IBM ISS Proventia Network Security Controller

User Guide

IBM Internet Security Systems

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America.

March 27, 2009

Contents

Preface

Overview

Introduction This guide is designed to help you connect and configure your Proventia Network Security Controller (NSC).

Scope This guide includes basic information and required procedures for connecting the unit and configuring basic settings.

Audience This guide is intended for network system administrators responsible for installing and configuring the network and system appliances. A fundamental knowledge of network policies and IP network configuration is helpful.

About Proventia appliance documentation

Introduction

This guide explains how to set up and configure the Proventia Network Security Controller for use with Proventia Network Intrusion Prevention System (IPS) appliances.

Locating additional documentation

Additional documentation about IBM ISS products is available on the IBM ISS Web site at http://www.iss.net/support/documentation/.

Related publications

See the following documents for more information about the IPS appliances supported by Proventia Network Security Controller:

Document	Contents
IBM Proventia GX5000 Series Getting Started Card	Instructions for connecting and configuring a GX5000 Series IPS appliance
IBM Proventia GX5000 Series Getting Started Card	Instructions for connecting and configuring a GX6000 Series IPS appliance
IBM Proventia Network Intrusion Prevention System G and GX Appliance User Guide	Overviews and procedures for creating and managing policies and responses, as well as maintaining appliance settings.

Table 1: *Reference documentation*

Knowledgebase

The IBM ISS support knowledgebase is a valuable source of information. Visit the knowledgebase at http://www.iss.net/support/knowledgebase/. You can search the knowledgebase using key works or Answer IDs.

Tip: See Answer ID 3321 for the latest tips and known issues for Proventia Network Intrusion Prevention System appliances.

Licensing agreement

For licensing information on IBM Internet Security System products, download the IBM Licensing Agreement from http://www.ibm.com/services/us/iss/html/contracts_landing.html. In addition, the licensing information is included on the CD-ROM that is provided with the unit.

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 task bar or menu bar.	From the task bar, select **Start→Run**. On the **File** menu, select **Utilities→Compare Documents.**

Table 2: *Typographic conventions for procedures*

Command conventions

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

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

Table 3: *Typographic conventions for commands*

Getting Technical Support

Introduction

IBM Internet Security Systems provides technical support through its Web site and by email or telephone.

The IBM ISS Web site

The Customer Support Web page (http://www.ibm.com/services/us/iss/support/) provides direct access to online user documentation, current versions listings, detailed product literature, white papers, and the Technical 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 IBM ISS published holidays **Note:** If your local support office is located outside the Americas, you may call or send an email to the Americas office for help during off-hours.

Table 4: *Hours for technical support*

Contact information

For contact information, go to the Contact us section of the Customer Support Web page at http://www.ibm.com/services/us/iss/support/.

Chapter 1

Introducing the Proventia Network Security Controller

Overview

Introduction

Proventia Network Security Controller (NSC) is a 10 Gigabit (Gb) to 1 Gb intelligent link aggregation/segregation bypass switch. Proventia Network Security Controller provides twenty-four 1 Gb ports and four 10 Gb SR or LR ports. This chapter introduces the features and operating principles for Proventia Network Security Controller.

In this chapter

This chapter contains the following topics:

About Proventia Network Security Controller

Overview

Before you add the unit to your network, familiarize yourself with the controller's features.

Front panel

The front panel of Proventia Network Security Controller is illustrated in the following figure.

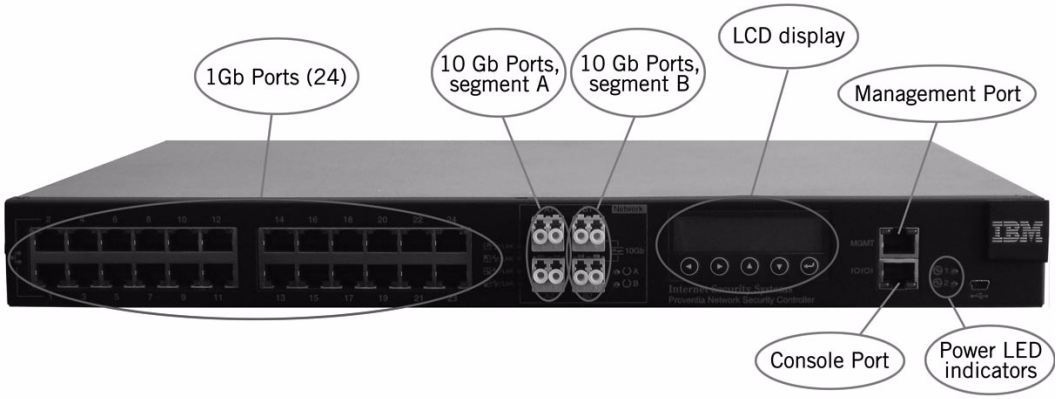


Figure 1: *Front panel*

Ethernet ports

- 1 Gb ports (24 total)
- LC-type connectors for 10 Gb interface. (4 total)

Device Management

- LCD
- Ethernet management port
- Serial console port

Status LEDs

- Power LEDs
- Active/Bypass status LEDs

Power adapter

This unit is intended to be powered by a UL Listed power supply, with rated output: 12 VDC, 5 A, marked LPS or NEC Class 2. Use only a suitable power supply with these specifications to power the product.

Features

Overview

This section describes the features of Proventia Network Security Controller.

List of features

- 10Gb to 1Gb link (4, 6, or 8 ports) aggregation/segregation
- Independent 10Gb segments (2)
- 10GBASE-SR/LR Passive/Active Network Bypass (configurable)
- Flexible management interface
- Secure WEB management Interface (SSL)
  - SNMP, CLI by serial console or SSH
  - LCD
- Auto heartbeat
- E-mail notification for status changes
- Field programmable over Ethernet or Serial Console Port
- Power fail protection

Secured Web management

Proventia Network Security Controller provides a secured Web management interface. You can use the management interface to configure and monitor Proventia Network Security Controller from any Web browser. The management port for Proventia Network Security Controller has a default IP address assigned. You can retrieve or change the IP address by using command line parameters.

Access the management interface by opening a Web browser, and typing **`https://`** followed by the management port IP address. The default IP address for the management port is 192.168.0.111. The default management port URL is **`https://192.168.0.111.`**

The management interface is covered in more detail in Chapter 3, "Configuring Proventia Network Security Controller Through the Management Interface."

Power fail protection

Proventia Network Security Controller provides two redundant power supplies for maximum reliability.

In case of a power failure, two optical switches effectively remove Proventia Network Security Controller from the network. Then, the unit functions as two straight cables.

Basic operation

Overview

This section describes some of the basic operating principles for Proventia Network Security Controller.

Independent segments

The Proventia Network Security Controller consists of two independent 10Gb segments. Each 10Gb segment consist of two 10Gb ports. The 1Gb segments are mapped to the 10Gb segments in blocks of 8, 12, or 16, depending on how you configure the segments.

Each segment operates independently and is controlled by dedicated optical switches for bypass operation.

Sample port mapping

This section outlines a basic port mapping scenario between the 10Gb ports and the 1Gb ports. In this example, the 1Gb ports are evenly divided between Segments A and B to support two Proventia Intrusion Prevention System (IPS) appliances using six 1Gb segments each.

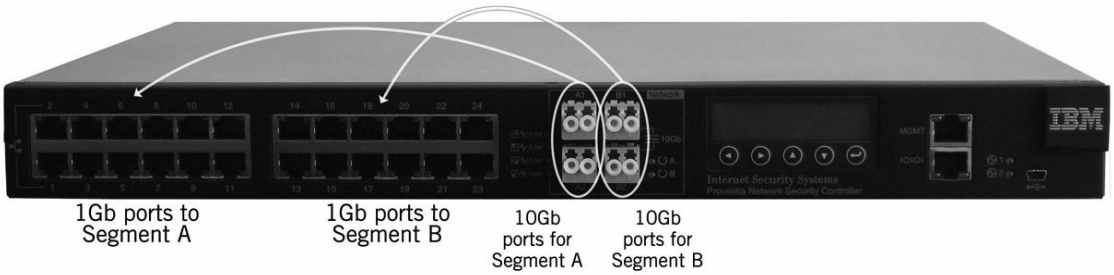


Figure 2: *Sample port mapping for Segments A and B*

In this example, the 10Gb ports for Segment A correspond to the 1Gb ports labeled 1 through 12. The 10Gb ports for Segment B correspond to the 1Gb ports labeled 13 through 24.

This 10Gb port...	Maps to these 1Gb ports
A1	2, 4, 6, 8, 10, 12
A2	1, 3, 5, 7, 9, 11
B1	14, 16, 18, 20, 22, 24
B2	13, 15, 17, 19, 21, 23

Table 5: *Sample port mapping*

Different configurations

The port mapping may shift slightly to accommodate different segment configurations. For example, a configuration which uses all segments on an 8 segment IPS appliance requires more ports than are available in Segment A. Therefore, ports from Segment B are reassigned to Segment A to support this configuration.

Note: The segment configuration utility (available from the management interface) helps you determine the proper port mappings and cabling for the configuration you select.

Traffic path

Traffic comes in the 10Gb port (either Port A1 or B1) and out the corresponding 1Gb ports to the IPS appliance. After inspection, traffic comes from the IPS appliance back in through the 1Gb ports and out the corresponding 10Gb port (A2 or B2). Traffic also flows using the reverse path.

Switching modes

Proventia Network Security Controller provides three switching modes, as indicated in the following table.

Switching mode	Description
Active - not in bypass	Ethernet traffic comes in the 10Gb port, through the 1Gb ports to the IPS appliance, and out the 10Gb port.
Active - in bypass	Ethernet traffic goes in and out through the 10Gb ports. The traffic does not pass to the 1Gb ports or to the IPS appliance.
Bypass (pass through because of power failure)	The security controller functions as two straight cables in case of a power failure. Traffic enters and exits through the 10Gb ports without being sent to the 1Gb ports.

Table 6: *Switching modes*

Package contents

Overview

Verify that you have all of the package contents necessary to install and deploy Proventia Network Security Controller.

In the box

The following items should be included:

- One Proventia Network Security Controller
- Nine copper cables (green)*
  * If you want to connect all 24 1Gb ports, you will need to use additional cables.
- One blue console cable (blue)
- Two desk top power modules
- Power cords
- One CD

Chapter 2

Setting Up Proventia Network Security Controller

Overview

Introduction

This chapter contains the information you need in order to connect and configure the Proventia Network Security Controller.

In this chapter

This chapter contains the following topics:

Process overview: Configuring and deploying Proventia Network Security Controller

Overview

This section outlines the steps you need to complete in order to set up and introduce Proventia Network Security Controller into your network.

Process overview

Here is an overview of the process required to configure and deploy the Proventia Network Security Controller.

1. Rack the unit and the IPS appliances. Cable and configure the Proventia GX appliances using the instructions provided in the *Getting Started Guide* for the appliance.
2. Connect the power cables to the controller and to two different power sources (for added redundancy).
3. Use a browser to access the management interface and log in.
4. Verify that the unit is passing traffic.
5. Use the management interface to set the segment configuration. (This process maps the ports on the Proventia Network Security Controller to the ports on the appliances and sets bypass tolerances.)
6. Cable the Proventia Network Security Controller to the IPS appliances.

These steps are covered in more detail in the pages that follow.

Configuring and deploying Proventia Network Security Controller

Overview

This section contains detailed steps for configuring and deploying the security controller.

Rack the unit and appliances

1. Decide where to locate the Proventia Network Security Controller and the appliances.
2. Add the controller and the appliances to the rack.
3. Cable and configure the appliances using the instructions provided in the *Getting Started Guide* for the appliance.

Note: Proventia Network Security Controller has two 10Gb segments and can support up to two IPS appliances.

Connect the power cables

1. Plug the DC connector of each AC adapter into the Network Security Controller.
2. Plug one of the power cords into an AC outlet. Plug the other power cord into an AC outlet serviced by a different AC feed.

   Tip: Use independent AC power sources to maximize power redundancy in the event of AC power loss from a single source.
3. Check the power LEDs to confirm that the controller is receiving power.

Log on to the management interface

1. Use the management cable to connect a computer to the management port on the security controller.

   Important: Be sure to follow industry best practices for securing critical network infrastructure. Do no t connect the management port to any network that is open to external traffic. The management port should be connected only to a restricted network dedicated to managing the security controller and IPS appliances.
2. Start Internet Explorer.
3. Type **`https://192.168.0.111`**.

   Note: The default IP address for the management port is **`192.168.0.111`**. If you change the management port IP address, the URL to access the management port is changed to include the new IP address.
4. Log in to the management interface. The first time you connect, use the default user name and password.

Field	Default setting
User Name	**`admin`**
Password	**`admin`**

Note: If you change the default log in settings on the **Users** page of the management interface, the values you set are in effect for future log in attempts.

Verify that the unit is passing traffic

1. In the management interface, select the **Status** page.
2. Verify that the status for both 10Gb segments is “Bypass.”
3. Connect the unit’s 10G segments (A1/A1 or B1/B2) to the network and verify that the unit is passing traffic.

Optional step: Set email up notification

As part of the segment configuration process, you have can have the wiring table sent to you through e-mail. If you want to use this option, you must set up email notification *before* you proceed to segment configuration.

Set segment configuration and bypass tolerances

1. In the management interface, select the **Segment Configuration** page.
2. Use the configuration tool to describe the appliances and the ports you want to use. Select a configuration for Segment A, and then select a configuration for Segment B.

   Note: There are eight configurations options available to maximize your protected ports. The configuration you select for Segment A determines the options you have available for Segment B.
3. Click **Next**.
4. For each 10Gb segment, set the number of 1Gb segments that must fail before the 10Gb segment goes into bypass.
5. Click **Save**.

   The interface displays a diagram of the security controller that illustrates how to cable the security controller to the ports on the IPS appliances.

   Note: There is an option to send a wiring table in an e-mail message.

Cable the unit and appliances

Use the wiring diagram provided by the configuration tool or the wiring table you receive in e-mail to connect the security controller to the IPS appliances.

Chapter 3

Configuring Proventia Network Security Controller Through the Management Interface

Overview

Introduction

You can use either the management interface or the command line interface to set most configuration options for Proventia Network Security Controller. This chapter lists configuration options available through the user interface, and describes how to set them.

In this chapter

This chapter contains the following topics:

About the management interface

Overview

Proventia Network Security Controller provides a secured Web management interface. You can manage and monitor Proventia Network Security Controller from any Web browser.

Management pages

The management interface consists of a series of pages, as indicated in the following table:

Management Page	Description
Status	Status information about Proventia Network Security Controller
Management Port	IP settings for the management port
Email Notifications	Settings required for email notification, such as email accounts and mail server information
SNMP Settings	Settings for sending SNMP traps to an SNMP trap server
Users	User name and password combinations for accessing the management interface
Backup/Restore	Backup, restore, and reset to factory default functions
Firmware Update	Access to the latest update packages

Table 7: *Management interface pages*

Accessing the management interface

Overview

Proventia Network Security Controller provides a secured Web management interface. You can manage and monitor Proventia Network Security Controller from any Web browser.

Prerequisite

Make sure that the ethernet management port for Proventia Network Security Controller is connected to the local network or to the host computer.

Default management port IP address and URL

Proventia Network Security Controller has a default IP address assigned to the management port. The default IP address and URL are shown in the following table.

Item	Default value
Management port IP address	**192.168.0.111**
Management port URL	**https://192.168.0.111**

Table 8: *Default IP address and URL for the management port*

These default values remain in effect until you change them. If you need to change the IP address for the management port, you can do so using command line parameters or using the **Management Port** page of the management interface.

Important: Any changes to the management port may interrupt your ability to maintain a connection from the management interface. Make sure that the new IP address is accessible before you make any changes. Any change to the IP address changes the management port URL

URL for accessing the management interface

You can access the management interface using a URL that consists of **https://** followed by the management port's IP address. The URL format is as follows:

https://*xxx.xxx.xxx.xxx*

When you type the URL, replace *xxx.xxx.xxx.xxx* with the IP address assigned to the management port.

For example, the default URL is **https://192.168.0.111**.

Note: When you enter the URL, you see a message regarding the website's security certificate. Click "Continue to this website (not recommended)" to proceed.

Logging in

When you enter the management website, you see the log in screen. Complete the fields as indicated in the following table.

Field	Description
User	Type the user name Note: The default user is **admin**
Password	Type the password Note: The default password is **admin**

The default values remain in effect until you change them. If you need to change the user name or password, you can do so using the **Users** page of the management interface or the command line interface.

Monitoring Proventia Network Security Controller

Overview

This section includes information on how to monitor the status of Proventia Network Security Controller using the management interface.

Checking overall status

The **Status** page is the first page you see when you log in to the management interface. Use the **Status** page to view information for Proventia Network Security Controller. The information on the Status page is presented in sections, as indicated in the following table.

Section	Description
System	Provides general information about the controller
Power Supply Status	Indicates if power supplies are present or not present
Segment A	Shows the active/bypass status and bypass threshold for segment A
Segment B	Shows the active/bypass status and bypass threshold for segment B
Segments Settings	Shows current segment configuration

Table 9: *Sections on the Status page*

Viewing system status

The System section provides general system status, as indicated in the following table.

Field	Description
Product Name	Displays the name of the controller: “Proventia NSC”
Product ID	Displays the product ID of the controller
Manufacture Revision	Displays the hardware version of the controller
Firmware Version	Displays the current firmware version of the controller
Management IP	Displays the IP address for the management port **Tip:** Use the **Management Port** page if you want to change IP settings for the management port.
Email Notifications	Indicates whether email notifications are enabled or disabled Default: Disabled (Don’t send) **Tip:** Use the **Email Notification** page if you want to change email settings.

Table 10: *Status information*

Managing Proventia Network Security Controller

Overview

Use the management interface to view or change settings for Proventia Network Security Controller.

Setting segment configurations and bypass tolerances

1. In the management interface, select the **Segment Configuration** page.
2. Use the configuration tool to describe the appliances and the ports you want to use. Select a configuration for Segment A, and then select a configuration for Segment B.

   Note: There are eight configurations options available to maximize your protected ports. The configuration you select for Segment A determines the options you have available for Segment B.
3. Click **Next**.
4. For each 10Gb segment, set the number of 1Gb segments that must fail before the 10Gb segment goes into bypass.
5. Click **Save**.

   The interface displays a diagram of the security controller that illustrates how to cable the security controller to the ports on the IPS appliances.

   Note: There is an option to send a wiring table in an e-mail message.

Setting Management Port settings

Use the **Management Port** page to configure IP settings for the management port.

Field	Description
IP Address	IP address of the management port Default value: 192.168.0.111
Network Mask	IP address of the network or subnet mask Default value: 255.255.255.0
Gateway	IP address of the network gateway Default value: 192.168.0.1
DNS 1	IP address of the primary domain name system server Default: 192.168.0.1
DNS 2	IP address of the secondary domain name system server Default: 0.0.0.0

Table 11: *Management Port information*

Setting Email Notifications

Proventia Network Security Controller provides an e-mail notification function which can send an e-mail message when the switching mode of a segment changes. Use the **Email Notification** page to configure e-mail servers and accounts, and to enable or disable notifications.

Set the values as indicated in the following table.

Field	Description
Email Notification	Enable or disable e-mail notification Default: Disabled (don't send)
Outgoing Mail Server (SMTP)	Address of the appropriate outgoing SMTP mail server
Outgoing Mail Server (SMTP) Port	Port number of the outgoing SMTP mail server Default: 25
SMTP Username	Username for the outgoing SMTP mail server
SMTP Password	Password for the outgoing SMTP mail server (if applicable)
From (Sender's email address)	Name or address that should appear in the "From" field on an outgoing e-mail message
To (List of recipients, comma separated)	List of e-mail addresses to whom the notification should be sent.
Subject	Subject to appear in the subject line of the outgoing email message

Table 12: *Email settings*

Setting SNMP traps

Proventia Network Security Controller provides an SNMP trap function which can send messages to a trap server when the segment status or power supply status changes. Use the **SNMP Settings** page to configure the SNMP destination IP and SNMPv2 community name, and to enable or disable the SNMP trap function.

Complete the fields as indicated in the following table.

Field	Description
Send SNMP Traps	Enable or disable the sending of SNMP traps Default: Disabled
SNMP traps destination IP	Destination IP of the SNMP trap server Default: **`Local Host`**
SNMPv2 community	Community name of the SNMP trap server. Default: **`public`**

Table 13: *SNMP settings*

Reference: Appendix A, "MIB File Reference"

Managing User Account settings

Use the **Users** page to change the user name and password required to access the web management interface. The fields are described in the following table.

Field	Description
Admin User Name:	User name required to access the management interface from a web browser

Table 14: *User Account settings*

Field	Description
Password	Password required to access the management interface from a web browser

Table 14: *User Account settings*

Backing up or restoring settings

Use the **Backup/Restore** page to make a backup or to return Proventia Network Security Controller to its default settings. Complete the fields as indicated in the following table.

Field	Description
Backup	Saves a copy of current settings on Proventia NSC in a file called **`config.txt`**
Restore From	Location of a stored backup file. Type the file location or navigate to the file, and click **Restore From**.
Restore to Factory Default Configuration	Restores Proventia NSC to the default configuration and then restarts it **Note:** The IP address for the management interface will not be reset to the default value.

Table 15: *Configuration Backup/Restore settings*

Firmware Update

Use the **Firmware Update** page to update Proventia Network Security Controller with the latest firmware.

Updates are available from the IBM ISS Download Center at https://webapp.iss.net/myiss/login.jsp. Download the firmware to a computer that is accessible from the management interface on the controller. Then, browse to the file location, and click **Upload Firmware**.

Note: The firmware update may take up to 5 minutes to complete. Some firmware updates may require the controller to restart.

Check the **Status** page to verify that the new firmware version is reflected.

Chapter 4

Configuring Proventia Network Security Controller Using the Command Line Interface

Overview

Introduction

You can use either the management interface or the command line interface to set most configuration options for Proventia Network Security Controller. This chapter lists the command line parameters, and describes how to set configuration options through the command line interface.

In this chapter

This chapter contains the following topics:

Accessing the command line interface

Overview

This section contains information you need in order to access the command line interface.

Connection types

You can access the command line interface for Proventia Network Security Controller in one of two ways:

- through a serial terminal emulator
- through an SSH remote shell emulator

Connection requirements

The requirements for both connection types are shown in the following table.

Connection Type	Port on PNSC	Cable
Serial terminal emulator	Console port	Console cable
SSH remote shell emulator	Management port	Management cable

Table 16: *Connection requirements to access command line interface*

Serial terminal settings

Use a serial terminal emulator and the following terminal settings:

Setting	Value
Communications Port	Typically COM1 (depending on computer setup)
Emulation	VT100
Bits per second:	115,200
Data bits:	8
Parity:	None
Stop:	1
Flow Control:	None

Table 17: *Serial terminal settings to access command line interface*

SSH port

Proventia Network Security Controller SSH server uses standard port 22.

User name and password

Use the administrator account to configure parameters and to monitor the status of Proventia Network Security Controller. The default user name and password is listed in the following table.

Field	Description
User	Type the user name Note: The default user is **admin**
Password	Type the password Note: The default password is **admin**

Note: You can change the password through the command line interface or through the management interface.

Syntax for command line parameters

Overview

This section outlines the syntax required to set or retrieve values using the command line parameters.

Permissions required

Only the Admin account has permissions to set and retrieve system parameters.

Command line syntax

Use the following command line syntax to set or retrieve values for parameters.

Command	Action
`cli get |more`	Outputs values for all parameters
`cli get` *`parameter_name`*	Display a value for the parameter you specify **Example:** Typing **`cli get timeout0`** displays the time-out value of Segment A in decimal value
`cli set` *`parameter_name parameter_value`*	Sets a value for parameter you specify **Example:** Typing **`cli set timeout1 20`** sets the time-out value for Segment B to 20

Table 18: *Command line syntax*

Command line parameters

Overview

This section lists the command line parameters available for use with Proventia Network Security Controller. The parameters are divided into the following categories:

- Management port parameters
- Communication parameters
- Email notification parameters
- SNMP parameters
- Operational parameters

Use parameters with care

Use these command line parameters carefully, as they control the behavior of Proventia Network Security Controller. Do not change a default value unless you are sure of the effect the change will have on your network. Some parameters should not be changed unless you are instructed to do so by a representative from IBM ISS Customer Support.

Management port parameters

The parameters in the following table control the IP settings for the management port.

Parameter	Description
ip	Current IP address for the management port for Proventia Network Security Controller Default: 192.168.0.111
mask	Subnet mask for the management port Default: 255.255.255.0
gw	Gateway IP address for the management port Default: 192.168.0.1

Table 19: *Management port parameters*

Communication parameters

The parameters in the following table control the communication features of the unit.

Parameter	Description
dns	DNS server IP address **Note:** This parameter corresponds to DNS1 in the user interface.
dns2	Second DNS server IP address
domain	Domain name for local host Default: **`local`**
host	Hostname for the unit **Usage: `cli get mac`** This parameter is read only. Default: Proventia_NSC
username	Administrator account name Default: admin

Table 20: *Communication parameters*

Parameter	Description
password	Administrator password Default: admin
https	Enables or disables the HTTPS server • **0** - disables the secure WEB MGT interface • **1** - enables access to secure WEB MGT interface Default: 1 (enabled)

Table 20: *Communication parameters (Continued)*

Email notification parameters

The parameters in the following table control the email notification feature.

Parameter	Description
Email	Enables or disables the email notification feature • **0** - disables email notification • **1** - enables email notification Default: 1
email_from	Name or email address to appear in the “From” field on the email notification
email_security	Enables or disables the email security feature • **0** - disables email security feature • **1** - enables email security feature Default: 1
email_username	User name for the email account used to send email notifications from Proventia Network Security Controller
email_password	Password for the email account used to send email notifications from Proventia Network Security Controller
email_server	SMTP server address for email server
email_subject	Text to appear in the subject line of notification email messages Sample: “**`Notice: PNSC segment(s) have switched modes`**”
email_to	List of email addresses to which the notification should be sent

Table 21: *Email notification parameters*

SNMP parameters

The parameters in the following table control sending SNMP traps.

Parameter	Description
snmp	Enables or disables SNMP function • **0** - disables SNMP function • **1** - enables SNMP function. Default: 0 (disabled)

Table 22: *SNMP parameters*

Parameter	Description
snmp_community	Snmp_community name Default: **public**
snmp_destination	Snmp_destination Default: **localhost**

Table 22: *SNMP parameters (Continued)*

Operational parameters

The parameters in the following table control the behavior of the unit.

Parameter	Description
seg_trunk_cfg	Segment configuration for mapping 10Gb segments to 1Gb ports. 1 – Segment A connects to 4 segments IPS. Segment B is unused. 2 – Segment A connects to 4 segments IPS with all 4 segments used. Segment B connects to 4 segments IPS with all segments used. 3 – Segment A connects to 4 segments IPS with all 4 segments used. Segment B connects to 8 segments IPS with all segments used. 4 – Segment A connects to 8 segments IPS with segments 1, 2, 7 and 8 used. Segment B connects to 8 segments IPS with all segments used 5 – Segment A connects to 8 segments IPS with segments 1, 2, 3, 6, 7, and 8 used. Segment B connects to 8 segments IPS with segments 1,2,3,6,7 and 8 used. 6 –Segment A connects to 8 segments IPS with all 8 segments used. Segment B is unused. 7 – Segment A connects to 8 segments IPS with all 8 segments used. Segment B connects to 4 segments IPS with all segments used. 8 –Segment A connects to 8 segments IPS with all 8 segments used. Segment B connects to 8 segments IPS with segments 1, 2, 7, and 8 used. Default: 1
link_lose_cnt0, link_lose_cnt1	Sets the bypass tolerances for segments A and B. These parameters set the number of 1Gb segments that must be lost before the corresponding 10Gb segment goes into bypass. If the number of lost segments is greater than or equal to the value you set, the segment goes into bypass. A segment goes into bypass o You can set different values for Segment A and Segment B. Values: 1-8

Table 23: *Operational parameters*

Appendix A

MIB File Reference

Overview

Introduction

This appendix shows the information contained in the MIB file and outlines the process required to set up SNMP traps.

In this appendix

This appendix contains the following topics:

SNMP and the ISS.MIB file

Overview

Simple Network Management Protocol (SNMP) is a protocol for monitoring the status of networking equipment. You can configure SNMP notification responses to send events to an SNMP manager. The ISS.MIB file contains information that helps identify the source of the traps on the SNMP server.

How SNMP works

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

About the MIB file

To display the IBM ISS-assigned Event Name in SNMP trap messages, you can import or compile the IBM ISS MIB file (`iss.mib`) into an SNMP management application. The IBM ISS MIB file defines the format of SNMP traps for IBM ISS products, and is used by your management application to provide translations of the numeric Object Identifiers (OIDs) contained in the trap messages. You can download the iss.mib file from the IBM ISS Download Center at http://www.iss.net/download/.

MIB file location

The ISS.MIB file is available from the following locations:

- IBM ISS Download Center ("MyISS Log in" link at www.iss.net)
- the **/etc/** directory in the Proventia Network Security Controller file system

Copy the MIB file to your SNMP trap server.

Process overview: setting up SNMP traps

Overview

This section outlines a typical process for setting up an SNMP agent. The set up process for your SNMP management application may be different. Refer to the documentation for your SNMP management application for instructions specific to your software.

Typical process

1. Install the SNMP software package of your choice on a Linux platform.
2. Locate the file called **`snmptrapd.conf`** in **`/etc/snmp/`** directory on Proventia Network Security Controller.
3. Set the snmp trap daemon community parameter by adding the following line to the end of the file.

   ```
   authCommunity log public
   ```

   Note: The default community name is **`public`**. You can change this value using the Web management interface or the command line interface.
4. Locate the file called ISS.MIB on the IBM ISS Download Center or in the **`/etc`** directory on Proventia Network Security Controller.
5. Copy the ISS.MIB file to the Linux system you are using as the SNMP trap server.
6. Run the following command:

   ```
   snmptrapd -m <full_path_to_ISS.MIB_file> -Os -Le -f
   ```

Contents of ISS.MIB file

Overview

The ISS.MIB file identifies SNMP traps on your SNMP trap server.

File contents

```
-- ISS-MIB { iso org(3) dod(6) internet(1) private(4) enterprises(1) 2499
  }
-- Title:   Internet Security Systems Private Enterprise MIB
-- Version: 2.0

ISS-MIB DEFINITIONS ::= BEGIN

IMPORTS
    MODULE-IDENTITY,
    OBJECT-TYPE,
    NOTIFICATION-TYPE,
    Integer32,
    Gauge32,
    enterprises
       FROM SNMPv2-SMI
    DisplayString, TruthValue
       FROM SNMPv2-TC
    MODULE-COMPLIANCE, OBJECT-GROUP, NOTIFICATION-GROUP
       FROM SNMPv2-CONF;

iss       MODULE-IDENTITY
    LAST-UPDATED        "200812220000Z"-- 22 Dec 2008
    ORGANIZATION        "Internet Security Systems Inc"
    CONTACT-INFO        "ISS customer support:support@iss.net"
    DESCRIPTION        "This MIB module defines objects for use with ISS
  products."
    REVISION            "200812220000Z"-- 22 Dec 2008
    DESCRIPTION         "IBM ISS MIB"
    ::= { enterprises 2499 }


-- ************************************************************
-- High-level identifiers
-- ************************************************************

notifications                          OBJECT IDENTIFIER ::= { iss 0 }
products                               OBJECT IDENTIFIER ::= { iss 1 }
issMIBGroups                           OBJECT IDENTIFIER ::= { iss 2 }

realSecure                           OBJECT IDENTIFIER ::= { products 1 }
internetScanner                        OBJECT IDENTIFIER ::= { products
  2 }
systemSecurityScanner                  OBJECT IDENTIFIER ::= { products
  3 }
common                               OBJECT IDENTIFIER ::= { products 4 }

-- ************************************************************
-- mailSecurity branch
-- ************************************************************
mailSecurity                           OBJECT IDENTIFIER ::= { products
  5 }
```

```
bypassMgmt                          OBJECT IDENTIFIER ::= { products 6 }

logdata                              OBJECT IDENTIFIER ::= { common 1 }

v1-5                                OBJECT IDENTIFIER ::= { realSecure
  1 }
engine                                OBJECT IDENTIFIER ::= { v1-5 1 }
console                               OBJECT IDENTIFIER ::= { v1-5 2 }
daemon                                OBJECT IDENTIFIER ::= { v1-5 3 }
events                               OBJECT IDENTIFIER ::= { engine 1 }

v2-5                                OBJECT IDENTIFIER ::= { realSecure
  2 }
engine2-5                             OBJECT IDENTIFIER ::= { v2-5 1 }
events2-5                             OBJECT IDENTIFIER ::= { engine2-
  5 1 }


-- ************************************************************************
-- bypass  sub-branches
-- ************************************************************************
bypassTraps                         OBJECT IDENTIFIER ::= { bypassMgmt
  1 }
bypassTrapInfo                      OBJECT IDENTIFIER ::= { bypassMgmt
  2 }
bypassSystem                        OBJECT IDENTIFIER ::= { bypassMgmt
  3 }
bypassSystemScalars                   OBJECT IDENTIFIER ::= {
  bypassSystem 1 }
bypassSystemTables                    OBJECT IDENTIFIER ::= {
  bypassSystem 2 }

-- ************************************************************************
-- Groups
-- ************************************************************************
realSecureMIBGroups                   OBJECT IDENTIFIER ::= {
  issMIBGroups 1 }
internetScannerMIBGroups              OBJECT IDENTIFIER ::= {
  issMIBGroups 2 }
systemScannerMIBGRoups                OBJECT IDENTIFIER ::= {
  issMIBGroups 3 }
commonMIBGroups                       OBJECT IDENTIFIER ::= {
  issMIBGroups 4 }
notificationMIBGroups                 OBJECT IDENTIFIER ::= {
  issMIBGroups 5 }

-- ************************************************************************
-- mailSecurity sub-branches
-- ************************************************************************
msCommon                           OBJECT IDENTIFIER ::= { mailSecurity
  1 }
msPolicy                           OBJECT IDENTIFIER ::= { mailSecurity
  2 }
msSMTP                             OBJECT IDENTIFIER ::= { mailSecurity
  3 }
msFilterDB                            OBJECT IDENTIFIER ::= {
  mailSecurity 4 }
```

```
-- ************************************************************************
-- 1-5 EventData
-- ************************************************************************

eventTable OBJECT-TYPE
    SYNTAX SEQUENCE OF EventEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION ""
    ::= { events 1 }

eventEntry OBJECT-TYPE
    SYNTAX EventEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION ""
    INDEX { eventEntryName }
    ::= { eventTable 1 }

EventEntry ::= SEQUENCE
{
    eventEntryName DisplayString,
    eventEntryTime DisplayString,
    eventEntryAmask Integer32,
    eventEntryPriority INTEGER,
    eventEntryProtocol INTEGER,
    eventEntrySourceIpAddress DisplayString,
    eventEntryDestinationIpAddress DisplayString,
    eventEntrySourceName DisplayString,
    eventEntryDestinationName DisplayString,
    eventEntryIcmpType DisplayString,
    eventEntryIcmpCode DisplayString,
    eventEntrySourcePort Integer32,
    eventEntryDestinationPort Integer32,
    eventEntrySourcePortName DisplayString,
    eventEntryDestinationPortName DisplayString,
    eventEntryUserActionList DisplayString
}

eventEntryName OBJECT-TYPE
    SYNTAX DisplayString
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION "The name of the decode/event for this trap."
    ::= { eventEntry 1 }

eventEntryTime OBJECT-TYPE
    SYNTAX DisplayString
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION "The time the event was discovered relative to the
  RealSecure engine."
    ::= { eventEntry 2 }

eventEntryAmask OBJECT-TYPE
    SYNTAX Integer32
    MAX-ACCESS read-only
    STATUS current
```

```
    DESCRIPTION "A Mask to indicate what actions are configured for this
  event:
    ACT_IGN (Ignore)                                          = 0x00000000,
    ACT_KILL (Kill Session)                                   = 0x00000001,
    ACT_VIEW_SESS (Send Stream to Console for View Session) = 0x00000002,
    ACT_EMAIL (Send an e-mail message)                       = 0x00000004,
    ACT_LOG_RAW (Record stream data for viewing)              = 0x00000008,
    ACT_DISPLAY (Send event to console)                       = 0x00000040,
    ACT_LOG_DB (Record to database)                           = 0x00000200,
    ACT_FIREWALL (Send message to lock firewall)              = 0x00000400,
    ACT_SNMP_TRAP (Send SNMP Trap)                            = 0x00000800,
    ACT_USER_SPECIFIED1 (User Specified 1)                    = 0x00001000,
    ACT_USER_SPECIFIED2 (User Specified 2)                    = 0x00002000,
    ACT_USER_SPECIFIED3 (User Specified 3)                    = 0x00004000,
    ACT_USER_SPECIFIED4 (User Specified 4)                   = 0x00008000 "

    ::= { eventEntry 3 }

eventEntryPriority OBJECT-TYPE
    SYNTAX INTEGER { other(1), low(2), medium(3), high(4) }
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION "The priority of the decode as determined from the
  current engine policy."
    ::= { eventEntry 4 }

eventEntryProtocol OBJECT-TYPE
    SYNTAX INTEGER { other(1), tcp(2), udp(3), icmp(4)  }
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION "Protocol type for this event."
    ::= { eventEntry 5 }

eventEntrySourceIpAddress OBJECT-TYPE
    SYNTAX DisplayString
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION "Source Ip Address"
    ::= { eventEntry 6 }

eventEntryDestinationIpAddress OBJECT-TYPE
    SYNTAX DisplayString
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION "Destination Ip Address"
    ::= { eventEntry 7 }

eventEntrySourceName OBJECT-TYPE
    SYNTAX DisplayString
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION "Source Ip Address (engine no longer does dns lookup)"
    ::= { eventEntry 8 }

eventEntryDestinationName OBJECT-TYPE
    SYNTAX DisplayString
    MAX-ACCESS read-only
    STATUS current
```

```
    DESCRIPTION "Destination Ip Address (engine no longer does dns
  lookup)"
    ::= { eventEntry 9 }

eventEntryIcmpType OBJECT-TYPE
    SYNTAX DisplayString
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION "ICMP Type"
    ::= { eventEntry 10 }

eventEntryIcmpCode OBJECT-TYPE
    SYNTAX DisplayString
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION "ICMP Code"
    ::= { eventEntry 11 }

eventEntrySourcePort OBJECT-TYPE
    SYNTAX Integer32
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION "Source Port"
    ::= { eventEntry 12 }

eventEntryDestinationPort OBJECT-TYPE
    SYNTAX Integer32
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION "Destination Port"
    ::= { eventEntry 13 }

eventEntrySourcePortName OBJECT-TYPE
    SYNTAX DisplayString
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION "The name of the network service usually associated with
  the source port."
    ::= { eventEntry 14 }

eventEntryDestinationPortName OBJECT-TYPE
    SYNTAX DisplayString
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION "The name of the network service usually associated with
  the dest port."
    ::= { eventEntry 15 }

eventEntryUserActionList OBJECT-TYPE
    SYNTAX DisplayString
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION "This field is obsolete.
                 This same information can be found in the AMask field."
    ::= { eventEntry 16 }


-- ****************************************************************
```

```
-- Log Data
-- ********************************************************************

logTable OBJECT-TYPE
    SYNTAX SEQUENCE OF LogEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION ""
    ::= { logdata 1 }

logEntry OBJECT-TYPE
    SYNTAX LogEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION ""
    INDEX { logEntryTime }
    ::= { logTable 1 }

LogEntry ::= SEQUENCE
{
    logEntryTime TimeTicks,
    logEntrySource DisplayString,
    logEntryCategory DisplayString,
    logEntryEventId Integer32,
    logEntryDescription DisplayString,
    logEntryData OCTET STRING
}


logEntryTime OBJECT-TYPE
    SYNTAX TimeTicks
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION "The TimeTicks when the log entry was written."
    ::= { logEntry 1 }

logEntrySource OBJECT-TYPE
    SYNTAX DisplayString
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION "The Application that sent the message"
    ::= { logEntry 2 }

logEntryCategory OBJECT-TYPE
    SYNTAX DisplayString
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION ""
    ::= { logEntry 3 }

logEntryEventId OBJECT-TYPE
    SYNTAX Integer32
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION ""
    ::= { logEntry 4 }

logEntryDescription OBJECT-TYPE
```

```
        SYNTAX DisplayString
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION ""
        ::= { logEntry 5 }

    logEntryData OBJECT-TYPE
        SYNTAX OCTET STRING
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION ""
        ::= { logEntry 6 }

    -- ************************************************************************
    -- 2-5 EventData
    -- ************************************************************************

    event25Table OBJECT-TYPE
        SYNTAX SEQUENCE OF Event25Entry
        MAX-ACCESS not-accessible
        STATUS current
        DESCRIPTION ""
        ::= { events2-5 1 }

    event25Entry OBJECT-TYPE
        SYNTAX Event25Entry
        MAX-ACCESS not-accessible
        STATUS current
        DESCRIPTION ""
        INDEX { eventEntryName25 }
        ::= { event25Table 1 }

    Event25Entry ::= SEQUENCE
    {
        eventEntryName25 DisplayString,
        eventEntryTime25 DisplayString,
        eventEntryProtocol25 DisplayString,
        eventEntrySourceIpAddress25 DisplayString,
        eventEntryDestinationIpAddress25 DisplayString,
        eventEntryIcmpType25 DisplayString,
        eventEntryIcmpCode25 DisplayString,
        eventEntrySourcePort25 DisplayString,
        eventEntryDestinationPort25 DisplayString,
        eventEntryUserActionList25 DisplayString,
        eventEntryEventSpecificInfo25 DisplayString
    }

    eventEntryName25 OBJECT-TYPE
        SYNTAX DisplayString
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION "The name of the decode/event for this trap."
        ::= { event25Entry 1 }

    eventEntryTime25 OBJECT-TYPE
        SYNTAX DisplayString
        MAX-ACCESS read-only
        STATUS current
```

```
        DESCRIPTION "The time the event was discovered relative to the
      RealSecure engine."
        ::= { event25Entry 2 }

    eventEntryProtocol25 OBJECT-TYPE
        SYNTAX DisplayString
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION "Protocol type for this event."
        ::= { event25Entry 3 }

    eventEntrySourceIpAddress25 OBJECT-TYPE
        SYNTAX DisplayString
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION "Source Ip Address"
        ::= { event25Entry 4 }

    eventEntryDestinationIpAddress25 OBJECT-TYPE
        SYNTAX DisplayString
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION "Destination Ip Address"
        ::= { event25Entry 5 }

    eventEntryIcmpType25 OBJECT-TYPE
        SYNTAX DisplayString
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION "ICMP Type"
        ::= { event25Entry 6 }

    eventEntryIcmpCode25 OBJECT-TYPE
        SYNTAX DisplayString
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION "ICMP Code"
        ::= { event25Entry 7 }

    eventEntrySourcePort25 OBJECT-TYPE
        SYNTAX DisplayString
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION "Source Port"
        ::= { event25Entry 8 }

    eventEntryDestinationPort25 OBJECT-TYPE
        SYNTAX DisplayString
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION "Destination Port"
        ::= { event25Entry 9 }

    eventEntryUserActionList25 OBJECT-TYPE
        SYNTAX DisplayString
        MAX-ACCESS read-only
        STATUS current
       DESCRIPTION "A string which indicates what actions are configured for
```

```
    this event.
      Currently available actions:
      KILL (Kill Session - ends a tcp-based session)
      VIEW_SESS (Send Stream to Console for View Session)
      EMAIL (Send an e-mail message to a configured email account)
      LOG_RAW (Record stream data for later analysis or viewing)
      DISPLAY (Send event to console)
      LOG_DB (Record the event to database)
      FIREWALL (Send message to lock firewall)
      SNMP_TRAP (Send SNMP Trap to configured SNMP manager)
      USER_SPECIFIED1 (User Specified 1 - launch a program as configured
    per engine setup)
      USER_SPECIFIED2 (User Specified 2)
      USER_SPECIFIED3 (User Specified 3)
      USER_SPECIFIED4 (User Specified 4)"
      ::= { event25Entry 10 }

  eventEntryEventSpecificInfo25 OBJECT-TYPE
      SYNTAX DisplayString
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION "This variable contains a listing of other
    variables:values
                   which are specific to the given event."
      ::= { event25Entry 11 }



  -- ****************************************************************
  -- NOTIFICATIONS
  -- ****************************************************************

  eventinfo NOTIFICATION-TYPE
      OBJECTS
      {
          eventEntryName,
          eventEntryTime,
          eventEntryAmask,
          eventEntryPriority,
          eventEntryProtocol,
          eventEntrySourceIpAddress,
          eventEntryDestinationIpAddress,
          eventEntrySourceName,
          eventEntryDestinationName,
          eventEntryIcmpType,
          eventEntryIcmpCode,
          eventEntrySourcePort,
          eventEntryDestinationPort,
          eventEntrySourcePortName,
          eventEntryDestinationPortName,
          eventEntryUserActionList
      }
      STATUS current
      DESCRIPTION
      "This trap is sent from a RealSecure engine whenever a event
       is encountered that the RealSecure engine is configured to send
    traps
       for.  The details of the event are contained in the trap."
```

```
    ::= { notifications 1 }

-- ****************************************************************

logdatatrap NOTIFICATION-TYPE
    OBJECTS
    {
        logEntryTime,
        logEntrySource,
        logEntryCategory,
        logEntryEventId,
        logEntryDescription,
        logEntryData
    }
    STATUS current
    DESCRIPTION
    "This trap is sent for certain types of log data.
     Only configured types of log data which will be sent as a trap."
    ::= { notifications 2 }

-- ****************************************************************

highpriorityevent NOTIFICATION-TYPE
    OBJECTS
    {
        eventEntryName25,
        eventEntryTime25,
        eventEntryProtocol25,
        eventEntrySourceIpAddress25,
        eventEntryDestinationIpAddress25,
        eventEntryIcmpType25,
        eventEntryIcmpCode25,
        eventEntrySourcePort25,
        eventEntryDestinationPort25,
        eventEntryUserActionList25,
        eventEntryEventSpecificInfo25
    }
    STATUS current
    DESCRIPTION
    "This trap is sent from a RealSecure engine whenever a high priority
  event
     is encountered that the RealSecure engine is configured to send
  traps
     for.  The details of the event are contained in the trap."
    ::= { notifications 3 }

-- ****************************************************************

mediumpriorityevent NOTIFICATION-TYPE
    OBJECTS
    {
        eventEntryName25,
        eventEntryTime25,
        eventEntryProtocol25,
        eventEntrySourceIpAddress25,
        eventEntryDestinationIpAddress25,
        eventEntryIcmpType25,
        eventEntryIcmpCode25,
```

```
        eventEntrySourcePort25,
        eventEntryDestinationPort25,
        eventEntryUserActionList25,
        eventEntryEventSpecificInfo25
}
    STATUS current
    DESCRIPTION
    "This trap is sent from a RealSecure engine whenever a medium
  priority event
     is encountered that the RealSecure engine is configured to send
  traps
     for.  The details of the event are contained in the trap."
    ::= { notifications 4 }

-- ****************************************************************

lowpriorityevent NOTIFICATION-TYPE
    OBJECTS
    {
        eventEntryName25,
        eventEntryTime25,
        eventEntryProtocol25,
        eventEntrySourceIpAddress25,
        eventEntryDestinationIpAddress25,
        eventEntryIcmpType25,
        eventEntryIcmpCode25,
        eventEntrySourcePort25,
        eventEntryDestinationPort25,
        eventEntryUserActionList25,
        eventEntryEventSpecificInfo25
    }
    STATUS current
    DESCRIPTION
    "This trap is sent from a RealSecure engine whenever a low priority
  event
     is encountered that the RealSecure engine is configured to send
  traps
     for.  The details of the event are contained in the trap."
    ::= { notifications 5 }


-- ****************************************************************
-- RealSecure Groups
-- ****************************************************************

v15EventObjectsGroup OBJECT-GROUP
    OBJECTS
    {
        eventEntryName,
        eventEntryTime,
        eventEntryAmask,
        eventEntryPriority,
        eventEntryProtocol,
        eventEntrySourceIpAddress,
        eventEntryDestinationIpAddress,
        eventEntrySourceName,
        eventEntryDestinationName,
        eventEntryIcmpType,
```

```
            eventEntryIcmpCode,
            eventEntrySourcePort,
            eventEntryDestinationPort,
            eventEntrySourcePortName,
            eventEntryDestinationPortName,
            eventEntryUserActionList
        }
        STATUS current
        DESCRIPTION "A collection of objects used for RealSecure v1.5 traps"
        ::= { realSecureMIBGroups 1 }

    v25EventObjectsGroup OBJECT-GROUP
        OBJECTS
        {
            eventEntryName25,
            eventEntryTime25,
            eventEntryProtocol25,
            eventEntrySourceIpAddress25,
            eventEntryDestinationIpAddress25,
            eventEntryIcmpType25,
            eventEntryIcmpCode25,
            eventEntrySourcePort25,
            eventEntryDestinationPort25,
            eventEntryUserActionList25,
            eventEntryEventSpecificInfo25
        }
        STATUS current
        DESCRIPTION "A collection of objects defining RealSecure v2.5 events"
        ::= { realSecureMIBGroups 2 }

    -- ********************************************************************
    -- Mail Security Common
    -- ********************************************************************
    msCommonVersion  OBJECT-TYPE
           SYNTAX     DisplayString
           MAX-ACCESS read-only
           STATUS     current
           DESCRIPTION
                  "Software version"
           ::= { msCommon 1 }

    -- ********************************************************************
    -- Mail Security Policy System
    -- ********************************************************************
    msPolicyMailsProcessedOBJECT-TYPE
           SYNTAX       Unsigned32
           MAX-ACCESSread-only
           STATUS       current
           DESCRIPTION
                  "Number of mails processed by the mail security policy
      system"
           ::= { msPolicy 1 }

    msPolicyMailsBlockedOBJECT-TYPE
           SYNTAX       Unsigned32
           MAX-ACCESSread-only
           STATUS       current
           DESCRIPTION
```

```
                "Number of mails blocked by the mail security policy system"
        ::= { msPolicy 2 }

msPolicyMailsAllowedOBJECT-TYPE
        SYNTAX       Unsigned32
        MAX-ACCESSread-only
        STATUS       current
        DESCRIPTION
                "Number of mails allowed by the mail security policy system"
        ::= { msPolicy 3 }

msPolicyMailsWithActionOBJECT-TYPE
        SYNTAX       Unsigned32
        MAX-ACCESSread-only
        STATUS       current
        DESCRIPTION
                "Number of mails the mail security policy system performed
  an action on"
        ::= { msPolicy 4 }

msPolicyMailsQuarantinedOBJECT-TYPE
        SYNTAX       Unsigned32
        MAX-ACCESSread-only
        STATUS       current
        DESCRIPTION
                "Number of mails the mail security stored in the qurantine
  stores"
        ::= { msPolicy 5 }

msPolicyMailsReleasedOBJECT-TYPE
        SYNTAX       Unsigned32
        MAX-ACCESSread-only
        STATUS       current
        DESCRIPTION
                "Number of mails the mail security released from the
  qurantine stores"
        ::= { msPolicy 6 }

msPolicyAnalysesCountOBJECT-TYPE
        SYNTAX       Unsigned32
        MAX-ACCESSread-only
        STATUS       current
        DESCRIPTION
                "Number of mails analyzed by the mail security system"
        ::= { msPolicy 7 }

msPolicyAnalysesErrorsOBJECT-TYPE
        SYNTAX       Unsigned32
        MAX-ACCESSread-only
        STATUS       current
        DESCRIPTION
                "Number of mails that could not be analyzed by the mail
  security system"
        ::= { msPolicy 7 }



-- ****************************************************************
```

```
-- Mail Security Filter Database
-- ***********************************************************************
fdbVersion  OBJECT-TYPE
       SYNTAX     DisplayString
       MAX-ACCESS read-only
       STATUS     current
       DESCRIPTION
              "Current filter database version"
       ::= { msFilterDB 1 }

fdbLastUpdateTime  OBJECT-TYPE
       SYNTAX     DateAndTime
       MAX-ACCESS read-only
       STATUS     current
       DESCRIPTION
              "The time of the most recent filter database update"
       ::= { msFilterDB 2 }

-- ***********************************************************************
-- Mail Security SMTP Server
-- ***********************************************************************
smtpUncheckedQueueSizeOBJECT-TYPE
       SYNTAX       Unsigned32
       MAX-ACCESSread-only
       STATUS       current
       DESCRIPTION
              "Number of mails received by SMTP server but not yet
  analyzed"
       ::= { msSMTP 1 }

smtpMailsSentOBJECT-TYPE
       SYNTAX       Unsigned32
       MAX-ACCESSread-only
       STATUS       current
       DESCRIPTION
              "Number of mails sent by the SMTP server"
       ::= { msSMTP 2 }

smtpSendQueueSizeOBJECT-TYPE
       SYNTAX       Unsigned32
       MAX-ACCESSread-only
       STATUS       current
       DESCRIPTION
              "Number of mails in the SMTP server's send queue"
       ::= { msSMTP 3 }

smtpResendQueueSizeOBJECT-TYPE
       SYNTAX       Unsigned32
       MAX-ACCESSread-only
       STATUS       current
       DESCRIPTION
              "Number of mails in the SMTP server's resend queue"
       ::= { msSMTP 4 }

-- --------------------
-- bypass traps
-- --------------------
```

```
bypassInOut NOTIFICATION-TYPE
    OBJECTS
    {
        bypassTrapModuleId,
        bypassTrapModuleName,
        bypassTrapStateBypass
    }
    STATUS      current
    DESCRIPTION
            "Trap issued when a module goes in and out of bypass."
    ::= { bypassTraps 1 }

bypassDiagnostics NOTIFICATION-TYPE
    OBJECTS
    {
        bypassTrapDiagnostics
    }
    STATUS      current
    DESCRIPTION
            "Trap issued when an internal hw diagnostics event occurs."
    ::= { bypassTraps 2 }

-- --------------------
-- bypass trap info: varbinds sent with traps
-- --------------------

bypassTrapModuleId OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
            "This is the ID (starting from 0) of the
             module going in/out of the bypass."
    ::= { bypassTrapInfo 1 }

bypassTrapModuleName OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
            "This is the name of the
             module going in/out of the bypass."
    ::= { bypassTrapInfo 2 }

bypassTrapStateBypass OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
            "This is the state (true for bypass, false for active)
            of the module going in/out of the bypass."
    ::= { bypassTrapInfo 3 }

bypassTrapDiagnostics OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
```

```
            "This is the description of a diagnostics event."
    ::= { bypassTrapInfo 4 }

-- ************************************************************************
-- Common Groups
-- ************************************************************************

logDataObjectsGroup OBJECT-GROUP
    OBJECTS {
        logEntryTime,
        logEntrySource,
        logEntryCategory,
        logEntryEventId,
        logEntryDescription,
        logEntryData
    }
    STATUS current
    DESCRIPTION "A collection of objects defining log events"
    ::= { commonMIBGroups 1 }


-- ************************************************************************
-- Notification Groups
-- ************************************************************************

logNotificationsGroup NOTIFICATION-GROUP
    NOTIFICATIONS { logdatatrap }
    STATUS current
    DESCRIPTION "Collection of log notifications"
    ::= { notificationMIBGroups 1 }

v15NotificationsGroup NOTIFICATION-GROUP
    NOTIFICATIONS { eventinfo }
    STATUS current
    DESCRIPTION "Collection of RealSecure v1.5 event notifications"
    ::= { notificationMIBGroups 2 }

v25NotificationsGroup NOTIFICATION-GROUP
    NOTIFICATIONS {
        highpriorityevent,
        mediumpriorityevent,
        lowpriorityevent
    }
    STATUS current
    DESCRIPTION "Collection of RealSecure v2.5 event notifications"
    ::= { notificationMIBGroups 3 }

END
```

Appendix B

Safety, Environmental, and Electronic Emissions Notices

Overview

Introduction

This section contains important information related to safe use and environmental responsibility.

In this appendix

This appendix contains the following topics:

DANGER and CAUTION notices

Introduction

This topic lists the **DANGER** and **CAUTION** notices that apply to your product. Language translations are available on the CD provided with your Proventia Network Security Controller.

Safety notices may be printed throughout this guide. **DANGER** notices warn you of conditions or procedures that can result in death or severe personal injury. **CAUTION** notices warn you of conditions or procedures that can cause personal injury that is neither lethal nor extremely hazardous. **Attention** notices warn you of conditions or procedures that can cause damage to machines, equipment, or programs.

DANGER Notices

The following **DANGER** notices apply to this product:

DANGER

To prevent a possible shock from touching two surfaces with different protective ground (earth), use one hand, when possible, to connect or disconnect signal cables. (D001)

DANGER

Overloading a branch circuit is potentially a fire hazard and a shock hazard under certain conditions. To avoid these hazards, ensure that your system electrical requirements do not exceed branch circuit protection requirements. Refer to the information that is provided with your device or the power rating label for electrical specifications. (D002)

DANGER

If the receptacle has a metal shell, do not touch the shell until you have completed the voltage and grounding checks. Improper wiring or grounding could place dangerous voltage on the metal shell. If any of the conditions are not as described, STOP. Ensure the improper voltage or impedance conditions are corrected before proceeding. (D003)

DANGER

An electrical outlet that is not correctly wired could place hazardous voltage on the metal parts of the system or the devices that attach to the system. It is the responsibility of the customer to ensure that the outlet is correctly wired and grounded to prevent an electrical shock. (D004)

DANGER

When working on or around the system, observe the following precautions:

Electrical voltage and current from power, telephone, and communication cables are hazardous. To avoid a shock hazard:

- Connect power to this unit only with the IBM ISS provided power cord. Do not use the IBM ISS provided power cord for any other product.
- Do not open or service any power supply assembly.
- Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.
- The product might be equipped with multiple power cords. To remove all hazardous voltages, disconnect all power cords.
- Connect all power cords to a properly wired and grounded electrical outlet. Ensure that the outlet supplies proper voltage and phase rotation according to the system rating plate.
- Connect any equipment that will be attached to this product to properly wired outlets.
- When possible, use one hand only to connect or disconnect signal cables.
- Never turn on any equipment when there is evidence of fire, water, or structural damage.
- Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.
- Connect and disconnect cables as described in the following procedures when installing, moving, or opening covers on this product or attached devices.

To disconnect:

1. Turn off everything (unless instructed otherwise).
2. Remove the power cords from the outlets.
3. Remove the signal cables from the connectors.
4. Remove all cables from the devices.

To connect:

1. Turn off everything (unless instructed otherwise).
2. Attach all cables to the devices.
3. Attach the signal cables to the connectors.
4. Attach the power cords to the outlets.
5. Turn on the devices.

(D005)

CAUTION Notices

The following **CAUTION** notices apply to this product:

CAUTION

Data processing environments can contain equipment transmitting on system links with laser modules that operate at great than Class 1 power levels. For this reason, never look into the end of an optical fiber cable or open receptacle. (C027)

CAUTION

For 19″ rack mount products:

- Do not install a unit in a rack where the internal rack ambient temperatures will exceed the manufacturer's recommended ambient temperature for all your rack-mounted devices.
- Do not install a unit in a rack where the air flow is compromised. Ensure that air flow is not blocked or reduced on any side, front, or back of a unit used for air flow through the unit.
- Consideration should be given to the connection of the equipment to the supply circuit so that overloading the circuits does not compromise the supply wiring or overcurrent protection. To provide the correct power connection to a rack, refer to the rating labels located on the equipment in the rack to determine the total power requirement of the supply circuit.
- *(For sliding drawers)* Do not pull or install any drawer or feature if the rack stabilizer brackets are not attached to the rack. Do not pull out more than one drawer at a time. The rack might become unstable if you pull out more than one drawer at a time.
- *(For fixed drawers)* This drawer is a fixed drawer and must not be moved for servicing unless specified by the manufacturer. Attempting to move the drawer partially or completely out of the rack might cause the rack to become unstable or cause the drawer to fall out of the rack.

(R001 Part 2 of 2)

CAUTION

This part or unit is heavy but has a weight smaller than 18 kg (39.7 lb). Use care when lifting, removing, or installing this part or unit. (C008)

World trade safety information

Several countries require the safety information contained in product publications to be presented in their national languages. If this requirement applies to your country, a safety information booklet is included in the publications package shipped with the product. The booklet contains the safety information in your national language with references to the US English source. Before using a US English publication to install, operate, or service this IBM ISS product, you must first become familiar with the related safety information in the booklet. You should also refer to the booklet any time you do not clearly understand any safety information in the US English publications.

Laser safety information

Introduction

The laser safety notices in this topic apply to this product.

C026

CAUTION

This product may contain one or more of the following devices: CD-ROM drive, DVD-ROM drive, DVD-RAM drive, or laser module, which are Class 1 laser products. Note the following information:

- Do not remove the covers. Removing the covers of the laser product could result in exposure to hazardous laser radiation. There are no serviceable parts inside the device.
- Use of the controls or adjustments or performance of procedures other than those specified herein might result in hazardous radiation exposure. (C026)

C026

CAUTION

Data processing environments can contain equipment transmitting on system links with laser modules that operate at greater than Class 1 power levels. For this reason, never look into the end of an optical fiber cable or open receptacle. (C027)

Laser compliance

All lasers are certified in the U.S. to conform to the requirements of DHHS 21 CFR Subchapter J for class 1 laser products. Outside the U.S., they are certified to be in compliance with IEC 60825 as a class 1 laser product. Consult the label on each part for laser certification numbers and approval information.

Environmental notices

Product recycling and disposal

This unit must be recycled or discarded according to applicable local and national regulations. IBM encourages owners of information technology (IT) equipment to responsibly recycle their equipment when it is no longer needed. IBM offers a variety of product return programs and services in several countries to assist equipment owners in recycling their IT products. Information on IBM ISS product recycling offerings can be found on IBM's Internet site at http://www.ibm.com/ibm/environment/products/prp.shtml.

Esta unidad debe reciclarse o desecharse de acuerdo con lo establecido en la normativa nacional o local aplicable. IBM recomienda a los propietarios de equipos de tecnología de la información (TI) que reciclen responsablemente sus equipos cuando éstos ya no les sean útiles. IBM dispone de una serie de programas y servicios de devolución de productos en varios países, a fin de ayudar a los propietarios de equipos a reciclar sus productos de TI. Se puede encontrar información sobre las ofertas de reciclado de productos de IBM en el sitio web de IBM http://www.ibm.com/ibm/environment/products/prp.shtml.

Notice: This mark applies only to countries within the European Union (EU) and Norway.

Appliances are labeled in accordance with European Directive 2002/96/EC concerning waste electrical and electronic equipment (WEEE). The Directive determines the framework for the return and recycling of used appliances as applicable through the European Union. This label is applied to various products to indicate that the product is not to be thrown away, but rather reclaimed upon end of life per this Directive.

In accordance with the European WEEE Directive, electrical and electronic equipment (EEE) is to be collected separately and to be reused, recycled, or recovered at end of life. Users of EEE with the WEEE marking per Annex IV of the WEEE Directive, as shown above, must not dispose of end of life EEE as unsorted municipal waste, but use the collection framework available to customers for the return, recycling, and recovery of WEEE. Customer participation is important to minimize any potential effects of EEE on the environment and human health due to the potential presence of hazardous substances in EEE. For proper collection and treatment, contact your local IBM representative.

注意: このマークは EU 諸国およびノルウェーにおいてのみ適用されます。

この機器には、EU 諸国に対する廃電気電子機器指令 2002/96/EC(WEEE) のラベルが貼られています。この指令は、EU 諸国に適用する使用済み機器の回収とリサイクルの骨子を定めています。このラベルは、使用済みになった時に指令に従って適正な処理をする必要があることを知らせるために種々の製品に貼られています。

Remarque: Cette marque s'applique uniquement aux pays de l'Union Européenne et à la Norvège.

L'etiquette du système respecte la Directive européenne 2002/96/EC en matière de Déchets des Equipements Electriques et Electroniques (DEEE), qui détermine les dispositions de retour et de recyclage applicables aux systèmes utilisés à travers l'Union européenne. Conformément à la directive, ladite étiquette précise que le produit sur lequel elle est apposée ne doit pas être jeté mais être récupéré en fin de vie.

Product information (B)

For Turkey:

This notice is effective as of May 30, 2009: Pursuant to Turkey's Directive on the Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment (EEE Directive), IBM, commencing as of May 30, 2009, provides Turkey's Ministry of Environment and Forestry with an annual Compliance Declaration Form, certifying to such entity that the applicable IBM product(s), as and when introduced by IBM into Turkey, conforms to the EEE Directive. (B1)

Ürün bilgileri (B)

Türkiye için:

Bu bildirim 30 Mayis 2009 tarihi itibariyle geçerlidir: Türkiye'nin Elektrikli ve Elektronik Esyalarda Bazi Zararli Maddelerin Kullaniminin Sinirlandirilmasina Dair Yönetmelik (EEE Yönetmeligi) uyarinca, IBM, 30 Mayis 2009'dan baslayarak, Türkiye Çevre ve Orman Bakanligi'na her yil, IBM tarafindan Türkiye'ye sunuldugunda ve sunulduktan sonra geçerli IBM ürününün (ürünlerinin) EEC Yönetmeligi'ne uygun oldugunu onaylayan bir Uygunluk Beyan Formu saglayacaktir. (B1)

Product handling information

Introduction

One of the safety notices in this topic may apply to this product. Please refer to the specific product specifications to determine the weight of the product to see which applies.

C008

CAUTION

This part or unit is heavy but has a weight smaller than 18 kg (39.7 lb). Use care when lifting, removing, or installing this part or unit. (C008)

C009

CAUTION

The weight of this part or unit is between 18 and 32 kg (39.7 and 70.5 lb). It takes two persons to safely lift this part or unit. (C009)

Product safety labels

Introduction

One or more of the safety labels in this topic may apply to this product.

L001

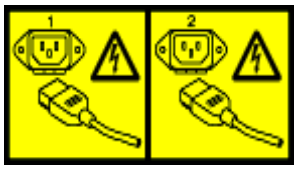
DANGER

Hazardous voltage, current, or energy levels are present inside any component that has this label attached. Do not open any cover or barrier that contains this label.

L003

DANGER

Multiple power cords. The product might be equipped with multiple power cords. To remove all hazardous voltages, disconnect all power cords. (L003)



Electromagnetic compatibility notices

Electronic emissions notices

The following statements apply to this IBM product. The statement for other IBM products intended for use with this product will appear in their accompanying manuals.

Federal Communications Commission (FCC) Statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. this equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions contained in the installation manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Note: Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors, by installation or use of this equipment other than as specified in the installation manual, or by any other unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

Note: This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Canadian Department of Communications Compliance Statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformité aux normes du ministère des Communications du Canada

Cet appareil numérique de las classe A est conform à la norme NMB-003 du Canada.

European Union (EU) Electromagnetic Compatibility Directive

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM ISS cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM ISS option cards.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to European Standard EN 55022. The limits for Class equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

Warning:

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

European Community contact:

IBM Technical Regulations
Pascalstr. 100, Stuttgart, Germany 70569
Telephone: 0049 (0) 711 785 1176
Fax: 0049 (0) 711 785 1283
e-mail: tjahn@de.ibm.com

EC Declaration of Conformity (In German)

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.
Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der IBM gesteckt/eingebaut werden.
EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden: "Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen."

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten Dieses Produkt entspricht dem "Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)". Dies ist die Umsetzung der EU-Richtlinie 2004/108/EG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) für Geräte der Klasse A
Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.
Verantwortlich für die Konformitätserklärung des EMVG ist die IBM Deutschland GmbH, 70548 Stuttgart.

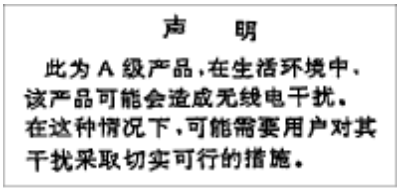
Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

update: 2007/05/25

People's Republic of China Class A Compliance Statement:

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may need to perform practical actions.



Japan Class A Compliance Statement:

This product is a Class A Information Technology Equipment and conforms to the standards set by the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に
基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を
引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求
されることがあります。

Korean Class A Compliance Statement:

이 기기는 업무용으로 전자파적합등록을 한 기기이오니 판매자
또는 사용자는 이점을 주의하시기 바라며, 만약 잘못 판매 또는
구입하였을 때에는 가정용으로 교환하시기 바랍니다.

Index

t

u

w