INTERNET SECURITY SYSTEMS™

proventia™

A604, A1204, and A1204F Appliance User Guide

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

June 18, 2003

Contents

Preface

Overview

Purpose of this guide

This guide describes the procedures and requirements for configuring the Proventia A604, A1204, and A1204F appliances. The guide contains instructions for the following:

- setting up a local configuration interface
- changing configuration settings
- reinstalling the appliance software

Audience

This guide is intended for current and new users of the appliances.

First version of this guide

The *Proventia™ A604, A1204, and A1204F User Guide* includes information about the following topics:

- configuring packet captures for Proventia appliances
- configuring the no packet alert for Proventia appliances
- configuring the port ID for Proventia appliances
- reinstalling the appliance software
- configuring an agent name and the RSKILL response

About Appliance Documentation

Using this guide

Use this guide together with the *Proventia™ A604, A1204, and A1204F Appliance Quick Start Card*.

Related publications

For additional information, see the following publications:

- *SiteProtector Help*
- *ISS Response, Policy, and Event Collector Help*

Conventions Used in this Guide

Introduction

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

In procedures

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

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

Table 1: *Typographic conventions for procedures*

Command conventions

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

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

Table 2: *Typographic conventions for commands*

Getting Technical Support

Introduction

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

The ISS Web site

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

Hours of support

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

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

Table 3: *Hours for technical support*

Contact information

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

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

Table 4: *Contact information for technical support*

Chapter 1

Introduction to Proventia A604, A1204, and A1204F Appliances

Overview

Introduction

This chapter describes the Proventia A604, A1204, and A1204F appliances. It also contains instructions for logging on to the local configuration interface.

In this chapter

This chapter contains the following topics:

About the Proventia™ A604, A1204, and A1204F Appliances

What are Proventia appliances?

ISS Proventia appliances dynamically protect your network from threats and significantly reduce your company's acquisition, deployment, and support costs. Centrally manage appliances, along with all other ISS network, server, and desktop protection agents, with one security management platform: SiteProtector™.

Hardware differences between models

The A604 and A1204 appliances include gigabit copper detection ports (A/B and C/D). The A1204F appliance includes gigabit fiber detection ports (A/B and C/D).

Reference: For more information about the appliance hardware, see the following Internet Security Systems documents:

- *Proventia A604, A1204, and A1204F Quick Start Card*
- *Proventia A Series Specifications*
- *ISS Proventia Dynamic Threat Protection Appliances Frequently Asked Questions*

Installing and configuring an appliance

ISS delivers appliances with pre-installed software. See the Quick Start Card that is provided with the appliance for instructions on installing the appliance in a rack and for initial configuration.

Note: Installation and configuration procedures for the A1204 and A1204F appliances are the same as for the A604 appliance.

Managing the appliance from the console

After you complete the configuration steps listed on the Quick Start Card, you must continue to configure the appliance from the management console.

Reference: For instructions on viewing events and managing the appliance from the SiteProtector management console, see the management console user documentation at http://www.iss.net/support/documentation/.

Licensing

Proventia A604, A1204, and A1204F appliances require a properly configured license key. If you have not installed the appropriate license key through the management console, you will not be able to manage the appliance.

Purchasing a license: To purchase a license for a Proventia A604, A1204, or A1204F appliance, contact your local sales representative.

Setting Up a Local Configuration Interface and Logging In

Introduction

Before you can view or change appliance settings, you must set up a local configuration interface and log in to the appliance.

Procedure

To set up a local configuration interface and log in to the appliance:

1. Do one of the following:
   - Connect a keyboard and monitor to the connectors on the rear panel of the appliance.
   - Connect a computer (such as a laptop) to the serial port on the rear panel of the appliance.
     – Specify 8 data bits, no parity, and 1 stop bit (8-N-1).
     – Set the computer to VT-100 terminal emulation mode at 9600 bps.
     – Set flow control to **None**.
     – Select the com port to which you have connected the appliance.

     The appliance displays the login prompt: `<appliance name> login: _`
2. Type **`admin`**, and then press ENTER.
3. Type the admin password, and then press ENTER.

   Note: The default password is **admin**.

   An introductory screen appears.
4. Press ENTER.

   The Configuration menu appears.
5. Use the UP and DOWN arrow keys to move from one menu item to another.
6. Press ENTER to select a menu item.
7. Configure the appliance's settings as described in Chapter 2, "Configuring and Viewing Appliance Settings" on page 5.

Chapter 2

Configuring and Viewing Appliance Settings

Overview

Introduction

This chapter describes how to configure the appliance software and view appliance settings.

In this chapter

This chapter contains the following topics:

Changing the Administrative Password

Introduction

You can change the administrative password at any time.

⚠ **Caution:** Record and protect this password. If you lose the password, you must reinstall the appliance.

Procedure

To change the administrative password:

1. Set up a local configuration interface and log in, as described in "Setting Up a Local Configuration Interface and Logging In" on page 3.
2. Select **Change Admin Password** from the Configuration menu, and then press ENTER.
3. Type the old password, and then press ENTER.

   Note: The default password is **admin**.
4. Type the new password, and then press ENTER.

   Note: You must use a minimum of six characters.
5. Retype the new password to confirm it, and then press ENTER.

   The appliance displays a confirmation screen.
6. Press ENTER to return to the Configuration menu.

Changing the Network Configuration Settings

Introduction

You can change the following network configuration settings that you configured when you installed the appliance:

- IP address
- subnet mask
- gateway

Procedure

To change the network configuration settings:

1. Set up a local configuration interface and log in, as described in "Setting Up a Local Configuration Interface and Logging In" on page 3.
2. On the Configuration menu, select **Change Network Configuration**, and then press ENTER.
3. Type the new settings.
4. Press ENTER.

   The appliance displays a progress message while it configures the host settings, and then displays the message `Host configuration has been saved` when the configuration is complete.
5. Press ENTER to return to the Configuration menu.

Changing the Host Configuration Settings

Introduction

You can change the following host configuration settings that you configured when you installed the appliance:

- hostname (required)
- domain name (recommended)
- name server (recommended)

Note: The appliance uses domain names and DNS information to send Email and SNMP responses. If you do not provide this information now, the appliance can still send Email and SNMP responses. You must specify the IP address of the appliance's mail server when you define the Email response on the management console. The appliance must have network access to the mail server. For more information, see the management console's user documentation.

Procedure

To change the host configuration settings:

1. Set up a local configuration interface and log on, as described in "Setting Up a Local Configuration Interface and Logging In" on page 3.
2. On the Configuration menu, select **Change Host Configuration**, and then press ENTER.
3. Type the new settings.
4. Press ENTER.

   A confirmation screen appears.
5. Press ENTER to return to the Configuration menu.

Changing the Date and Time Settings

Introduction

You can change the date and time settings for the appliance that you configured when you installed the appliance.

Procedure

To change the date and time settings:

1. Set up a local configuration interface and log in, as described in "Setting Up a Local Configuration Interface and Logging In" on page 3.
2. On the Configuration menu, select **Set Date and Time**, and then press ENTER.
3. Type the new date, and then press ENTER.

   Note: Use the format [`MM/DD/YYYY`].
4. Type the new time, and then press ENTER.

   Note: Use the format [`HH:MM:SS`] and a 24-hour clock.

   The appliance displays a confirmation screen.
5. Press ENTER to return to the Configuration menu.

Changing the Time Zone Setting

Introduction

You can change the time zone settings. The appliance sets the time zone according to your selections.

Procedure

To change the time zone setting:

1. Set up a local configuration interface and log in, as described in "Setting Up a Local Configuration Interface and Logging In" on page 3.
2. On the Configuration menu, select **Set Timezone**, and then press ENTER.
3. Select the continent or ocean in which the appliance is located, and then press ENTER.
4. Select the country in which the appliance is located, and then press ENTER.
5. Select the region in which the appliance is located, and then press ENTER.

   Note: This screen does not appear if the country you selected contains only one region (time zone).
6. Type **y** to confirm.

   The appliance displays the Configuration menu.

Viewing Appliance Host, Network Configuration, Date/Time, and Time Zone Settings

Introduction

You can view the following settings that you configured during the appliance installation:

- the IP address, subnet mask, and gateway of the appliance management interface
- the hostname, domain name, and name server (if provided during initial installation) of the appliance
- the current date, time, and time zone settings of the appliance

Procedure

To view the settings:

1. Set up a local configuration interface and log on, as described in "Setting Up a Local Configuration Interface and Logging In" on page 3.
2. On the Configuration menu, select **Proventia A604 or A1204 Information**, and then press ENTER.

   The appliance displays the information.
3. Press ESC to return to the Configuration menu.

Viewing the Status of Appliance Components

Introduction

You can view the status and version of the agent and daemon components of the appliance.

Procedure

To view the status of the appliance components:

1. Set up a local configuration interface and log in, as described in "Setting Up a Local Configuration Interface and Logging In" on page 3.
2. On the Configuration menu, select **Agent Status**, and then press ENTER.

   The appliance displays the following items:

   - status of the agent
   - status of the daemon
   - version of the agent
   - version of the daemon
3. View the information, and then press ESC to return to the Configuration menu.

   The appliance displays a confirmation screen.
4. Press ENTER to return to the Configuration menu.

Restarting the Agent

Introduction

You may want to restart the agent to troubleshoot a problem with the appliance.

Procedure

To restart the agent:

1. Set up a local configuration interface and log in, as described in "Setting Up a Local Configuration Interface and Logging In" on page 3.
2. On the Configuration menu, select **Agent Status**, and then press ENTER.

   The appliance displays the following items:

   - status of the agent
   - status of the daemon
   - version of the agent
   - version of the daemon
3. Type **y**.

   The agent restarts, and then a confirmation screen appears.
4. Press ENTER to return to the Configuration menu.

Allowing SiteProtector Access to the Appliance

Introduction

You can automatically import authentication keys when you connect to SiteProtector. You only need to import authentication keys once. All SiteProtector consoles that connect to the appliance are granted access levels according to user permissions.

Note: If you do not set up Site Protector access, the management console cannot communicate with the appliance.

Procedure

To allow SiteProtector access:

1. Set up a local configuration interface and log in, as described in "Setting Up a Local Configuration Interface and Logging In" on page 3.
2. On the Configuration menu, select **Allow SiteProtector Access**, and then press ENTER.
3. Type **A** to automatically import the authentication key.

   Note: When you select option **A**, the appliance receives the initial authentication key over a standard network connection initiated from the SiteProtector console.
4. Press ENTER.

   The message `Auto Import configured successfully` appears.
5. Press ENTER to return to the Configuration menu.

Configuring the RSKILL Response

Introduction

The RSKILL response enables you to minimize attack damage and stop many attacks before damage is done. You can use RSKILL to prevent unauthorized hosts or networks from connecting to services on the monitored computer. When the appliance detects an attack, it terminates or resets the connection to the targeted computer. You can configure the kill interface for the RSKILL response from the local configuration interface or from the management console.

Reference: For more information about the RSKILL response, see the *ISS Response, Policy, and Event Collector Help*.

Procedure

To configure the RSKILL response:

1. Set up a local configuration interface and log in, as described in "Setting Up a Local Configuration Interface and Logging In" on page 3.
2. On the Configuration menu, select **Configure RSKill**, and then press ENTER.

   The RSKill Configuration screen appears.
3. Do you want to use a DHCP server?
   - If *yes*, press the SPACE BAR to select DHCP.
   - If *no*, type the static addresses in the **IP Address**, **Subnet Mask**, and **Gateway**.

   Tip: To move from one field to the next, press TAB.

   Note: The RSKill response occurs in stealth mode. The appliance uses these static network addresses to determine the gateway MAC address. If the appliance cannot determine the MAC address, then you must manually enter the address on the next screen.
4. Press ENTER.

   The appliance saves the settings, and then attempts to determine the gateway MAC address.
5. Did the appliance determine its MAC address?
   - If *yes*, press ENTER.
   - If *no*, type the MAC address.

   Note: If you do not know the MAC address, contact your system administrator.
6. Press ENTER to return to the Configuration menu.

Configuring Packet Captures

Introduction

The Proventia A604, A1204, and A1204F appliances can capture attack packets that you can view and analyze from the SiteProtector management console. The system associates these captured packets with specific events, which can benefit a forensic investigation.

Where configured

You configure packet captures on the SiteProtector management console.

Overview

To configure packet captures, you must first set the LOGDB response in the Policy Editor to the LogwithRaw response name. The LOGDB response displays the detected event on the monitoring console. Together with the Display response, raw data from the LogWithRaw response is translated into a format that appears in the Event Details window on the management console. There are two packet capture files: **FirstPacket.enc** and **LastPacket.enc**. These packet capture files display as icons in the Event Details window, under the Attribute value.

Reference: For more information about using the Policy Editor, see the *ISS Response, Policy, and Event Collector Help*.

Setting the LogwithRaw response

To set the LOGDB response to LogwithRaw:

1. In the SiteProtector Site Manager, select the appliance.
2. Select **Apply Policy**.

   The Select Policy window opens.
3. Select the policy, and then click **Derive New**.
4. In the Policy Editor window, select the tab for the type of event to which you are assigning responses.
5. In the signature pane, click the signature to which you want to assign responses.
6. The response list in the right pane displays the responses that are currently assigned to this signature.
7. Select the check box next to the LOGDB response type.
8. Select the **LogwithRaw** response name.
9. From the **File** menu, select **Save**.

   A confirmation message appears.
10. Click **OK**.
11. From the **File** menu, select **Exit**.
12. Select the policy, and then click **OK**.

    The policy opens.
13. Verify that the policy is correct, and then click **OK**.

Viewing packet captures

To view packet captures:

1. In the SiteProtector SiteManager, select the **Network Sensor Analysis** tab.

   A list of events by tag name appears.
2. Select a row, and then right-click the tag name.

3. Select **View Event Details**.

   The Event Details window appears.

4. View the Event Attribute Data pairs, and then look at the **Attribute** value.

   An icon appears under the **Attribute** value to indicate that packet data has been captured.

5. Double-click the icon.

   A text file appears in the right pane. This text file includes information about data in the packet, such as URLs, IP addresses, and cookies.

   Note: When you scroll to a new event, the Help information returns to the right pane.

Customizing the No Packet Alert

Introduction

The Proventia appliance can send an alert to the management console when the appliance is not analyzing traffic. Sending a no packet alert is beneficial in a reconfigured network that does not pass traffic to the appliance. The no packet alert also provides a quick and effective way to determine whether the appliance is properly monitoring traffic.

Reference: For more information about configuring the appliance, see the *ISS Response, Policy, and Event Collector Help*.

Where configured

You configure the no packet alert on the SiteProtector management console.

Default parameter settings

The no packet alert parameters are enabled by default in the management console. Under most circumstances, you do not need to reconfigure these parameter settings. However, you may want to customize the settings if the level of network activity is low. You may also want to change the interval at which the network measures traffic.

Audit events

No packet alert parameter settings correspond to each of the four adapters (A, B, C, and D) that receive traffic on the appliance. These settings affect the Network_Quiet (high) and Network_Normal (low) audit events.

- The Network_Quiet event indicates that the level of network activity is unusually quiet. The packets per sampling interval has dropped below the configured low-water mark.
- The Network_Normal event indicates that the appliance is properly receiving traffic and the level of network activity has returned to normal.

Default parameters

The following table describes the default parameters that support no packet alert on the Proventia appliance:

Name	Value	Description
traffic.sample	true	Enables traffic sampling to detect unusual levels of network activity. Affects the Network_Quiet (high) and Network_Normal (low) audit events.
traffic.sample.interval	300 seconds	Determines the rate at which traffic flow is sampled, for the purpose of detecting abnormal levels of network activity. Affects the Network_Quiet and Network_Normal audit events.
adapter.A.low-water adapter.B.low-water adapter.C.low-water adapter.D.low-water	0	Indicates the minimum number of packets per traffic sampling interval expected on the adapter (A, B, C or D) on the appliance. If the packet rate falls below this threshold, the network issues a warning that network traffic is abnormally low. Low traffic can indicate a loss of network connectivity or a change in the sensor's spanning port configuration.

Table 5: *No packet alert parameters*

Name	Value	Description
adapter.A.high-water adapter.B.high-water adapter.C.high-water adapter.D.high-water	2	Indicates the number of packets per traffic sampling interval expected on the adapter (A, B, C, or D) on the appliance. The network uses the high-water mark to prevent multiple low-traffic warnings when the traffic flow is hovering around the low-water mark. The network also uses the high-water mark as the threshold to issue the Network_Normal event.

Table 5: *No packet alert parameters*

Procedure

Open the SiteProtector management console. Use the **Advanced Parameters** tab on the Sensor Properties window to view or customize no packet alert settings.

To customize the no packet alert:

1. In the SiteProtector grouping tree, select the group to which the appliance is assigned, and then select the **Sensor** tab in the right pane.

   A list of sensors and appliances appears.
2. Right-click the appliance, and then select **Network Sensor**.
3. Select **Edit Properties**.

   The Sensor Properties window appears.
4. In the Sensor Properties window, select the **Advanced Parameters** tab.
5. Select the parameter name, and then click **Edit**.

   The Advanced Value window appears.
6. Edit the value setting, and then click **OK**.
7. Repeat Steps 5 and 6 for each parameter you want to configure.
8. Click **OK**.

   The Sensor Properties window appears.

Changing the Port ID Value

Introduction

The Proventia A604, A1204, and A1204F appliances can identify the specific port that detected an event. This enables you to identify the affected network segment. Identifying the port and network segment aids forensic investigation when up to four unrelated segments are monitored on one appliance.

Where configured

You change the port ID value on the SiteProtector management console.

Port and adapter names

Four ports on the back of the appliance, labeled A, B, C, and D, correspond to a parameter setting for an adapter that is enabled on the management console. The corresponding settings are adapter.A.name, adapter.B.name, adapter.C.name, and adapter.D.name. Events detected by the adapter for a port appear in the Event Details window.

Parameters settings for adapters

The parameter settings for the adapters are enabled by default in the management console. Under most circumstances, you do not need to change these parameters. However, you may want to customize the parameters if you change the name of the adapter or change the segment that the adapter is monitoring.

Changing the port ID value

Open the SiteProtector management console. Use the **Advanced Parameters** tab on the Sensor Properties window to view or change the port ID value.

To change the port ID value:

1. In the SiteManager grouping tree, select the group to which the appliance is assigned, and then select the **Sensor** tab in the right pane.

   A list of sensors and appliances appears.
2. Right-click the appliance, and then select **Network Sensor**.
3. Select **Edit Properties**.

   The Sensor Properties window appears.
4. In the Sensor Properties window, select the **Advanced Parameters** tab.
5. Select the adapter name, and then click **Edit**.

   The Advanced Value window appears.
6. Change the adapter value for the port ID, and then click **OK**.

   Example: You may want to change the adapter to correspond to a segment. For example, the value **A** could change to **Marketing Segment 3**.
7. Repeat Steps 5 and 6 for each adapter name you want to change.
8. Click **OK**.

   The Sensor Properties window appears.

Viewing events generated for a port

To events generated for a port:

1. In the SiteProtector SiteManager, select the **Sensor Analysis** tab.

   A list of events appears.
2. Select an event, and then right-click it.
3. Select **View event details**.

   The Event Details window appears.
4. In the **Attribute Pair**, locate the adapter name, and then locate the corresponding port ID.
5. Click **Next** to display the next alert, click **OK** to close the window.

Shutting Down or Rebooting the Appliance

Introduction

You can shut down or reboot the appliance using the local configuration interface.

Procedure

To shut down or reboot the appliance:

1. Set up a local configuration interface and log in, as described in "Setting Up a Local Configuration Interface and Logging In" on page 3.
2. On the Configuration menu, select **Shutdown/Reboot A604 or A1204**, and then press ENTER.
3. Do one of the following:
   - To reboot the appliance, type `R`.

     The appliance reboots and displays the Login prompt.
   - To shut down the appliance, type `S`.

     The appliance shuts down and displays a message when it is safe for you to turn off the power.

Logging Out of the Local Configuration Interface

Introduction

Log out of the local configuration interface when you are finished viewing or changing the appliance's settings.

Procedure

To log out of the local configuration interface:

- On the Configuration menu, select **Logout**, and then press ENTER.

  The appliance displays the Login prompt.

Chapter 3

Troubleshooting

Overview

Introduction

This chapter describes techniques for troubleshooting appliance problems, and includes the procedures for reinstalling the appliance software.

In this chapter

This chapter contains the following topics:

Reinstalling the Appliance Software

Introduction

You can reinstall the appliance by using the *Proventia Appliance Recovery CD*. The CD reinstalls the original, unconfigured software. To reinstall the software, you must complete the following procedures:

- reinstall the appliance
- log in and change the password
- configure the network and host
- configure the date and time
- configure the agent name
- configuring the RSKILL response
- apply settings and log out

Note: After rebooting with the recovery CD, the appliance reverts to the default login name and password.

Prerequisites

Before you configure the appliance, you must have completed the following prerequisites:

- Verify the IP address, subnet mask, and default gateway of the appliance's management interface.
- Verify the hostname (required), domain name (recommended), and DNS name server (recommended) for the appliance.
- Verify that the appliance is running. If your appliance is not running, contact ISS Customer Support at support@iss.net.

Reinstalling the appliance

To reinstall the appliance:

1. If there is a bezel cover on the front of the appliance, remove it.
2. Place the *Proventia Appliance Recovery CD* in the CD-ROM drive.
3. Connect a computer or monitor and keyboard to the appliance.

   Reference: For more information, see "Setting Up a Local Configuration Interface and Logging In" on page 3.
4. Reboot the appliance. See "Shutting Down or Rebooting the Appliance" on page 22.

   Tip: You can manually turn the power off and on if the appliance is not responding.

   The appliance reboots and reloads the operating system.
5. Type **`reinstall`**, and then press ENTER.

   The appliance displays status messages, ejects the CD, and then reboots.
6. Go to "Logging in and changing the password," next in this topic.

Logging in and changing the password

To log in and change the password:

1. When the appliance has rebooted, type **`admin`** at the unconfigured login prompt, and then press ENTER.
2. Type **`admin`** at the Password prompt, and then press ENTER.

The Software License Agreement appears.

3. Read the Software License Agreement, and then type **y** to accept its terms.

   The appliance displays a change password prompt.

4. Type the old password, **admin**, and then type a new password.

   Note: You must use a minimum of six characters.

5. Retype the new password to confirm it, and then press ENTER.

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

6. Press ENTER.

   The Network Configuration screen appears.

7. Go to "Configuring the network and host," next in this topic.

Configuring the network and host

To configure the network and host:

1. Type the **IP Address**, **Subnet Mask**, and **Gateway** for the appliance management interface, and then press ENTER.

   The appliance displays a progress message while it configures the network settings, and then displays the message `Network configured`.

2. Press ENTER.

   The Host Configuration screen appears.

3. Type the **Hostname** (required), **Domain Name** (recommended), and **Name Server** (recommended) for the appliance, and then press ENTER.

   Note: The appliance uses domain names and 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 response on the management console. The appliance must have network access to the mail server. For more information, see the management console's user documentation.

   The appliance displays a progress message while it configures the host settings, and then displays the message `Host configuration has been saved` when the configuration is complete.

4. Press ENTER.

   The Timezone Configuration screen appears.

5. Go to "Configuring the date and time," next in this topic.

Configuring the date and time

To configure the date and time at which events occur:

1. Select the continent or ocean in which the appliance is located, and then press ENTER.
2. Select the country in which the appliance is located, and then press ENTER.
3. Select the region in which 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. Type **y** to confirm, and then press ENTER.

   The Date/Time Configuration screen appears.

5. Press ENTER to accept the **Date** and **Time** for the appliance, or type a new time and press ENTER.

   Note: Use the format [HH:MM:SS] and a 24-hour clock.

6. Press ENTER.

   The Agent Name Configuration screen appears.

7. Go to "Configuring the agent name," next in this topic.

Configuring the agent name

To configure the agent name:

1. Press ENTER to accept the default agent name, or type a specific name, and then press ENTER.

   Note: This is the name that appears for this appliance in your management interface. ISS recommends that you select a name that corresponds to the appliance's geography, business unit, building address, or some other name that is meaningful to you.

   The appliance continues to apply your configuration settings. The status bar displays a message when the configuration ends.

2. Press ENTER.

   The RSKill Configuration screen appears.

3. Go to "Configuring the RSKILL response," next in this topic.

Configuring the RSKILL response

To configure the RSKILL response:

1. Do you want to configure the RSKill response?
   - If *yes*, type **y**, and then go to Step 2.
   - If *no*, type **n**, and then go to Step 1 in "Applying settings and logging out," next in this topic.

   Note: When the appliance detects an attack, the RSKill response terminates or resets the connection to the targeted computer.

2. Do you want to use a DHCP server?
   - If *yes*, press the SPACE BAR to select DHCP.
   - If *no*, type the static addresses in the **IP Address**, **Subnet Mask**, and **Gateway**.

   Tip: To move from one field to the next, press TAB.

   Note: The RSKill response occurs in stealth mode. The appliance uses these static network addresses to determine the gateway MAC address. If the appliance cannot determine the MAC address, then you must manually enter the address on the next screen.

3. Press ENTER.

   The appliance attempts to determine and display the gateway MAC address.

4. Did the appliance determine its MAC address?
   - If *yes*, press ENTER.
   - If *no*, type the MAC address.

   Note: If you do not know the MAC address, contact your system administrator.

5. Press ENTER.

   The appliance continues to apply your configuration settings, and then displays a message when the configuration is complete.

6. Go to "Applying settings and logging out," next in this topic.

Applying settings and logging out

To apply settings and log out:

1. Press ENTER to continue.

   The appliance displays a message that it will now log you off. You can log back in at any time to change configuration settings.

2. Press ENTER to log out.

   The login prompt appears.

Using Advanced Settings

Changing advanced settings

The appliance software includes advanced configuration settings that are intended to provide ISS Customer Support with additional troubleshooting options. You may need to change these settings to help resolve problems with the appliance software.

⚠ **Caution:** ISS recommends that you contact Technical Support before you change or reconfigure the advanced settings. Changing these settings may adversely affect the appliance operation if they are not properly configured.

Index

p

q

r

s

t

v

w

Internet Security Systems, Inc. Software License Agreement

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

1. License - Upon payment of the applicable fees, Internet Security Systems, Inc. ("ISS") grants to you as the only end user ("Licensee") a nonexclusive and nontransferable, limited license for the accompanying ISS software product in machine-readable form and the related documentation ("Software") and the associated license key for use only on the specific network configuration, for the number and type of devices, and for the time period ("Term") that are specified in Licensee's purchase order, as accepted and invoiced by ISS. ISS limits use of Software based upon the number and type of devices upon which it may be installed, used, gather data from, or report on, depending upon the specific Software licensed. A device includes any network addressable device connected to Licensee's network, including remotely, including but not limited to personal computers, workstations, servers, routers, hubs and printers. A device may also include ISS hardware delivered with pre-installed Software and the license associated with such shall be a non-exclusive, nontransferable license to use such pre-installed Software only in conjunction with the ISS hardware with which it is originally supplied and only during the usable life of such hardware. Except as provided in the immediately preceding sentence, Licensee may reproduce, install and use the Software on multiple devices, provided that the total number and type are authorized in Licensee's purchase order, as accepted by ISS. Licensee acknowledges that the license key provided by ISS may allow Licensee to reproduce, install and use the Software on devices that could exceed the number of devices licensed hereunder. Licensee shall implement appropriate safeguards and controls to prevent loss or disclosure of the license key and unauthorized or unlicensed use of the Software. Licensee may make a reasonable number of backup copies of the Software and the associated license key solely for archival and disaster recovery purposes. Use of third party product(s) supplied hereunder, if any, will be subject solely to the manufacturer's terms and conditions that will be provided to Licensee upon delivery. ISS will pass any third party product warranties through to Licensee to the extent authorized.
2. Evaluation License - If ISS is providing Licensee with the Software and related documentation on an evaluation trial basis at no cost, such license Term is 30 days from installation, unless a longer period is agreed to in writing by ISS. ISS recommends using Software for evaluation in a non-production, test environment. The following terms of this Section 2 additionally apply and supercede any conflicting provisions herein. Licensee agrees to remove the Software from the authorized platform and return the Software and documentation to ISS upon expiration of the evaluation Term unless otherwise agreed by the parties in writing. ISS has no obligation to provide support, maintenance, upgrades, modifications, or new releases to the Software under evaluation. **LICENSEE AGREES THAT THIS SOFTWARE AND RELATED DOCUMENTATION ARE BEING DELIVERED "AS IS " WITHOUT WARRANTIES OF ANY KIND, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, TITLE OR NON-INFRINGEMENT. IN NO EVENT WILL ISS BE LIABLE TO LICENSEE OR ANY OTHER PERSON FOR DAMAGES, DIRECT OR INDIRECT, OF ANY NATURE, OR EXPENSES INCURRED BY LICENSEE IN CONNECTION WITH THE SOFTWARE LICENSED HEREUNDER. LICENSEE'S SOLE AND EXCLUSIVE REMEDY SHALL BE TO TERMINATE THIS EVALUATION LICENSE BY WRITTEN NOTICE TO ISS.**
3. Covenants - ISS reserves all intellectual property rights in the Software. Licensee agrees: (i) the Software is owned by ISS and/or its licensors, is a valuable trade secret of ISS, and is protected by copyright laws and international treaty provisions; (ii) to take all reasonable precautions to protect the Software from unauthorized access, disclosure, copying or use; (iii) not to modify, adapt, translate, reverse engineer, decompile, disassemble, or otherwise attempt to discover the source code of the Software; (iv) not to use ISS trademarks; (v) to reproduce all of ISS' and its licensors' copyright notices on any copies of the Software; and (vi) not to transfer, lease, assign, sublicense, or distribute the Software or make it available for time-sharing, service bureau, managed services offering, or on-line use.
4. Support and Maintenance - Maintenance for ISS Software includes technical support and electronic delivery to Licensee of software and security content updates as they become available to ISS' supported customers generally. Depending upon what maintenance programs Licensee has purchased, maintenance for ISS hardware delivered with pre-installed Software may include (i) technical support for the pre-installed Software and ISS hardware including the repair, replacement or advanced exchange of the ISS hardware, and/or (ii) related Software security content updates for the pre-installed Software. During the period for which Licensee has paid the applicable maintenance fees, ISS will provide maintenance in accordance with its prevailing Maintenance and Support Policy that is available at http://documents.iss.net/maintenance_policy.pdf.
5. Limited Warranty - The commencement date of this limited warranty is the date on which ISS furnishes to Licensee the license key for the Software. For a period of ninety (90) days after the commencement date or for the Term (whichever is less), ISS warrants that the Licensed Software will conform to material operational specifications described in its then current documentation. However, this limited warranty shall not apply unless (i) the Software is installed, implemented, and operated in accordance with all written instructions and documentation supplied by ISS, (ii) Licensee notifies ISS in writing of any nonconformity within the warranty period, and (iii) Licensee has promptly and properly installed all corrections, new versions, and updates made available by ISS to Licensee. Furthermore, this limited warranty shall not apply to nonconformities arising from any of the following: (i) misuse of the Software, (ii) modification of the Software, (iii) failure by Licensee to utilize compatible computer and networking hardware and software, or (iv) interaction with software or firmware not provided by ISS. If Licensee timely notifies ISS in writing of any such nonconformity, then ISS shall repair or replace the Software or, if ISS determines that repair or replacement is impractical, ISS may terminate the applicable licenses and refund the applicable license fees, as the sole and exclusive remedies of Licensee for such nonconformity. **THIS WARRANTY GIVES LICENSEE SPECIFIC LEGAL RIGHTS, AND LICENSEE MAY ALSO HAVE OTHER RIGHTS THAT VARY FROM JURISDICTION TO JURISDICTION. ISS DOES NOT WARRANT THAT THE SOFTWARE WILL MEET LICENSEE'S REQUIREMENTS, THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT ALL SOFTWARE ERRORS WILL BE CORRECTED. LICENSEE UNDERSTANDS AND AGREES THAT LICENSED SOFTWARE IS NO GUARANTEE AGAINST INTRUSIONS, VIRUSES, TROJAN HORSES, WORMS, TIME BOMBS, CANCELBOTS OR OTHER SIMILAR HARMFUL OR DELETERIOUS PROGRAMMING ROUTINES AFFECTING LICENSEE'S NETWORK, OR THAT ALL SECURITY THREATS AND VULNERABILITIES WILL BE DETECTED OR THAT THE PERFORMANCE OF THE LICENSED SOFTWARE WILL RENDER LICENSEE'S SYSTEMS INVULNERABLE TO SECURITY BREACHES. THE REMEDIES SET OUT IN THIS SECTION 5 ARE THE SOLE AND EXCLUSIVE REMEDIES FOR BREACH OF THIS LIMITED WARRANTY.**
6. Warranty Disclaimer - **EXCEPT FOR THE LIMITED WARRANTY PROVIDED ABOVE, THE SOFTWARE IS PROVIDED "AS IS" AND ISS HEREBY DISCLAIMS ALL WARRANTIES, BOTH EXPRESS AND IMPLIED, INCLUDING IMPLIED WARRANTIES RESPECTING MERCHANTABILITY, TITLE, NONINFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE. SOME JURISDICTIONS DO NOT ALLOW DISCLAIMERS OF IMPLIED WARRANTIES, SO THE ABOVE LIMITATION MAY NOT APPLY TO LICENSEE. LICENSEE EXPRESSLY ACKNOWLEDGES THAT NO REPRESENTATIONS OTHER THAN THOSE CONTAINED IN THIS LICENSE HAVE BEEN MADE REGARDING THE GOODS OR SERVICES TO BE PROVIDED HEREUNDER, AND THAT LICENSEE HAS NOT RELIED ON ANY REPRESENTATION NOT EXPRESSLY SET OUT IN THIS LICENSE.**
7. Proprietary Rights - ISS represents and warrants that ISS has the authority to license the rights to the Software that are granted herein. ISS shall defend and indemnify Licensee from any final award of costs and damages against Licensee for any actions based on infringement of any U.S. copyright, trade secret, or patent as a result of the use or distribution of a current, unmodified version of the Software; but only if ISS is promptly notified in writing of any such suit or claim, and only if Licensee permits ISS to defend, compromise, or settle same, and only if Licensee provides all available information and reasonable assistance. The foregoing is the exclusive remedy of Licensee and states the entire liability of ISS with respect to claims of infringement or misappropriation relating to the Software.
8. Limitation of Liability - **ISS' ENTIRE LIABILITY FOR MONETARY DAMAGES ARISING OUT OF THIS LICENSE SHALL BE LIMITED TO THE AMOUNT OF THE LICENSE FEES ACTUALLY PAID BY LICENSEE UNDER THIS LICENSE, PRORATED OVER A THREE-YEAR TERM FROM THE DATE LICENSEE RECEIVED THE SOFTWARE. IN NO EVENT SHALL ISS BE LIABLE TO LICENSEE UNDER ANY THEORY INCLUDING CONTRACT AND TORT (INCLUDING NEGLIGENCE AND STRICT PRODUCTS LIABILITY) FOR ANY SPECIAL, PUNITIVE, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING, BUT NOT LIMITED TO, COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, DAMAGES FOR LOST PROFITS, LOSS OF DATA, LOSS OF USE, OR COMPUTER HARDWARE MALFUNCTION, EVEN IF ISS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.**
9. Termination - Licensee may terminate this License at any time by notifying ISS in writing. All rights granted under this License will terminate immediately, without prior written notice from ISS, at the end of the term of the license, if not perpetual. If Licensee fails to comply with any provisions of this License, ISS may immediately terminate this License if such default has not been cured within ten (10) days following written notice of default to Licensee. Upon termination or expiration of a license for Software, Licensee shall cease all use of such Software, including Software pre-installed on ISS hardware, and destroy all copies of the Software and associated documentation. Termination of this License shall not relieve Licensee of its obligation to pay all fees incurred prior to such termination and shall not limit either party from pursuing any other remedies available to it.
10. General Provisions - This License, together with the identification of the Software, pricing and payment terms stated in the applicable Licensee purchase order as accepted by ISS constitute the entire agreement between the parties respecting its subject matter. Standard and other additional terms or conditions contained in any purchase order or similar document are hereby expressly rejected and shall have no force or effect. Unless otherwise set forth in the applicable purchase order, ISS Software is delivered to Customer by supplying Customer with license key data. If Customer has not already downloaded the Software and documentation, then it is available for download at http://www.iss.net/download/. All ISS hardware with pre-installed Software is delivered f.o.b. origin. This License will be governed by the substantive laws of the State of Georgia, USA, excluding the application of its conflicts of law rules. This License will not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded. If any part of this License is found void or unenforceable, it will not affect the validity of the balance of the License, which shall remain valid and enforceable according to its terms. This License may only be modified in writing signed by an authorized officer of ISS.
11. Notice to United States Government End Users - Licensee acknowledges that any Software furnished under this License is commercial computer software and any documentation is commercial technical data developed at private expense and is provided with RESTRICTED RIGHTS. Any use, modification, reproduction, display, release, duplication or disclosure of this commercial computer software by the United States Government or its agencies is subject to the terms,

conditions and restrictions of this License in accordance with the United States Federal Acquisition Regulations at 48 C.F.R. Section 12.212 and DFAR Subsection 227.7202-3 and Clause 252.227-7015 or applicable subsequent regulations. Contractor/manufacturer is Internet Security Systems, Inc., 6303 Barfield Road, Atlanta, GA 30328, USA.

12. Export and Import Controls; Use Restrictions - Licensee will not transfer, export, or reexport the Software, any related technology, or any direct product of either except in full compliance with the export controls administered by the United States and other countries and any applicable import and use restrictions. Licensee agrees that it will not export or reexport such items to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Commerce Department's Denied Persons List or Entity List or such additional lists as may be issued by the U.S. Government from time to time, or to any country to which the United States has embargoed the export of goods, or for use with chemical or biological weapons, sensitive nuclear end-uses, or missiles. Licensee represents and warrants that it is not located in, under control of, or a national or resident of any such country or on any such list. Many ISS software products include encryption and export outside of the United States or Canada is strictly controlled by U.S. laws and regulations. Please contact ISS' Customer Operations for export classification information relating to the Software (customer_ops@iss.net). Licensee understands that the foregoing obligations are U.S. legal requirements and agrees that they shall survive any term or termination of this License.
13. Authority - Because the Software is designed to test or monitor the security of computer network systems and may disclose or create problems in the operation of the systems tested, Licensee and the persons acting for Licensee represent and warrant that: (a) they are fully authorized by the Licensee and the owners of the computer network for which the Software is licensed to enter into this License and to obtain and operate the Software in order to test and monitor that computer network; (b) the Licensee and the owners of that computer network understand and accept the risks involved; and (c) the Licensee shall procure and use the Software in accordance with all applicable laws, regulations and rules.
14. Disclaimers - Licensee acknowledges that some of the Software is designed to test the security of computer networks and may disclose or create problems in the operation of the systems tested. Licensee further acknowledges that the Software is not fault tolerant and is not designed or intended for use in hazardous environments requiring fail-safe operation, including, but not limited to, aircraft navigation, air traffic control systems, weapon systems, life-support systems, nuclear facilities, or any other applications in which the failure of the Licensed Software could lead to death or personal injury, or severe physical or property damage. ISS disclaims any implied warranty of fitness for High Risk Use. Licensee accepts the risk associated with the foregoing disclaimers and hereby waives all rights, remedies, and causes of action against ISS and releases ISS from all liabilities arising therefrom.
15. Confidentiality - "Confidential Information" means all information proprietary to a party or its suppliers that is marked as confidential. Each party acknowledges that during the term of this Agreement, it will be exposed to Confidential Information of the other party. The obligations of the party ("Receiving Party") which receives Confidential Information of the other party ("Disclosing Party") with respect to any particular portion of the Disclosing Party's Confidential Information shall not attach or shall terminate when any of the following occurs: (i) it was in the public domain or generally available to the public at the time of disclosure to the Receiving Party, (ii) it entered the public domain or became generally available to the public through no fault of the Receiving Party subsequent to the time of disclosure to the Receiving Party, (iii) it was or is furnished to the Receiving Party by a third parting having the right to furnish it with no obligation of confidentiality to the Disclosing Party, or (iv) it was independently developed by the Receiving Party by individuals not having access to the Confidential Information of the Disclosing Party. Each party acknowledges that the use or disclosure of Confidential Information of the Disclosing Party in violation of this License could severely and irreparably damage the economic interests of the Disclosing Party. The Receiving Party agrees not to disclose or use any Confidential Information of the Disclosing Party in violation of this License and to use Confidential Information of the Disclosing Party solely for the purposes of this License. Upon demand by the Disclosing Party and, in any event, upon expiration or termination of this License, the Receiving Party shall return to the Disclosing Party all copies of the Disclosing Party's Confidential Information in the Receiving Party's possession or control and destroy all derivatives and other vestiges of the Disclosing Party's Confidential Information obtained or created by the Disclosing Party. All Confidential Information of the Disclosing Party shall remain the exclusive property of the Disclosing Party.
16. Compliance - From time to time, ISS may request Licensee to provide a certification that the Licensed Software is being used in accordance with the terms of this License. If so requested, Licensee shall verify its compliance and deliver its certification within forty-five (45) days of the request. The certification shall state Licensee's compliance or non-compliance, including the extent of any non-compliance. ISS may also, at any time, upon thirty (30) days prior written notice, at its own expense appoint a nationally recognized independent auditor, to whom Licensee has no reasonable objection, to audit and examine records at Licensee offices during normal business hours, solely for the purpose of confirming that Licensee's use of the Licensed Software is in compliance with the terms of this License. ISS will use commercially reasonable efforts to have such audit conducted in a manner such that it will not unreasonably interfere with the normal business operations of Licensee. If such audit should reveal that use of the Licensed Software has been expanded beyond the scope of use and/or the number of Authorized Devices or Licensee certifies such non-compliance, ISS shall have the right to charge Licensee the applicable current list prices required to bring Licensee in compliance with its obligations hereunder with respect to its current use of the Licensed Software. In addition to the foregoing, ISS may pursue any other rights and remedies it may have at law, in equity or under this License.

Revised May 13, 2003.