default root user password **`admin`**.
2. Type a new root user password.

   Note: You will need this password for command line access.
3. Re-type the new password to confirm it, select **OK**, and then press ENTER.

   The Proventia Manager password screen appears.

   Note: You will need this password to access the web-based Proventia Manager interface.
4. Type the Proventia Manager default password, **`admin.`**
5. Type a new password.
6. Type the new password again to confirm it.
7. Select **OK**, and then press ENTER.

   The Network Configuration screen appears.

Configuring the network interface and host

To configure the network interface and host:

1. On the Network Configuration screen, type the following:
   - **IP Address**,
   - **Subnet Mask**
   - **Default Gateway** of the management interface.
2. Select **OK**, and then press ENTER.

   The Host Configuration screen appears.

3. Type the following:
   - Hostname (**Example:** *`myappliance`*)
   - **Domain Name** (**Example:** *`mydomain.com`*)
   - **Name Servers** (optional).

   Note: The appliance uses domain names and domain name system (DNS) information to send email and SNMP responses. If you do not provide this information now, then you must specify the IP address of the appliance's mail server when you define the **Email Responses** in Proventia Manager. The appliance must have network access to the mail server to deliver responses.
4. Select **OK**, and then press ENTER.
5. Continue to the next topic to configure the time and date.

Configuring the date and time

To configure the date and time:

1. Use the ARROW keys to select the continent or area where the appliance is located, and then press ENTER.
2. Select the country where the appliance is located, and then press ENTER.
3. Select the timezone region where the appliance is located, and then press ENTER.

   Note: This screen does not appear if the country you selected contains only one time zone.
4. Select **OK**, and then press ENTER.

   A Timezone Confirmation screen appears.
5. Review the entries, select **OK**, and then press ENTER.

   The Date/Time configuration screen appears.
6. Press ENTER to accept the default time, or type a new time.

   Note: Use the format [`HH:MM:SS`] and a 24-hour clock.
7. Press ENTER to accept the default date, or type a new date.

   Note: Use the format [`mm/dd/yyyy`]

   The Agent Name Configuration screen appears.

Configuring the Agent Name

The Agent Name is the asset name for your appliance that appears in your SiteProtector console and in Proventia Manager. ISS recommends that you select a name that corresponds to the appliance's geographic location, business unit, building address, or some other meaningful classification. See "What is the Agent Manager?" on page 4.

To configure the agent name:

1. On the Agent Name configuration screen, press ENTER to accept the default **Agent Name**, or type a specific name.
2. Select **OK**, and then press ENTER.

   The Port Link Configuration screen displays.
3. Continue to the next topic to configure your port link settings.

Configuring the port settings

You can configure port link speed and duplex settings as appropriate for each monitoring port on the appliance. Appliance models can have two ports (A and B) or up to eight ports (A through H). Your settings should correspond to the settings on devices that bracket the appliance.

If you are unsure, check your other network device settings or ask your network administrator.

To configure the link speed and duplex settings:

1. On the Port Link Configuration screen, select Port A, and then do one of the following:
   - Press the DOWN ARROW to select the port link speed and duplex setting.
   - Press ENTER to accept the default settings.
2. Press TAB to move from port to port.
3. Select Port B, and then do one of the following:
   - Press the DOWN ARROW to select the port link speed and duplex settings.
   - Press ENTER to accept the default settings.
4. Repeat Step 1 and Step 2 to select additional ports, depending on your appliance model.
5. Select **OK** and press ENTER.

   The Adapter Mode Configuration screen displays.

Configuring the adapter mode

The adapter mode is the operation mode for each port pair. To configure the adapter mode:

1. Select the adapter mode for each port pair, depending on your appliance model. Determine the adapter mode that best suits your network configuration. You can select a different mode for each port pair.

   Example:

Port pair	Adapter mode	Description
A-B	Inline Protection	The appliance monitors traffic inline, and blocks attacks that are configured with the block response, quarantine response, and firewall rules
C-D	Passive Monitoring	The appliance monitors traffic from a tap, hub, or span port.
E-F	Passive Monitoring	
G-H	Inline Simulation	The appliance monitors traffic inline, but does not block any traffic. Instead, the appliance monitors traffic and provides passive responses.

⚠ **Caution:** When selecting the adapter mode, you must physically configure the monitored network connection. If is it not configured correctly, the mode setting could have significant network implications.

Reference: Refer to the Appliance Settings chapter of the *Proventia G Intrusion Prevention User Guide* for more information.

2. Select **OK**, and then press ENTER.

Applying the settings and logging out

To apply your settings and exit:

1. After you configure the agent name, a progress bar displays as the appliance applies your settings.
2. The Log out screen displays, indicating that the configuration is complete.
3. Select **Logout**, and then press ENTER.

   Important: Setup is not complete until you log in to Proventia Manager. Proceed to Accessing Proventia Manager below.

   Note: You can view and adjust appliance settings in Proventia Manager. See the *Proventia G Intrusion Prevention Appliances User Guide* and the Help for information and procedures.

Accessing Proventia Manager

Use Proventia Manager to:

- monitor the status of the appliance
- automatically download and install updates
- change appliance settings
- configure firewall settings
- configure intrusion prevention settings
- configure system settings
- configure high availability (optional)
- manage appliance activities
- configure local and advanced parameters

Requirements

After you complete the Proventia Setup tasks, you must do the following to access Proventia Manager and complete the installation process:

✓	Item	Action
□	Reconnect to your network	Verify the appliance connections to your network and properly reconnect your computer to your internal network (LAN). Verify that your TCP/IP settings are properly configured to allow access to your network and the Internet, depending on your network configuration.

Table 3: *Requirements*

✓	Item	Action
□	Get a license	Make sure you have a valid a license for your Proventia G appliance. Contact your Sales Representative for a License Registration number. 1. Go to the ISS Registration Center: https://www1.iss.net/cgi-bin/lrc. 2. Enter the registration number and access the license key files. 3. Locate your license file, and then save it to your computer. 4. Log in to Proventia Manager. In the **Important System Messages** box, click **Install License**, and then follow the prompts as directed. **Important:** You will need to reinstall your license key after upgrading to the new firmware. Full instaaltion or perofrming an upgrade removes your local license file. After you perform the reinstallation process and re-license SiteProtector, the SiteProtector license is sent to the appliance. Obtaining the new G model-specific licenses is recommended.
□	Internet Access	Verify that you have Internet Explorer 6.0 or later installed. In Internet Explorer, select **Help→About** to verify the version number.

Table 3: *Requirements*

Logging on to Proventia Manager

To log on to the Proventia Manager interface:

1. Start Internet Explorer and then type https:// followed by the hostname and domain of the appliance you configured during initial configuration.

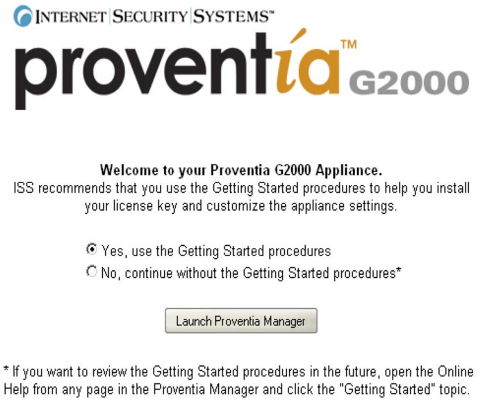
   Example: `https://hostname.domain.com`

   Note: You may also enter https:// followed by the management IP address. If you use the hostname, your DNS may not recognize the new appliance. If you receive a **Hostname Mismatch** message, click **Yes** to proceed.

2. Log in using the username **`admin`** and the password you configured for Proventia Manager in the procedure, “Setting the Proventia Manager password” on page 19.

   Note: If a message informs you that you do not have that latest version of Java2 Runtime Environment (JRE) installed, install it, and then return to this procedure. This Java plug-in is required for Proventia Manager.

   The Welcome screen appears.



Welcome to your Proventia G2000 Appliance.
ISS recommends that you use the Getting Started procedures to help you install your license key and customize the appliance settings.

● Yes, use the Getting Started procedures
○ No, continue without the Getting Started procedures*

* If you want to review the Getting Started procedures in the future, open the Online Help from any page in the Proventia Manager and click the "Getting Started" topic.

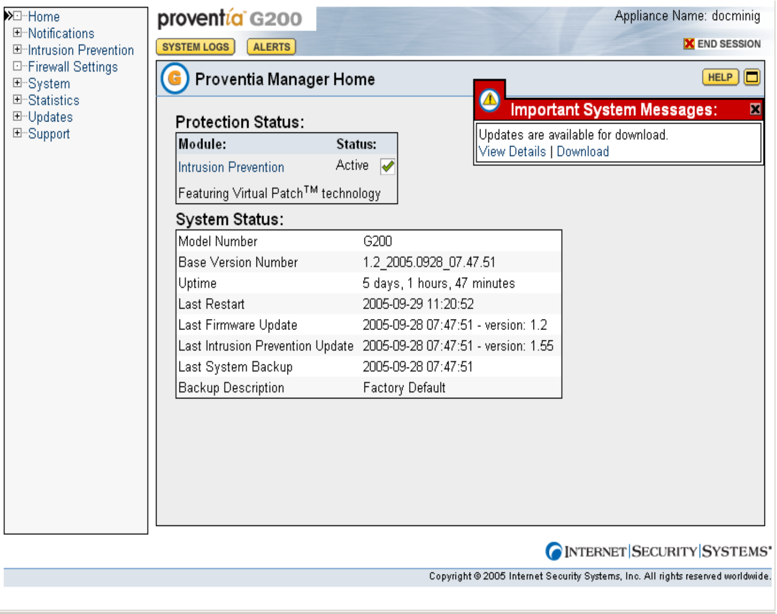
3. Do one of the following:

- Select *Yes* to use the Getting Started procedures.
- Select *No* to continue without using 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.

4. Click **Launch Proventia Manager**.

   The Proventia Manager Home page appears:



Appliance Name: docminig

Proventia Manager Home

Important System Messages:

Updates are available for download.
View Details | Download

Protection Status:

Module:	Status:
Intrusion Prevention	Active ✓
Featuring Virtual Patch™ technology	

System Status:

Model Number	G200
Base Version Number	1.2_2005.0928_07.47.51
Uptime	5 days, 1 hours, 47 minutes
Last Restart	2005-09-29 11:20:52
Last Firmware Update	2005-09-28 07:47:51 - version: 1.2
Last Intrusion Prevention Update	2005-09-28 07:47:51 - version: 1.55
Last System Backup	2005-09-28 07:47:51
Backup Description	Factory Default

Copyright © 2005 Internet Security Systems, Inc. All rights reserved worldwide.

5. Read the **Important System Messages**. Click **Install License** to install the license key file.
6. You should check for updates by selecting **Updates** in the Navigation pane.
7. See the Help or *Proventia G Inrusion Prevention User Guide* for more information.

SiteProtector Management

After installing and upgrading your appliance to the new functionality, you must reregister your appliance with SiteProtector and configure your SiteProtector management settings in Proventia Manager. See "Configuring SiteProtector Management" on page 22.

Creating a System Backup for an Existing Appliance Before You Upgrade

Introduction

Use the procedures in this topic to perform a backup of your current G appliance before upgrading. You will need this backup if you decide to uninstall the upgrade and return to your previous version with all of your settings.

⚠ **Caution:** If you do not follow the instructions in this section, you will lose all current settings and your previous configuration. A reinstallation from your existing appliance recovery CD reinstalls the appliance to factory-default settings, including passwords.

Creating a system backup

To create a system backup for your existing appliance:

1. Log in to the appliance as user **`admin`** and your current admin password.
2. Press ENTER.

   The Configuration Menu appears.
3. Select **Backup/Restore**.

   The Backup/Restore Menu appears.
4. Select **Backup Current Configuration**.
5. Type **`Y`** to start the backup process.

   The appliance restarts, takes a snapshot of the current system and then restarts again, This may take several minutes.
6. When appliance is back up, transfer the following files located in the `/backup/images` directory of the appliance to another computer on your network.

   - `image_sda1_.000`
   - `image_sda3_.000`
   - `image_sda5_.000`
   - `grub.cmd`
   - `info`
   - `partimage`

   Tip: Use a transfer program such as SCP to facilitate the transfer.

   Important: If you do not transfer these files to another location, they will be overwritten during the upgrade process and you will not be able to restore the appliance.

   Tip: Verify the checksums for these files after the file transfer to make sure they are not corrupted during the transfer.
7. Perform one of the update procedure as described in “Upgrading using the Next Generation Recovery CD” on page 17 or “Performing a Remote Upgrade” on page 17.

Applying the backup

Use this procedure if you want to uninstall the upgrade and return to your previous version. Use the backup you saved in the previous procedure to insure all of your previous settings are maintained.

Important: This requires physical access to the appliance. You cannot perform this restore procedure remotely.

To apply the backup:

1. If there is a bezel cover on the front of the appliance, remove it.
2. Connect to the appliance. There are two options:
   - connect directly to the appliance using the video and keyboard ports or,
   - connect using a serial cable and a terminal emulator to access the Proventia G Setup utility. To use this option you must:

     - Plug one end of the serial cable into the serial port on the back of the appliance and the other into the serial port on your computer or laptop.

     - Use a terminal emulation program, such as Hyperterminal, to create a connection to the appliance. Set the emulation to **Auto Detect**.
3. Place your original Recovery CD into the CD-ROM drive.

   Important: This is the Recovery CD that came with your older G appliance, not the new upgrade Recovery CD.
4. Restart the appliance.

   Tip: You can manually turn the power off and on if the appliance is not responding.
5. The appliance restarts and then at the **`boot:`** prompt, type `reinstall`, and then press ENTER.

   The appliance reloads the operating system, displays status messages, ejects the CD, and then restarts.
6. At the unconfigured login prompt, enter the default root username: **`admin`**
7. Enter the default root password: **`admin`**.

   The Proventia Setup screen displays.
8. At the log in prompt, enter the default administrative username **`admin`** and password **`admin`** to access Proventia Setup Utility.
9. Configure the appliance as described in your original documentation that came with your appliance, and then log out when prompted.

   Note: All G documentation is available online at: **Support→Product Documentation→ Proventia G Intrusion Prevention Appliance** (`http://www.iss.net/support/documentation`.

   Tip: Older G models should use the **Proventia G 100/200/1000/1200 Intrusion Prevention Appliance Service Release Documentation**.
10. After you perform the configuration tasks, log out and then transfer all of the backup files you have saved before the upgrade to the `/backup/images` directory of the appliance.

    Tip: Use a transfer program such as SCP to facilitate the transfer.

    The files you need to transfer are:
    - `image_sda1_.000`
    - `image_sda3_.000`
    - `image_sda5_.000`
    - `grub.cmd`
    - `info`
    - `partimage`

11. Log in to the Proventia Setup utility as username **`admin`** and your administrative password.
12. Press ENTER.

    The Configuration Menu appears.
13. Select **Backup/Restore**.

    The Backup/Restore Menu appears.
14. Select **Restore Config From Backup**
15. Type **`Y`** to start the restore process.

    The appliance restarts, restores the system from the backup and then restarts again.

Upgrading an Existing Appliance

Introduction

If you prefer not to do a new installation, you can also upgrade your existing Proventia G Series appliance to the Proventia G Next Generation Intrusion Prevention Appliance functionality.

Two upgrade methods

There are two methods available for upgrading the Proventia G Series appliances to the latest Proventia G Next Generation Intrusion Prevention Appliance functionality.

- Upgrading using a Next Generation Recovery CD

  This option requires physical access to the appliance.

- Performing a Remote Upgrade

  This option does not require physical access to the appliance. Users can update the appliance through an SSH (Secure Shell) connection.

  Note: Upgrading can save some of your current appliance settings, however additional configuration and policy verification may be required.

  Important: **BEFORE YOU PERFORM THE UPGRADE PROCEDURES, YOU MUST UNREGISTER THE SENSOR FROM THE SITEPROTECTOR CONSOLE AND REMOVE THE HOST.**

Settings that are saved during upgrade

The following settings are preserved during the upgrade process:

- root password
- admin password
- IP settings for management port
- host name and DNS settings
- time, date and timezone
- link speed and duplex settings for kill and management ports
- agent name
- operation mode (adapter mode)
- link speed and duplex settings for monitoring ports
- kill configuration

Note: You will need to set a password for Proventia Manager access. See “Setting the Proventia Manager password” on page 19.

Important: If you choose to uninstall the upgrade and reinstall your previous version using your original G Series Recovery CD, you will lose all settings unless you have performed the system backup procedure as described in “Creating a system backup” on page 13.

Upgrading using the Next Generation Recovery CD

To upgrade your appliance using the Next Generation Recovery CD:

1. Attach a monitor and keyboard to the appliance or connect the appliance to a computer and establish a serial connection.
2. Remove the bezel cover, insert the Recovery CD and start the appliance
3. When prompted, type **`upgrade`**.

   Note: The upgrade process verifies that the appliance qualifies for the upgrade. If it does not, the upgrade process displays an error message and exits the process.
4. The upgrade process saves your previous settings, and then installs the new image from the Recovery CD.
5. The process restores the saved settings, and then ejects the CD and restarts the appliance.
6. At the log in prompt, log in as `admin` to complete the upgrade process.

   Note: During the upgrade process your previous admin and root passwords and your network settings were saved. Use your existing passwords to log in to the appliance.
7. Enter your admin password.

   The Proventia Setup Utility screen appears.
8. Proceed to “Setting the Proventia Manager password” on page 19.

   Important: You must set the new Proventia Manager password and log in to Proventia Manager to complete the upgrade process.

Performing a Remote Upgrade

You may also upgrade the appliance remotely.

Important: BEFORE YOU PERFORM THE UPGRADE PROCEDURES, YOU MUST UNREGISTER THE SENSOR FROM THE SITEPROTECTOR CONSOLE AND REMOVE THE HOST.

1. Insert the Next Generation Recovery CD into the CD-ROM drive of a computer that resides on your network and browse to the `upgrade` directory of the CD.

   Important: Make sure you use the Next Generation Recovery CD associated with the model number of the appliance you wish to upgrade. For example, a G100 appliance can only be updated with the files copied from a G100 Next Generation Recovery CD and not from a G2000 Recovery CD.

2. Select and transfer the following files from the upgrade directory of the Recovery CD to the / directory on the appliance that you wish 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 a...
upgrade_G-Series.tgz	Proventia G100 or G200 appliance
upgrade_G1000.tgz	Proventia G1000 appliance
upgrade_G1200.tgz	Proventia G1200 appliance

   Note: These files are also available for download at the ISS Download Center at `http://www.iss.net/download/`.

3. Access the appliance (using SSH) and login as the root user.
4. Type `cd /` to access the / directory, and then do one of the following:
   - If upgrading a Proventia G1000 appliance, type:

     `tar -xzvpf  upgrade_G1000.tgz` to extract the update files.
   - If upgrading a Proventia G1200 appliance, type:

     `tar -xzvpf  upgrade_G1200.tgz` to extract the update files.
   - If upgrading a Proventia G100 or G200 appliance, type:

     `tar -xzvpf  upgrade_G-Series.tgz` to extract the update files.
5. Type `./remote_upgrade.sh` to run the remote_upgrade.sh script

   Note: The upgrade process verifies that the appliance qualifies for the upgrade. If it does not, the upgrade process displays an error message and exits the process. The upgrade process also verifies that all required files are present and valid. If an image is missing or cannot be verified, the upgrade process displays an error message and exits.
6. The upgrade process saves your existing settings, restarts the appliance, and then installs the new image and restores the saved settings.
7. The appliance restarts and the update process continues.

   Important: Please be patient. You cannot access the appliance remotely until the process is completed which includes setting the new password. This takes several minutes.

   ⚠ **Caution:** Setup is **NOT COMPLETE** until you log in again and change the password. You must complete the following steps in order to access Proventia Manager.
8. Wait for the appliance to restart and a connection is established, and then log in as user `admin`.

   Note: During the upgrade process your previous admin and root passwords and your network settings were saved. Use your existing passwords to log in to the appliance and continue the upgrade process.
9. Enter your admin password.

   The Proventia Setup Utility screen appears.
10. Proceed to “Setting the Proventia Manager password” on page 19.

Setting the Proventia Manager password

To complete the upgrade process you must set a password for Proventia Manager access. You must configure a password using the Proventia Setup utility before you can access Proventia Manager.

To set the Proventia Manager password:

1. On the Proventia Setup utility screen, select **Start** and then press ENTER.
2. Select **Accept** to accept the license agreement, and then press ENTER.

   The Proventia Manager password screen appears.
3. As prompted, under existing username `admin`, enter a password for Proventia Manager.

   A progress bar displays followed by a configuration complete message.
4. Select **Logout**, and press ENTER to exit the utility.
5. Continue to the next topic, Accessing Proventia Manager.

Accessing Proventia Manager

Proventia Manager is the new web-based local management interface. After you connect and configure the appliance, you must do the following to use Proventia Manager:

✓	Item	Action
❑	Reconnect to your network	Reconnect your computer to your internal network (LAN). Verify that your TCP/IP settings are properly configured, depending on your network configuration.
❑	Get a license	Make sure you have a valid a license for your Proventia G appliance. Contact your Sales Representative for a **License Registration number.** 1. Go to the ISS Registration Center: `https://www1.iss.net/cgi-bin/lrc`. 2. Enter the Registration number and you willb e able to access the license key files. 3. Locate the correct license file, and then save it to your computer. 4. You will be prompted by Proventia Manager once you log in to upload the license. Click Install License and then follow the prompts as directed. **Important:** You will need to reinstall your license key after installing or upgrading to the new firmware.Installing and upgrading removes your local license file even when you register with SiteProtector. After you perform the reinstallation process and license SiteProtector, the SiteProtector license is sent to the appliance. Obtaining the new G model-specific licenses is recommended.
❑	Internet Access	Verify that you have Internet Explorer 6.0 or later installed. In Internet Explorer, select **Help**→ **About** to verify the version number.

Table 4: *Prerequisites*

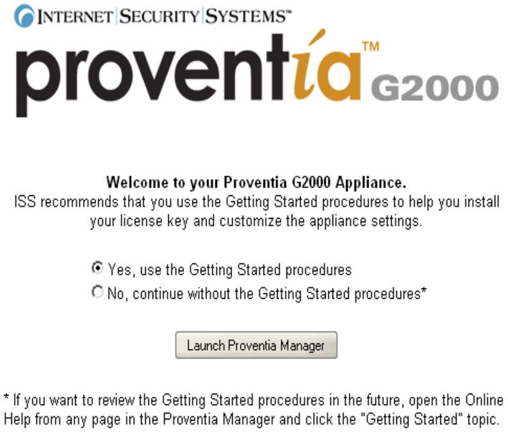
Logging on to Proventia Manager

To log on to the Proventia Manager interface:

1. Start the Internet Explorer, and then type https:// followed by the IP address of the appliance's management interface you configured during initial configuration.
   Example: https://192.168.123.123
2. Log in as username **`admin`** and the password you configured for Proventia Manager during setup, "Setting the Proventia Manager password" on page 19.

   Note: If a message informs you that you do not have that latest version of Java2 Runtime Environment (JRE) installed, install it, and then return to this procedure. This Java plug-in is required for Proventia Manager.

   The Welcome screen appears.



Welcome to your Proventia G2000 Appliance.
ISS recommends that you use the Getting Started procedures to help you install your license key and customize the appliance settings.

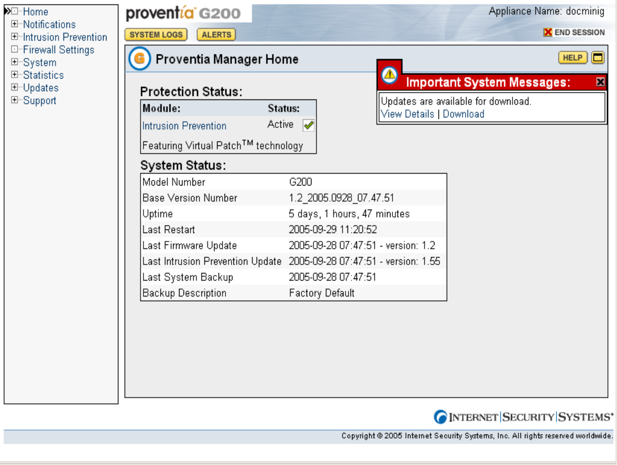
● Yes, use the Getting Started procedures
○ No, continue without the Getting Started procedures*

* If you want to review the Getting Started procedures in the future, open the Online Help from any page in the Proventia Manager and click the "Getting Started" topic.

3. Do one of the following:
   - Select *Yes* to use the Getting Started procedures.
   - Select *No* to continue without using 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.
4. Click **Launch Proventia Manager**.

   The Proventia Manager Home page appears:



Appliance Name: docminig

Proventia Manager Home

Important System Messages:
Updates are available for download.
View Details | Download

Protection Status:

Module:	Status:
Intrusion Prevention	Active ✓
Featuring Virtual Patch™ technology	

System Status:

Model Number	G200
Base Version Number	1.2_2005.0928_07.47.51
Uptime	5 days, 1 hours, 47 minutes
Last Restart	2005-09-29 11:20:52
Last Firmware Update	2005-09-28 07:47:51 - version: 1.2
Last Intrusion Prevention Update	2005-09-28 07:47:51 - version: 1.55
Last System Backup	2005-09-28 07:47:51
Backup Description	Factory Default

Copyright © 2005 Internet Security Systems, Inc. All rights reserved worldwide.

5. Read the **Important System Messages**. Click **Install License** to install the license key file.
6. You can check for updates by selecting **Updates** in the Navigation pane.

   Note: See the Help or the *Proventia G Intrusion Provention User Guide* for more information.

SiteProtector Management

After installing and upgrading your appliance to the new functionality, you must reregister your appliance with SiteProtector and configure your SiteProtector management settings in Proventia Manager. See “Configuring SiteProtector Management” on page 22.

Configuring SiteProtector Management

Introduction

After upgrading your appliance to the new functionality, you must configure your SiteProtector management console settings in Proventia Manager.

- Before you reinstall SiteProtector, verify you have the following versions:
  - SiteProtector Service Pack 5.2
  - Database Service Pack (DBSP) 5.18 or later.

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 your appliance.

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

Before registering the appliance

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

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

Configuring SiteProtector management

To configure SiteProtector management of your appliance:

1. In the navigation pane, 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. **Important**: You must assign the appliance to a group that contains only other G-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 60 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 the navigation pane, select **System→Management**.
2. Ensure you have enabled registration with SiteProtector.
3. In the Agent Manager Configuration area, click **Add**, or highlight and existing Agent Manager and click **Edit**.
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 successful registration of your appliance with SiteProtector:

1. Open the SiteProtector Console.
2. In the Enterprise Groups pane, select the group to which you added the appliance.

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

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

About Intrusion Prevention

Introduction

If you selected to install all of the new intrusion prevention features available to you in the 1.2 release, you will find that the way you create and manage your policies has changed substantially. The features in this release provide you with more control and more possibility. ISS strongly recommends that you adopt the new features for creating and managing your appliance policies, as these features ensure the greatest protection for your network.

Intrusion prevention features

In the Proventia G Intrusion Prevention Appliance 1.2 release, you will find the following new features:

- **Responses (see the *Proventia G Intrusion Prevention Appliance User Guide 1.2*, page 83)**

  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.
  - **Quarantine**. Use default quarantine responses to protect your network against attacks.
  - **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 (see the *Proventia G Intrusion Prevention Appliance User Guide 1.2, page 68*)**

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

- **Security Events and Response Filters (see the *Proventia G Intrusion Prevention Appliance User Guide 1.2*, pages 71 and 77)**

  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 controlling the number of events to which the appliance responds and the number of events reported to the management console, either the Proventia Manager Alerts page, or the SiteProtector Analysis tab.

- **Connection Events (see the *Proventia G Intrusion Prevention Appliance User Guide 1.2, page 97*)**

  Connection events are user-defined notifications of open connections to or from particular addresses or ports. They are generated when the appliance detects network activity at a designated port, regardless of the type of activity or network packets, or the content of the packets exchanged. The Connection Events page lists pre-defined connection events for different connection types, such as WWW, FTP, or IRC. Use this page to customize these events or to create your own events to cover the traffic you need to monitor.

- **User-Defined Events (see the *Proventia G Intrusion Prevention Appliance User Guide 1.2*, page 101)**

  You can create user-defined events around contexts, which basically specify the type and part of a network packet you want the appliance to scan for events. For example, you could specify the Email_Receiver context, which monitors incoming or outgoing email to a particular recipient. Once you have determined the context, you add a string that tells the appliance exactly what to look for in a particular context.

- **Quarantined Intrusions (see the *Proventia G Intrusion Prevention Appliance User Guide 1.2*, page 96)**

  The Quarantined Intrusions page shows quarantine rules dynamically generated in response to detected intruder events. These rules specify packets to block and the length of time to block them. They prevent worms from spreading, and deny access to systems infected with backdoors or trojans.

Working with Security Events: A Walk-Through

Introduction

If you have installed the new features in the Next Generation 1.2 release, you will find substantial differences in the way you create and edit your security policies. This section explains how to create your security events policy using the new features. ISS strongly recommends that you adopt the new features for creating and managing your appliance policies, as these features ensure the greatest protection for your network.

This walk-through covers the following steps:

- Step 1: Creating an Email response.
- Step 2: Creating a protection domain.
- Step 3: Selecting security events to monitor.
- Step 4: Editing security events.
- Step 5: Creating a response filter around security events.

For detailed information and procedures, see the *Proventia G Intrusion Prevention User Guide 1.2*.

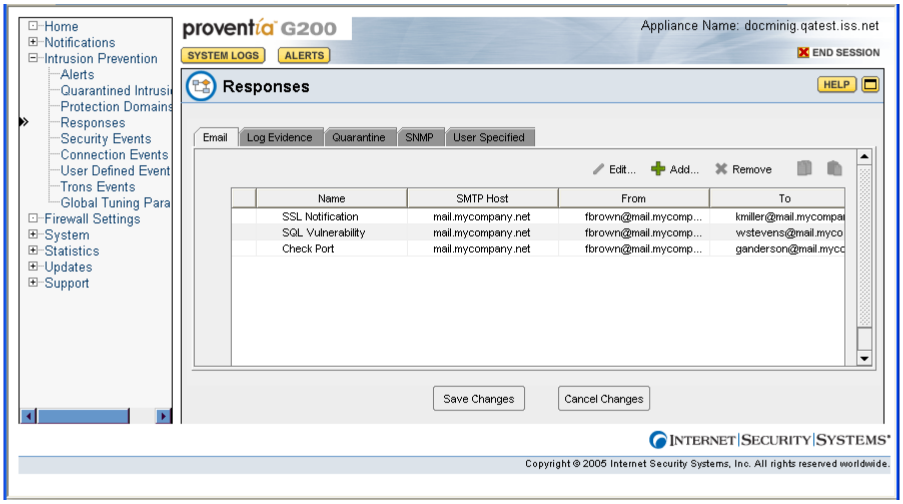
Step 1: Creating an Email response

Creating responses is a logical first step in managing your security policy. 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 could set up an email response that can automatically notifies that person when HTTP events you have specified occur on your network.

Let's say you want to create an email response for your Web Administrator, John Smith.

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

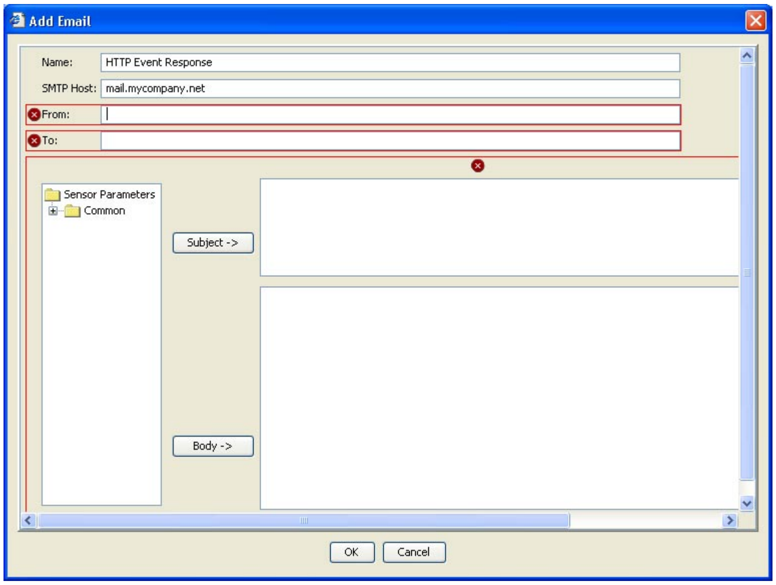
   Tip: In the SiteProtector G Series Policy Editor, you would select the appliance, and then select Response Objects.



Name	SMTP Host	From	To
SSL Notification	mail.mycompany.net	fbrown@mail.mycomp...	kmiller@mail.mycompa
SQL Vulnerability	mail.mycompany.net	fbrown@mail.mycomp...	wstevens@mail.myco
Check Port	mail.mycompany.net	fbrown@mail.mycomp...	ganderson@mail.mycc

Figure 1: *Response Object/Email screen shot*

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



Name: HTTP Event Response

SMTP Host: mail.mycompany.net

From:

To:

Figure 2: *Add Email screen shot*

3. In the Add Email window, provide the following information:

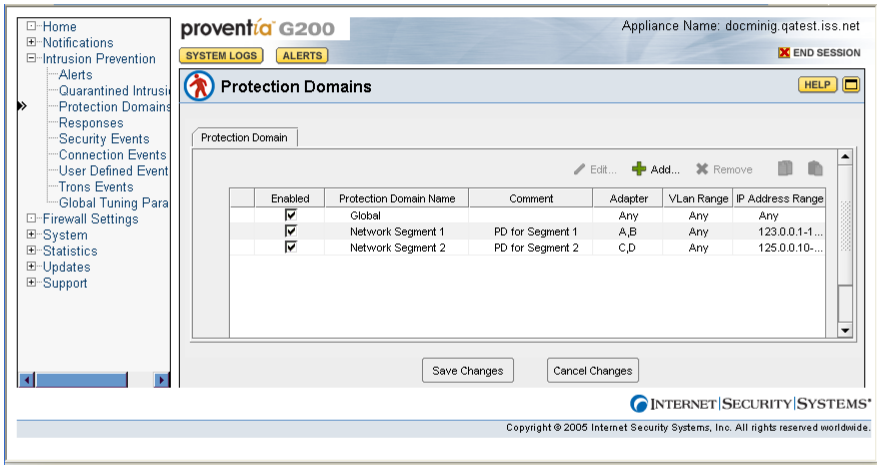
Setting	Description
Name	You would type a meaningful name for the response, such as “HTTP Event Response.”
SMTP Host	You would type the fully qualified domain name (mail.mycompany.net) or IP address of the mail server.
From	You would enter the email address for the person assigning this responsibility to John, the Web Administrator. Suppose the sender will appear to be his boss, Frank Brown, so you type “fbrown@mail.mycompany.net”
To	You would 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 will know exactly when the event took place.

Step 2: Creating a protection domain

Once you have created 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.

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

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



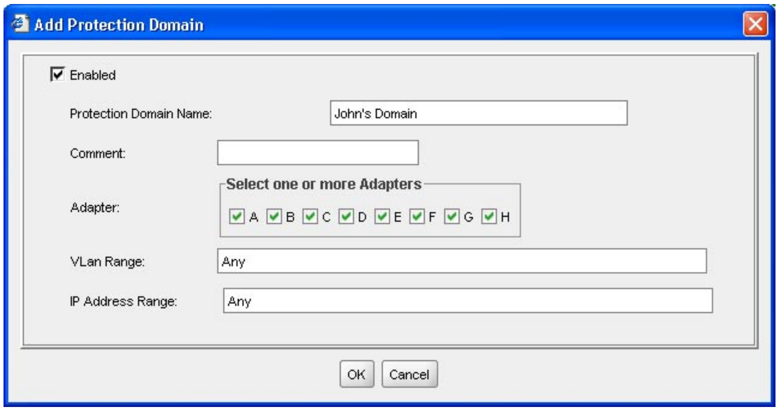
Protection Domains

Protection Domain

	Enabled	Protection Domain Name	Comment	Adapter	VLan Range	IP Address Range
	☑	Global		Any	Any	Any
	☑	Network Segment 1	PD for Segment 1	A,B	Any	123.0.0.1-1...
	☑	Network Segment 2	PD for Segment 2	C,D	Any	125.0.0.10-...

Figure 3: *Protection Domains window*

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



Add Protection Domain

☑ Enabled

Protection Domain Name: John's Domain

Comment:

Adapter: Select one or more Adapters ☑ A ☑ B ☑ C ☑ D ☑ E ☑ F ☑ G ☑ H

VLan Range: Any

IP Address Range: Any

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.”
Comment	You type a unique description for the domain. You could type “John Smith’s network segment.”

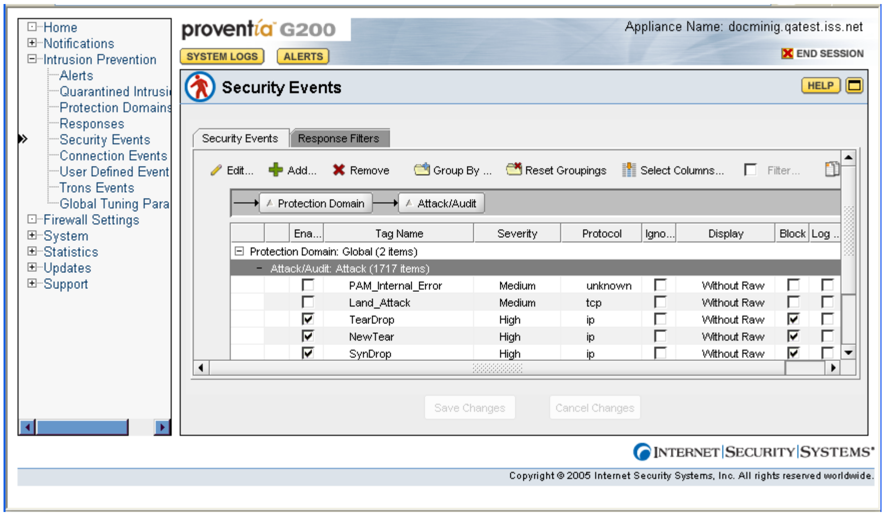
Setting	Description
Adapter	You select the appliance monitoring adapter or list of monitoring adapters for John’s domain.
VLAN Range	Here, you would type the range of virtual LAN tags, but this setting does not apply to John’s domain.
IP Address Range	Instead you type the range of source and destination 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

Once you have defined 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.

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



Appliance Name: docminig.qatest.iss.net

Protection Domain: Global (2 items)

Attack/Audit: Attack (1717 items)

		Ena...	Tag Name	Severity	Protocol	Igno...	Display	Block	Log ..
		☐	PAM_Internal_Error	Medium	unknown	☐	Without Raw	☐	☐
		☐	Land_Attack	Medium	tcp	☐	Without Raw	☐	☐
		☑	TearDrop	High	ip	☐	Without Raw	☑	☐
		☑	NewTear	High	ip	☐	Without Raw	☑	☐
		☑	SynDrop	High	ip	☐	Without Raw	☑	☐

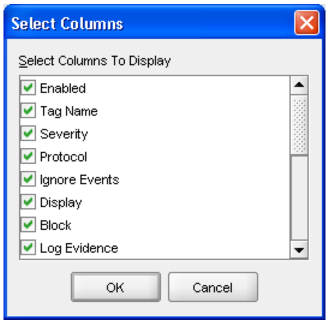
Copyright © 2005 Internet Security Systems, Inc. All rights reserved worldwide.

Figure 5: *Security Events list*

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

   - **Select Columns**

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



Select Columns To Display

- ☑ Enabled
- ☑ Tag Name
- ☑ Severity
- ☑ Protocol
- ☑ Ignore Events
- ☑ Display
- ☑ Block
- ☑ Log Evidence

Figure 6: *Select columns dialog box*

- **Group By**

  Once 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.

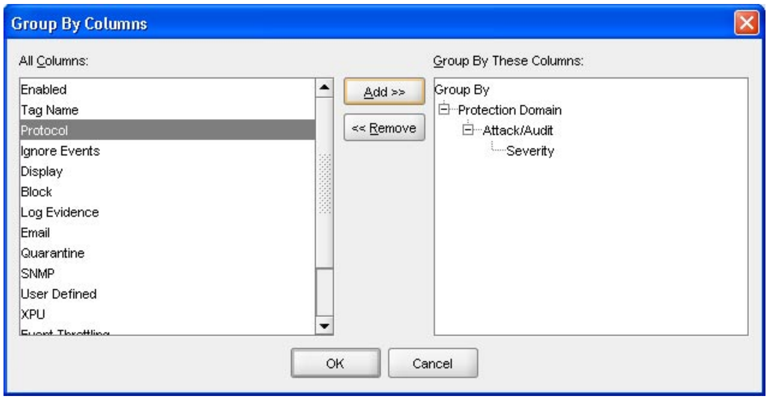


Figure 7: *Group By Columns dialog box*

- **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 will appear.

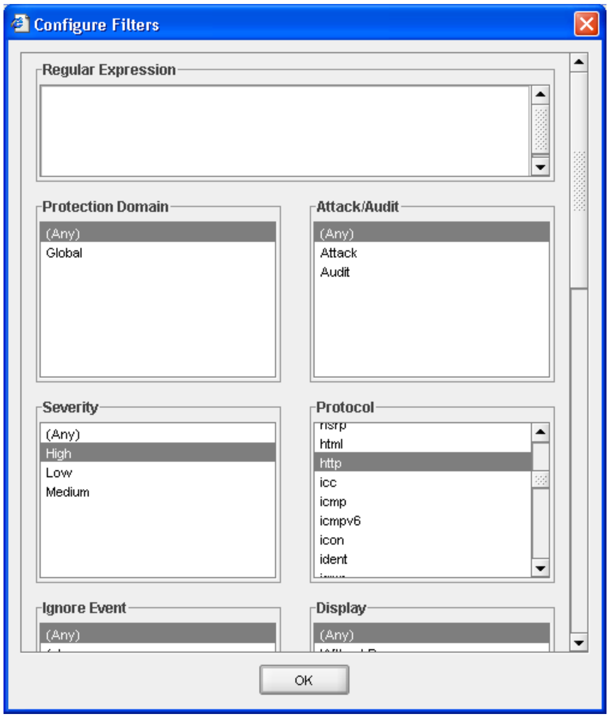


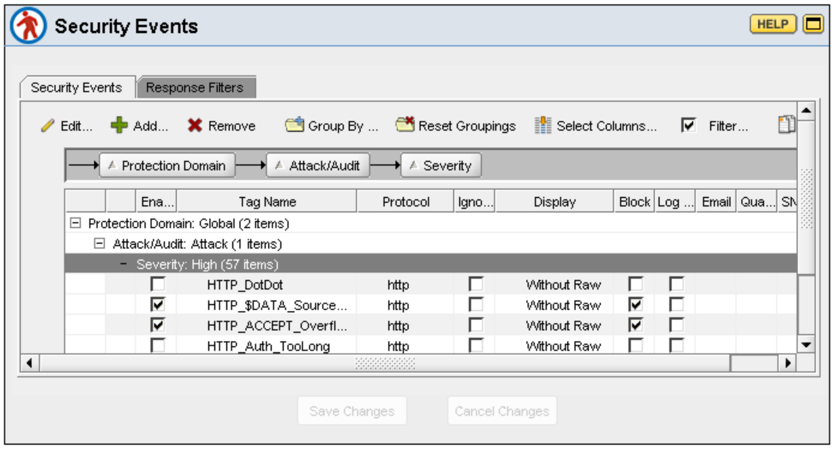
Figure 8: *Configure Filters dialog box*

Step 4: Editing security events

Once you have customized 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 the events to the protection domain you created in Step 2.

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 would select the Severity: High parent row, which automatically selects all the events in the list.

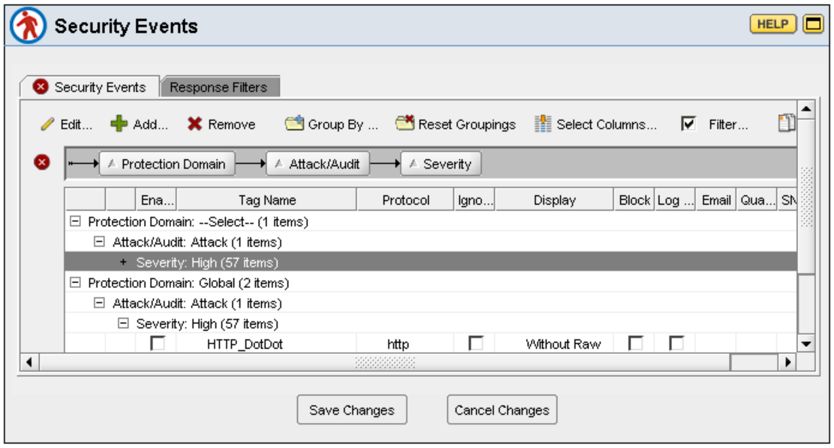
   Notice that all events are listed under the Global Protection Domain. The appliance always uses a global security policy, which means that it will handle security events in the same manner for all areas of your network. You should configure events at the Global level that you want to apply across all segments in your network.



	Ena...	Tag Name	Protocol	Igno...	Display	Block	Log ...	Email	Qua...	SN
⊟ Protection Domain: Global (2 items)										
⊟ Attack/Audit: Attack (1 items)										
− Severity: High (57 items)										
	□	HTTP_DotDot	http	□	Without Raw	□	□			
	☑	HTTP_$DATA_Source...	http	□	Without Raw	☑	□			
	☑	HTTP_ACCEPT_Overfl...	http	□	Without Raw	☑	□			
	□	HTTP_Auth_TooLong	http	□	Without Raw	□	□			

Figure 9: *Security Events page*

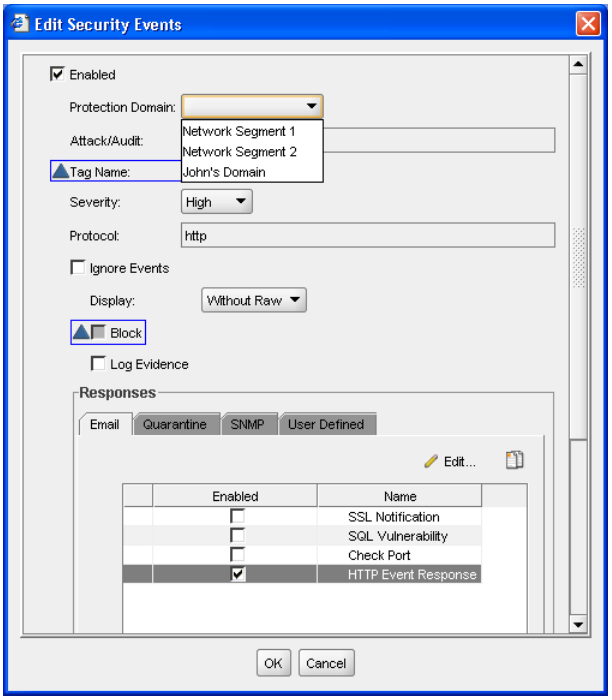
2. Click **Copy**, and then click **Paste**. This adds the filtered events to the list outside of the global protection domain.



	Ena...	Tag Name	Protocol	Igno...	Display	Block	Log ...	Email	Qua...	SN
⊟ Protection Domain: --Select-- (1 items)										
⊟ Attack/Audit: Attack (1 items)										
+ Severity: High (57 items)										
⊟ Protection Domain: Global (2 items)										
⊟ Attack/Audit: Attack (1 items)										
⊟ Severity: High (57 items)										
	□	HTTP_DotDot	http	□	Without Raw	□	□			

Figure 10: *Pasted security events*

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



Edit Security Events

☑ Enabled

Protection Domain:
- Network Segment 1
- Network Segment 2
- John's Domain

Attack/Audit:

Tag Name:

Severity: High

Protocol: http

□ Ignore Events

Display: Without Raw

□ Block

□ Log Evidence

Responses

Enabled	Name
□	SSL Notification
□	SQL Vulnerability
□	Check Port
☑	HTTP Event Response

Figure 11: *Edit Security Events dialog box*

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

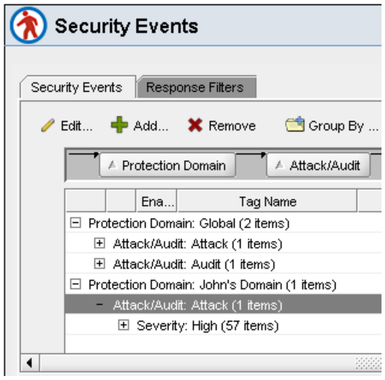
4. Select **Enabled** to enable the events in the list, and then select the **Protection Domain** "John's Domain" from the list.

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 custom events, this area is unavailable.
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.

Setting	Description
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 the attack by dropping packets and sending resets to TCP connections.
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	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.
Default Protection	For existing events only, displays the default protection set for the event, such as "Block." This setting is read-only.
User Overridden	For custom events, this check box is enabled by default to indicate a custom event. In the list on the Security Events tab, this item will appear 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.



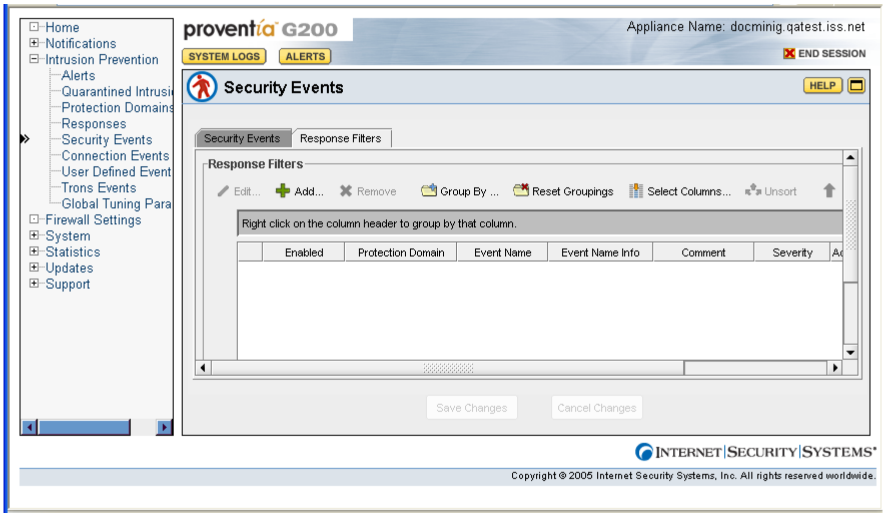
⊟ Protection Domain: Global (2 items)
⊞ Attack/Audit: Attack (1 items)
⊞ Attack/Audit: Audit (1 items)
⊟ Protection Domain: John's Domain (1 items)
− Attack/Audit: Attack (1 items)
⊞ Severity: High (57 items)

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

Step 5: Creating a response filter

At some point, you may need to refine the security policy. Perhaps a particular event in your security policy is triggering over and over on your network, but the Web Administrator has let you know that even though the event has a high severity, it really is not all that important to your network. Generally, this event is only occurring on a trusted host. You can set a response filter to ignore the event.

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



Appliance Name: docminig.qatest.iss.net

Security Events

Response Filters

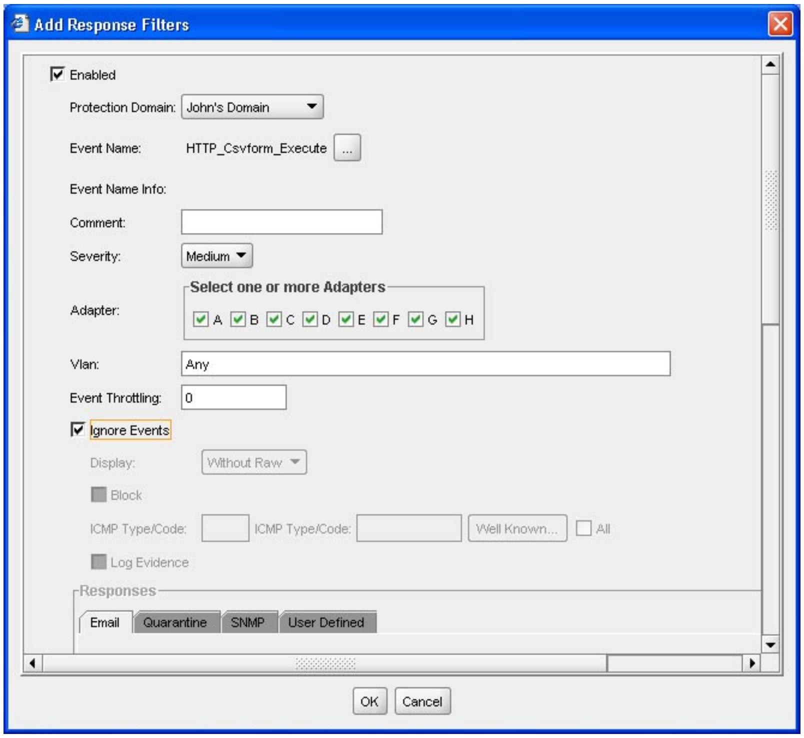
Right click on the column header to group by that column.

	Enabled	Protection Domain	Event Name	Event Name Info	Comment	Severity	Ac

Copyright © 2005 Internet Security Systems, Inc. All rights reserved worldwide.

Figure 13: *Response Filters page*

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



Add Response Filters

☑ Enabled

Protection Domain: John's Domain

Event Name: HTTP_Csvform_Execute

Event Name Info:

Comment:

Severity: Medium

Adapter: Select one or more Adapters ☑ A ☑ B ☑ C ☑ D ☑ E ☑ F ☑ G ☑ H

Vlan: Any

Event Throttling: 0

☑ Ignore Events

Display: Without Raw

□ Block

ICMP Type/Code: ICMP Type/Code: □ All

□ Log Evidence

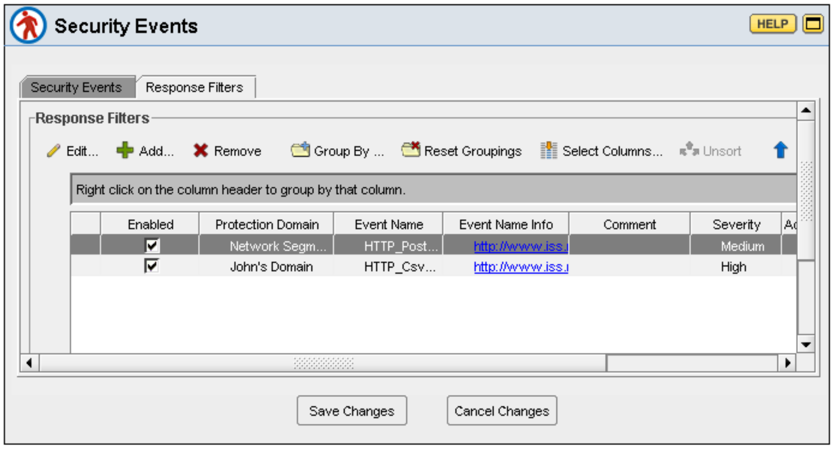
Figure 14: *Add Response Filters dialog box*

3. In the Add Response Filters dialog box, select the **Ignore Events** option. This enables the appliance to ignore this event in your security policy.

   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 the attack by dropping packets and sending resets to TCP connections.
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.



Right click on the column header to group by that column.

	Enabled	Protection Domain	Event Name	Event Name Info	Comment	Severity	Ac
	☑	Network Segm...	HTTP_Post...	http://www.iss.i		Medium	
	☑	John's Domain	HTTP_Csv...	http://www.iss.i		High	

Figure 15: *Response Filters list*

DOC-QSA-PROVIPAG-007-A