IBM Security

IBM Security SiteProtector System SP3001 Hardware Configuration Guide

Version 2.9

Publication Date: November 2011

Contents

About this publication

This publication describes the information you need to configure the IBM Security SiteProtector System SP3001 appliance hardware.

Audience

This guide is intended for network or security administrators or any other individuals who are responsible for configuring the SiteProtector SP3001 appliance and managing network security. This guide assumes that you have a working knowledge of network devices and Microsoft administration tasks.

Scope

This guide provides procedures for configuring the SiteProtector SP3001 appliance hardware and Windows administration options. This guide is designed to be a companion to the SiteProtector documentation suite. After you have configured the SiteProtector SP3001 appliance hardware, use the *IBM Security SiteProtector System Configuration Guide* to configure the SiteProtector security management software.

Technical Support

IBM® Security provides technical support to customers who are entitled to receive support.

The IBM Support Portal

Before you contact IBM Security Solutions about a problem, see the IBM Support Portal at http://www.ibm.com/software/support.

The IBM Software Support Guide

If you need to contact technical support, use the methods described in the IBM Software Support Guide at http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html.

The guide provides the following information:

- Registration and eligibility requirements for receiving support
- Customer support telephone numbers for the country in which you are located
- Information you must gather before you call

Chapter 1. Introduction to the SiteProtector SP3001 Appliance

This chapter introduces the SiteProtector SP3001 appliance and describes the components and functions of SiteProtector.

Topics

How to Use the SP3001 appliance documentation

Use this guide along with other SiteProtector documentation to find the information you need.

We explain how the information in the *IBM Security SiteProtector System SP3001 Hardware Configuration Guide* is organized and list other documents in the SiteProtector documentation suite that you may use to configure SiteProtector. We also provide links to SiteProtector documentation and IBM Security licensing information.

Document organization

This document is organized into logical units, as described in the following table:

Chapter	Description
Chapter 2, "Before You Begin," on page 7	Contains background information, prerequisites, and procedures for configuring the IBM Security SiteProtector SP3001 appliance hardware.
Chapter 3, "Connecting and configuring the SiteProtector SP3001 appliance," on page 11	Contains procedures for configuring the SiteProtector SP3001 appliance hardware and for accessing the SiteProtector software on the SiteProtector SP3001 appliance from the SiteProtector Console. To support less experienced users, this chapter provides significantly more background information than the SiteProtector *IBM Security SiteProtector System SP3001 Quick Start Guide*.
Chapter 4, "Configuring the SiteProtector Console," on page 17	Contains procedures for configuring the SiteProtector SP3001 appliance administration options using the SiteProtector Console. If you configured the SiteProtector SP3001 appliance hardware using the SiteProtector *IBM Security SiteProtector System SP3001 Quick Start Guide*, start here to continue the configuration process.
Chapter 5, "Optional configuration tasks," on page 21	Contains procedures for optional hardware and server administration tasks.

The following table describes other documents in the SiteProtector documentation suite:

Document	Content
IBM Security SiteProtector System SP3001 Quick Start Guide	Contains the minimal information required to configure SiteProtector SP3001 appliance hardware and to connect it to the Console. If you are an experienced hardware administrator and do not need significant background information about the tasks that you perform, consider using this Quick Start Guide to configure the SiteProtector SP3001 appliance hardware.
IBM Security SiteProtector System Configuration Guide	Contains information about configuring, updating, and maintaining the SiteProtector security management software.
IBM Security SiteProtector System Policies and Responses Configuration Guide	Contains information about configuring policies and responses, including Central Responses.
IBM Security SiteProtector System Information Center (Help)	Contains all the procedures that you need to use SiteProtector, including some procedures that may not be available in PDF-based user documents.

Latest product documentation

For the latest product documentation including SiteProtector-related documents in portable document format (PDF), go to the IBM Security Product Information Center at http:// publib.boulder.ibm.com/ infocenter/sprotect/v2r8m0/index.jsp. SiteProtector PDFs may also be available on the Deployment Manager, if installed at your Site.

License agreement

For licensing information on IBM Security products, download the IBM Licensing Agreement from http://www-935.ibm.com/services/us/iss/html/contracts_landing.html.

What is the SiteProtector SP3001 appliance?

The SiteProtector SP3001 appliance is a hardware implementation of SiteProtector that includes preinstalled instances of the required SiteProtector components on a single, rack-mountable appliance.

Included components

SiteProtector SP3001 appliance components and agents include the following:

- Components that provide the basic functionality necessary to accept, monitor, and analyze network events, such as the Agent Manager or Event Collector. See “SiteProtector components” on page 3 for a description of each component.
- Components that provide additional security and management functions, such as the SiteProtector Reporting component or the SecurityFusion module.
- IBM Security Server Protection for Windows (formerly Proventia Server for Windows), which provides host security protection for the SiteProtector SP3001 appliance.

SiteProtector components by type

The following table provides a list of the required and optional SiteProtector components and agents that SiteProtector manages:

Installed SiteProtector Components	Optional SiteProtector Components
Agent Manager	Deployment Manager
Console (user must install separately)	Event Viewer
SiteProtector Database	X-Press Update Servers
Event Collector	
SiteProtector Reporting	
SP Core (See “SiteProtector components” for details)	
IBM Security Server Protection for Windows	
SiteProtector SecurityFusion module	
Event Archiver	

Included licenses

The SiteProtector SP3001 appliance includes licenses for the SiteProtector Reporting component, IBM Security Server Protection for Windows, and the SecurityFusion module.

SiteProtector components

The SiteProtector SP3001 appliance consists of required and optional SiteProtector components that provide the base functionality necessary to accept, monitor, and analyze network events. Depending on your Site requirements, you may need to install more than one of some components.

Component descriptions

The following table describes the SiteProtector components:

SiteProtector Component	Description
Console	Use the SiteProtector Console to perform most SiteProtector functions, such as monitoring events, scheduling scans, generating reports, and configuring agents. You can also use the SiteProtector Console to configure the SiteProtector SP3001 appliance's administration options.
Event Collector	The Event Collector manages real-time events from agents and vulnerability data from scanners.
Site Database	The SiteProtector database stores raw agent data, occurrence metrics (statistics for security events triggered by agents), group information, command and control data, and the status of X-Press Updates (XPUs).

SiteProtector Component	Description
SP Core	The SP core includes the following components: • The Application Server, which includes the Sensor Controller component, enables communication between the SiteProtector Console and the SiteProtector database. • The X-Press Update Server stores X-Press Updates (XPUs) downloaded from the IBM Security Download center and makes them available to the agents and components on the network. The Update Server eliminates the need to download updates for similar products more than once and allows users to manage the update process more efficiently. • SiteProtector Web Access is a interface that provides easy access to SiteProtector for running reports and monitoring assets and security events.
SiteProtector Firmware	SiteProtector firmware consists of the operating system and the database that runs on the SiteProtector SP3001 appliance hardware.
Agent Manager	The Agent Manager manages the command and control activities of the Desktop Protection agents, IBM Security Server Protection, and Proventia Network MFS, and X-Press Update Server; and it also facilitates data transfer from agents to the Event Collector.
SecurityFusion module	The SiteProtector SecurityFusion module greatly increases your ability to quickly identify and respond to critical threats at your Site. Using advanced correlation and analysis techniques, the Module identifies both high impact events and patterns of events that may indicate attacks. *Impact analysis* — The module correlates intrusion detection events with vulnerability assessment and operating system data and immediately estimates the impact of events.
Standalone X-Press Update Servers (optional)	In addition to the X-Press Update (XPU) Server that is installed with the SP Core, you can install standalone X-Press Update Servers on separate computers.
Event Archiver	Store event data and improve performance by reducing the number of events the database must store. **Note:** See the *SiteProtector Configuration Guide* for information about configuring the Event Archiver.
Deployment Manager (optional)	The Deployment Manager is a Web server that lets you install any of the SiteProtector components and agents on computers on your network.
Event Viewer (optional)	The SiteProtector Event Viewer receives unprocessed events from the Event Collector to provide near real time access to security data for troubleshooting.

System requirements

See the "Hardware and software requirements" topic under *Planning* in the Information Center (online Help) for information regarding system requirements.

Note: The “Hardware and software requirements” topic applies only to add-on components because the SiteProtector SP3001 appliance hardware meets all SiteProtector requirements.

IBM Security Server Protection for Windows

An embedded version of the IBM Security Server Protection for Windows is installed and configured on the SiteProtector SP3001 appliance hardware and is delivered with a security policy that is predefined for the SiteProtector SP3001 appliance's operating system and configuration.

Purpose of IBM Security Server Protection

IBM Security Server Protection for Windows, formerly Proventia Server for Windows, is a comprehensive security application that protects the SiteProtector SP3001 appliance and your network from the following:

- theft of corporate information, passwords, and other sensitive information
- attempts to use the SiteProtector SP3001 appliance to attack other systems

IBM Security Server Protection features

The following table describes the IBM Security Server Protection features that are enabled on the SiteProtector SP3001 appliance:

Feature	Description
Intrusion prevention	IBM Security Server Protection includes an intrusion prevention system that alerts you to attacks and blocks threats to the SiteProtector SP3001 appliance and to your network. IBM Security Server Protection captures information about an intruder and logs suspicious activity, which preserves evidence of the attack.
Firewall	IBM Security Server Protection: • provides powerful firewall capabilities that inspect all inbound and outbound traffic on the computer for unauthorized activity • can control network communication based on port, IP address, and protocol • blocks unauthorized activity without affecting normal traffic
Buffer overflow exploit prevention	IBM Security Server Protection can prevent exploits based on buffer overflows. Some intruders attempt to send more data to the buffer than it can handle. This can enable intruders to effectively take control of the computer.

Chapter 2. Before You Begin

This chapter provides requirements, considerations, and pre-configuration checklists. Review this information before you install the SiteProtector SP3001 appliance hardware in a rack or connect the SiteProtector SP3001 appliance to a network.

Topics

Requirements and considerations

Certain requirements and considerations apply to the configuration process in this guide. Review these requirements and considerations before you begin to configure the SiteProtector SP3001 appliance.

Where to configure the SiteProtector SP3001 appliance

You must configure some basic SiteProtector SP3001 appliance settings -- IP address, subnet mask, default gateway, DNS server, and host name -- using the appliance's LCD panel. After the SiteProtector SP3001 is initially configured, management of the appliance is performed primarily through a Remote Desktop session using standard operating system tools.

Important consideration for rack-mounted appliances

Record the Product Key of the SiteProtector SP3001 appliance's operating system before you install it. This Product Key can be found on the Certificate of Authenticity (COA) that is affixed to the appliance or in the accessory box. You will need the operating system Product Key if you need to restore the appliance to its factory defaults.

Additionally, record the appliance's SQL Server license Product Key and Tracking IDs, also found on the COA. You will need the SQL Server license Product Key and Tracking IDs in the event of an RMA return.

The COA may become inaccessible if you install the SiteProtector SP3001 appliance in a rack.

Important: If you need to restore the SiteProtector SP3001 appliance to its factory defaults, you must know the Product Key. See "Restoring factory defaults" on page 25.

Unsupported configurations

IBM Security does not support customized configurations. To avoid putting the SiteProtector SP3001 appliance in an unsupported state, do not do the following:

- install, reinstall, or remove applications from the SiteProtector SP3001 appliance
- add the SiteProtector SP3001 appliance to a network domain in which domain group policies require Windows Automatic updates
- apply hardened Windows security policies that could make the SiteProtector SP3001 appliance unusable

To return the SiteProtector SP3001 appliance to a supported state, you must restore the SiteProtector SP3001 appliance to its factory image or default settings, which erases all data, including events, from the database.

Reference: See “Restoring factory defaults” on page 25.

Automatic restarts

To ensure that important configuration changes are saved, the SiteProtector SP3001 appliance automatically restarts. This only occurs if you change the following settings:

- IP address
- Host name
- Server language

Updating the SiteProtector SP3001 appliance

Ensure that the SiteProtector SP3001 appliance has the latest firmware and intrusion prevention updates installed. The SiteProtector SP3001 appliance retrieves updates from the IBM Security Download Center, which is accessible over the Internet. For more information about product issues and updates, see the IBM Security Download Center at http://www.iss.net/download/.

IBM Security Server Protection for Windows

IBM Security Server Protection for Windows, formerly IBM Proventia Server Intrusion Prevention System (IPS), is designed to provide optimum protection in typical environments. IBM Security Server Protection is configured to block suspicious activity and certain types of communication. See the *IBM Security Server Protection for Windows User Guide* for more information.

To ensure that you can troubleshoot and monitor the SiteProtector SP3001 appliance remotely using widely accepted protocols, the following types of traffic are allowed on the SiteProtector SP3001 appliance:

- ICMP traffic
- Remote desktop
- SNMP

Important: Do not change the IBM Security Server Protection policy settings unless absolutely necessary.

Pre-configuration checklists

Review the checklists in this topic to ensure that you have the items you need before you proceed with the configuration process.

This topic includes the following checklists:

- Information required
- Cables required

Information required checklist

To establish network connectivity, you must enter specific information about your network. Use the checklist in the following table to collect this information:

✓	**Setting**	**Description**
	Management Port IP Address	An IP address for the management network adapter. **Example:** 192.168.1.100
☐	**Your setting:**	

✓	Setting	Description
☐	Management port subnet mask	The subnet mask value for the network connected to the management port. **Example:** 255.255.255.0
☐	**Your setting:**	
☐	Management port default gateway	The IP address for the management gateway. **Example:**192.168.1.1
☐	**Your setting:**	
☐	Host name	The computer name for the SiteProtector SP3001 appliance. **Example:** SP3001
☐	**Your setting:**	
☐	DNS server name	The IP address of the domain name server that the SiteProtector SP3001 appliance will use. **Example:** 192.168.1.1
☐	**Your setting:**	

Cables required checklist

You must use certain cables to connect the SiteProtector SP3001 appliance to the network and to a power source. These cables are included with the SiteProtector SP3001 appliance:

✓	Item
☐	Ethernet cable
☐	Two (2) Power cords (included with the SiteProtector SP3001 appliance hardware)

Chapter 3. Connecting and configuring the SiteProtector SP3001 appliance

The first step is to connect the SiteProtector SP3001 appliance hardware to the network so that you can begin managing the SiteProtector SP3001 appliance. This chapter provides procedures for configuring the SiteProtector SP3001 appliance to communicate with the network and for starting the SiteProtector Console.

Attention: IBM Security does not support customized configurations on the appliance. Therefore, do not install, reinstall, or remove applications on the appliance.

Adding your IBM Security SiteProtector appliance into a domain can cause unintended consequences depending on domain group policies.

Example:

- Hardened security policies can render the appliance unusable.
- Group policies forcing Windows Automatic Updates can place the appliance in an unsupported state.

To return the appliance to a supported state, you must restore the appliance to its factory image or default settings, which erases all data, including events, from the database. For more information, see "Restoring factory defaults" on page 25.

Note: In prior SiteProtector appliance models (SP1001 and SP2001), management of the appliance was handled using the Console to configure various appliance settings. Beginning with the SP3001 model, many of the SiteProtector SP3001 appliance settings are managed with standard operating system tools that you can access using a Remote Desktop session on the appliance.

Note: You can use the *IBM Security SiteProtector System SP3001 Quick Start Guide* instead of the procedures in this chapter if you are an experienced network administrator, and you anticipate that your configuration will be straightforward. The *IBM Security SiteProtector System SP3001 Quick Start Guide* provides minimal guidance.

Topics

SiteProtector SP3001 appliance configuration checklist

The process of configuring the SiteProtector SP3001 appliance hardware requires that you perform tasks in a certain order. Follow the steps in this topic when you configure the SiteProtector SP3001 appliance.

Prerequisites

Before you configure your SiteProtector SP3001 appliance, you must have completed the following tasks:

- Ensure that you meet the requirements for configuring the SiteProtector SP3001 appliance.
  See "Requirements and considerations" on page 7.
- Gather the initial configuration items, including cables and network information.
  See "Pre-configuration checklists" on page 8.

Checklist

Use the checklist in the following table as a guide to help you perform the tasks in this chapter. The check boxes are provided as a convenience to help you check off the tasks as you complete them:

✓	Task	Description
☐	1	Connect the cables and start the SiteProtector SP3001 appliance. See Chapter 3, "Connecting and configuring the SiteProtector SP3001 appliance," on page 11.
☐	2	Specify network information, such as IP addresses, gateways, and subnet masks. See "Configuring the SiteProtector SP3001 appliance to communicate with the network" on page 14.
☐	3	Download, install, and point the SiteProtector Console to the SiteProtector SP3001 appliance. See "Installing and starting the SiteProtector Console" on page 15.

The SiteProtector SP3001 appliance front panel

The SiteProtector SP3001 appliance front panel consists of multiple features.

SiteProtector SP3001 appliance front panel

The following figure shows the SiteProtector SP3001 appliance front panel:

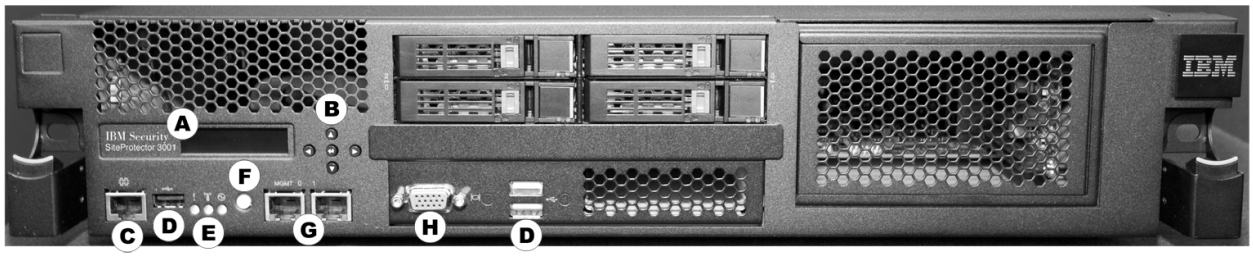


Figure 1. SP3001 appliance front panel

Front panel features

The following list describes the front panel features.

- **A: LCD panel -** use for initial network configuration, restarting or shutting down the appliance, viewing the serial number of the appliance, and setting the appliance PIN.
- **B: Arrow and enter keys -** use to select menu choices and interact with the appliance using the LCD panel.
- **C: Serial console RJ-45 port -** use for optional terminal-based setup, diagnostic testing, and recovery.
- **D: USB ports (3) -** for keyboard, mouse, and external DVD-ROM to retrieve data and install firmware.

- **E: Indicators -** to display status for alerts (amber), system ID (blue), and power (green) respectively.
- **F: Power switch -** to power the unit on or off.
- **G: Management interfaces (2 GbE NICs) -** use Management port 0 to manage the SiteProtector appliance; management port 1 is unused. The Management port handles all network communication.
- **H: VGA video port -** for external monitor.

  Note: Use the VGA port when you perform a procedure that requires a monitor to be attached, such as restoring the SiteProtector SP3001 appliance to a supported state as covered in "Restoring factory defaults" on page 25.

The SiteProtector SP3001 appliance back panel

The SiteProtector SP3001 appliance back panel includes cooling fans, fan status indicators, power connections, and power supplies.

SiteProtector SP3001 appliance back panel

The following figure shows the SiteProtector SP3001 appliance back panel:

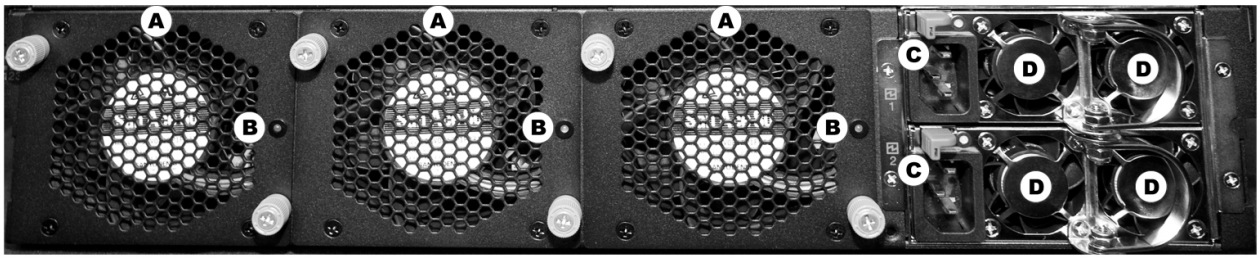


Figure 2. SP3001 appliance back panel

Back panel features

The following list describes the back panel features.

- **A: Cooling fans (3)**
- **B: Cooling fan status indicators (3)**
- **C: Power connections (2)**
- **D: Power supplies (4)**

Connecting the SiteProtector SP3001 appliance

Follow these instructions to connect the SiteProtector SP3001 appliance.

Procedure

1. Connect the power cords to the SiteProtector SP3001 appliance and to the power source.

   Important: You must connect both power cords to the SiteProtector SP3001 appliance to prevent warning signals from sounding.
2. Connect the Ethernet cable from the network to management port 0.
3. Turn on the SiteProtector SP3001 appliance. "IBM Security SiteProtector SP3001" appears on the LCD panel.

   Note: It may take several minutes for this message to appear.

Configuring the SiteProtector SP3001 appliance to communicate with the network

You must configure the SiteProtector SP3001 appliance before it can communicate with the network.

When you connect the SiteProtector SP3001 appliance to the network for the first time, you must enter some or all of the following information in the SiteProtector SP3001 appliance's LCD panel:

- IP Address
- subnet mask
- gateway address
- DNS Server
- host name

CAUTION:
Do not change the SiteProtector SP3001 appliance's host name or the IP address after the appliance has established communication with an external device. Doing so prevents the SiteProtector SP3001 appliance from communicating with the SiteProtector Console and any other external device. To re-establish this communication, you may be required to manually reconfigure the public and private keys that are exchanged between these devices, which can be a time-consuming and error prone process.

SP3001 LCD panel

The following table describes the buttons on the LCD panel:

Use this button...	To do this...
	Move left between digits. Referred to as the LEFT button.
	Move right between digits. Referred to as the RIGHT button.
	Move down or specify digits. Referred to as the DOWN button.
	Move up or specify digits. Referred to as the UP button.
	Enter information, or confirm a selection and move to a new screen. Referred to as the ENTER button.

Entering Network Information

Procedure

1. Locate the LCD panel on the front of the SiteProtector SP3001 appliance, and make sure that “IBM Security SiteProtector SP3001” appears on the screen.
2. Press the **ENTER** button. The Appliance PIN screen appears.

   Note: If you want to require that users enter a personal identification number (PIN) to use the LCD panel, see “Securing the SiteProtector SP3001 appliance hardware” on page 22.
3. Press the **DOWN** button.
4. When the message appears asking you to confirm that you want to change your configuration, select **OK**, and then press **ENTER**. A default IP address appears.

5. Is the default IP address correct?
   - If *yes*, return to the configuration menu, and then go to Step 7.
   - If no, enter the IP address of the SiteProtector SP3001 appliance in the field provided.

   Note: Press **UP** or **DOWN** to select a number, and then use the **LEFT** or **RIGHT** buttons to move to another digit.
6. Select **OK**, and then press the **ENTER** button to confirm.
7. Repeat Steps 4 through 6 to enter the following information:
   - subnet mask
   - default gateway
   - DNS server
   - host name

     Note: Certain characters cannot be used in the host name. See the Microsoft article at http://support.microsoft.com/kb/909264 for details on naming conventions.

   Note: The SiteProtector SP3001 appliance provides a default subnet mask and gateway address that is based on the IP address that you enter. You can skip the procedure for entering these addresses if you verify that the default gateway and subnet addresses are correct. See "SiteProtector SP3001 appliance configuration checklist" on page 11.
   A final confirmation screen appears.

   Note: If you want the SiteProtector SP3001 appliance to ignore the information that you have entered, select **Cancel**, and then press **ENTER**.
8. Select **OK**, and then press **ENTER** to confirm. The SiteProtector SP3001 appliance saves the configuration information you entered.

   Note: The SiteProtector SP3001 appliance restarts automatically if you change the IP address or the host name of the appliance.

What to do next

You have now connected the SiteProtector SP3001 appliance to the network using the LCD panel, so you are ready to download the SiteProtector Console and point it to the appliance. From the SiteProtector Console, you can install licenses. Then you will need to change administrator and database passwords.

Installing and starting the SiteProtector Console

To connect to SiteProtector for the first time, you must download, install, and start the SiteProtector Console on your computer.

Installing the SiteProtector Console

Procedure

1. From the local workstation, point a Web browser to the management address for the IBM Security SiteProtector System SP3001 appliance: `https://`*`appliance_IP_address`*`>:3994` (for example: `https://192.168.11.11:3994`).
2. Click **Yes** to accept the security certificate.
3. Read the IBM Security License Agreement, and then click **Accept**.

Note: The IBM Security License Agreement appears only when you access this Web site for the first time.
The system then displays the IBM Security SiteProtector System SP3001 home page with the following three links:

- SiteProtector Web Access
- Install SiteProtector Console
- IBM Security

4. Click the **Install SiteProtector Console** link.
5. Select **Run** to download the SiteProtector Console to your computer.
6. Select **Run** when asked to run this software to your computer.
7. Follow the steps in the SiteProtector Console - InstallShield Wizard to install the Console on your computer.

Starting the SiteProtector Console and logging on

Procedure

1. On your computer, open the SiteProtector Console.
2. Right-click the My Sites node in the left pane.
3. Select **New** > **Site**.
4. Log in using the SiteProtector SP3001 appliance's IP address.
5. Do the following:

In this Field...	Type the following...
User Name	Administrator
Password	ISSADMIN

Note: Change this password as soon as possible. See “Securing SP3001 appliance passwords” on page 18.

6. Click **OK**.

Chapter 4. Configuring the SiteProtector Console

After you connect and configure the SiteProtector SP3001 appliance hardware, you must perform additional configuration tasks in the SiteProtector Console. This chapter provides procedures for using the Console to perform these tasks.

Important: If you used the procedures in the *IBM Security SiteProtector System SP3001 Quick Start Guide* to connect the SiteProtector SP3001 appliance, start here to continue the configuration process.

Topics

SiteProtector Console configuration checklist

This topic provides a checklist that lists the tasks you should perform to configure the Console. Follow the steps in this topic when you configure the SiteProtector SP3001 appliance.

Note: This checklist provides the recommended order that the tasks in this chapter should be performed. This order may not always be required.

Checklist

Use the checklist in the following table as a guide to help you perform the tasks in this chapter. As you perform tasks, use the check boxes to check off the tasks that you have completed:

✓	Task	Description
☐	1	Install the license files for the reporting, correlation, and security features. See "Installing license files."
☐	2	Change the database and administrator passwords. See "Securing SP3001 appliance passwords" on page 18.
☐	3	Configure the date and time on the SiteProtector SP3001 appliance. See "Setting the date and time" on page 19.
☐	4	See the *IBM Security SiteProtector System Configuration Guide* to configure the SiteProtector security management software.

Installing license files

Now that you have logged on from the SiteProtector Console, you must install the new license files so that you can begin using the reporting, correlation, and security features that are installed on the SiteProtector SP3001 appliance. The SiteProtector SP3001 appliance requires properly configured licenses to run at full capability.

Before you begin

Install the SecurityFusion module before you install the license file. See the *SiteProtector SecurityFusion Module Guide* for detailed information.

Procedure

1. In the SiteProtector Console, select **Tools** > **Licenses** > **Agent/Module**.
2. Click the **Licenses** tab.
3. Click **Add**.
4. Locate and select the SiteProtector SP3001 appliance license file that you downloaded. This single license provides entitlements for all the SiteProtector SP3001 appliance components and modules.
5. Click **OK**.

Securing SP3001 appliance passwords

Now that you have logged on to the SiteProtector Console and installed the license files, you must secure your SiteProtector SP3001 appliance by changing your database and Windows administrator passwords.

Tip: The database administrator password is also known as the SA password.

Administrator passwords

The SiteProtector SP3001 appliance requires two administrator accounts that are configured with default user names and passwords. To avoid introducing a significant security vulnerability, you must change these passwords as soon as possible.

The following table lists the default user names and passwords:

Account type	Default user name	Default password
Database administrator	sa	ISSADMIN
Windows administrator	Administrator	ISSADMIN

Important: For the best security practices, IBM Security recommends that you use strong passwords and change these passwords frequently. See the Microsoft Windows Server documentation regarding the criteria required for creating strong passwords.

Setting the Database Administrator password

Procedure

1. Start the SiteProtector Console and log in.
2. Select the **System** view.
3. In the left pane, expand the site node for the SiteProtector SP3001 appliance site, and then click the **Appliance** icon.
4. Select the "Click here to connect to appliance" hyperlink. Clicking the hyperlink establishes a Remote Desktop session with the SiteProtector SP3001 appliance.
5. Log in to the Remote Desktop session on the appliance.
6. Run the SQL Server Management Studio.
7. Change the Database Administrator password.
8. Click **OK**.
9. When you are finished, close the Remote Desktop session.

Setting the Windows Administrator Password

Procedure

1. Start the SiteProtector Console and log in.
2. Select the **System** view.
3. In the left pane, expand the site node for the SiteProtector SP3001 appliance site, and then click the **Appliance** icon.
4. Select the "Click here to connect to appliance" hyperlink. Clicking the hyperlink establishes a Remote Desktop session with the SiteProtector SP3001 appliance.
5. Log in to the Remote Desktop session on the appliance.
6. Run the User Accounts tool from the Control Panel or run the Local Users and Groups snap-in by selecting **Start** > **Run** and entering `lusrmgr.msc`.
7. Change the Windows Administrator password.
8. Click **OK**.
9. When you are finished, close the Remote Desktop session.

Setting the date and time

The SiteProtector SP3001 appliance uses Windows time synchronization to update its date and time settings by default. However, you should verify that these settings are correct and change these settings if necessary.

Procedure

1. Select the **System** view.
2. Select the **Appliance** entry from the left pane.
3. Select the "Click here to connect to appliance" hyperlink. Clicking the hyperlink establishes a Remote Desktop session with the SiteProtector SP3001 appliance.
4. Log in to the Remote Desktop session on the appliance.
5. Open **Date and Time** from the Control Panel or select **Start** > **Run** and enter `timedate.cpl`.
6. Specify the correct **Date** and **Time**, and then select the correct **Time Zone**.
7. Click **OK**.

Chapter 5. Optional configuration tasks

This chapter provides procedures for configuring optional hardware and Windows administration options on the SiteProtector SP3001 appliance.

Topics

Starting and shutting down the SiteProtector SP3001

To ensure that the SiteProtector SP3001 appliance is properly maintained, you may need to restart or stop the SiteProtector SP3001 appliance hardware.

About this task

The topic provides procedures for manually restarting and shutting down the SiteProtector SP3001 appliance and scheduling these tasks so that they can occur automatically.

Important: If you completely shut down the SiteProtector SP3001 appliance hardware, you must physically access the SiteProtector SP3001 appliance to turn it on again. You cannot use the SiteProtector Console to turn on the SiteProtector SP3001 appliance.

Procedure

1. Start the SiteProtector Console and log in.
2. Select the **System** view.
3. In the left pane, expand the site node for the SiteProtector SP3001 appliance site, and then click the **Appliance** icon.
4. Select the "Click here to connect to appliance" hyperlink. Clicking the hyperlink establishes a Remote Desktop session with the SiteProtector SP3001 appliance.
5. Log in to the Remote Desktop session on the appliance.
6. Click **Start** and then do one of the following:

Click this option...	To do the following...
Shutdown > Restart	Shut down, and then restart the SiteProtector SP3001 appliance
Shutdown	Shut down, and then turn off the SiteProtector SP3001 appliance

Scheduling a server shut down or restart

Procedure

1. Start the SiteProtector Console and log in.
2. Select the **System** view.
3. In the left pane, expand the site node for the SiteProtector SP3001 appliance site, and then click the **Appliance** icon.

4. Select the "Click here to connect to appliance" hyperlink. Clicking the hyperlink establishes a Remote Desktop session with the SiteProtector SP3001 appliance.
5. Log in to the Remote Desktop session on the appliance.
6. Run the Task Scheduler by selecting **Start** > **All Programs** > **Administrative Tools** > **Task Scheduler** or by selecting **Start** > **Run** and entering `taskschd.msc`.
7. Use the Task Scheduler to schedule the Schedule the SiteProtector SP3001 appliance either to restart or to shut down and turn off.
8. Click **OK**.

Configuring SNMP services

SNMP is a network management protocol frequently used in TCP/IP networks to monitor and manage computers and other devices (such as printers) connected to the network.

About this task

By default, the Simple Network Management Protocol (SNMP) service is disabled on the SiteProtector SP3001 appliance but allowed by the IBM Security Server Protection policy. If your SiteProtector SP3001 appliance must be monitored by SNMP, you can enable SNMP services by following the instructions here.

Procedure

1. Start the SiteProtector Console and log in.
2. Select the **System** view.
3. In the left pane, expand the site node for the SiteProtector SP3001 appliance site, and then click the **Appliance** icon.
4. Select the "Click here to connect to appliance" hyperlink. Clicking the hyperlink establishes a Remote Desktop session with the SiteProtector SP3001 appliance.
5. Log in to the Remote Desktop session on the appliance.
6. Run the Services snap-in by selecting **Start** > **Run** and entering `services.msc`.
7. Use the SNMP Trap service to enable or disable SNMP services as needed.
8. Click **OK**.
9. When you are finished, close the Remote Desktop session.

Securing the SiteProtector SP3001 appliance hardware

You can secure the SiteProtector SP3001 appliance LCD settings by requiring that users specify a PIN to access the LCD panel.

About this task

If you specify a PIN for the SiteProtector SP3001 appliance LCD, users won't be able to access the LCD settings without first entering the PIN.

Procedure

1. On the LCD panel, press the ENTER button. The Appliance PIN screen appears.
2. On the Appliance PIN screen, press ENTER, and then specify a 4-digit number in the field.
3. Press ENTER.

Configuring other appliance settings

You manage the SP3001 appliance through a Remote Desktop session using standard operating system tools. Some of these settings may be covered in other topics.

About this task

A hyperlink available on the SiteProtector Console initiates a Remote Desktop session on the SP3001 appliance desktop.

Procedure

1. Start the SiteProtector Console and log in.
2. Select the **System** view.
3. Select the **Appliance** entry from the left pane.
4. Select the "Click here to connect to appliance" hyperlink. Clicking the hyperlink establishes a Remote Desktop session with the SiteProtector SP3001 appliance.
5. Log in to the Remote Desktop session on the appliance.
6. Use standard operating system tools to perform any of the following tasks:

Task	Operating System Tool
Change the Windows Administrator (default user name = Administrator) password	User Accounts tool from the Control Panel or run the Local Users and Groups snap-in by running `lusrmgr.msc`
Change the Database Administrator (default user name = sa) password	SQL Server Management Studio
Enable or disable SNMP[a] services as needed. SNMP is a network management protocol frequently used in TCP/IP networks to monitor and manage computers and other devices (such as printers) connected to the network.	Run the Services snap-in by running `services.msc` and then access the SNMP Trap service
Configure local users including creating new users, setting passwords, deleting existing users, and changing user properties	Run the Local Users and Groups snap-in by running `lusrmgr.msc`
Configure local groups including creating new groups, deleting existing groups, and changing group properties	Run the Local Users and Groups snap-in by running `lusrmgr.msc`
Configure folders including creating, removing, opening, editing properties for, and otherwise managing folders	Windows Explorer
Configure shares for existing or new folders including creating new shares, deleting existing shares, and changing share properties	Use the Administrative Tools > Share and Storage Management snap-in by running `StorageMgmt.msc` or the simpler Shared Folders management snap-in by running `fsmgmt.msc`. Note that the Shared Folders management tool is not present under Administrative Tools, but it is present on the operating system.
Configure file sharing protocols including enabling, disabling, and defining both general and security properties for file sharing	Run the Services snap-in by running `services.msc` and then access the Server service
Set the server date and time	Open Date and Time from the Control Panel or run `timedate.cpl`
Schedule a server shutdown or restart	Use the Task Scheduler by running Administrative Tools > Task Scheduler or run `Taskschd.msc`
Shut down and restart the server	Click **Start** > **Shutdown** > **Restart**

[a]By default, the Simple Network Management Protocol (SNMP) service is disabled on the SiteProtector SP3001 appliance but allowed by the IBM Security Server Protection policy. If your SiteProtector SP3001 appliance must be monitored by SNMP, you can enable SNMP services as needed.

7. Close the Remote Desktop session.

Chapter 6. Troubleshooting

This chapter contains information that can help you troubleshoot the SiteProtector SP3001 appliance hardware and Windows administration options.

Topics

Restoring factory defaults

Before you begin

Do the following before you perform this procedure:

- Make sure you have written down the Product Key from the Microsoft Certificate of Authenticity (COA) sticker that is affixed to the bottom of the SiteProtector SP3001 appliance.
- Attach a monitor and keyboard to the SiteProtector SP3001 appliance. See "The SiteProtector SP3001 appliance front panel" on page 12 for information about locating the VGA video (monitor) and USB (keyboard) ports.

About this task

If your SiteProtector SP3001 appliance has failed and cannot be recovered, you should return the SiteProtector SP3001 appliance to its factory defaults.

Important: When you restore the SiteProtector SP3001 appliance, you erase all the user data that is stored in the database, including events, policies, responses, and tickets. After you restore the SiteProtector SP3001 appliance, you must completely reconfigure the SiteProtector SP3001 appliance. Perform this procedure only when it is absolutely necessary to recover from a catastrophic failure.

Procedure

1. Restart the SiteProtector SP3001 appliance.

   Note: See "Starting and shutting down the SiteProtector SP3001" on page 21 for details.
   The SiteProtector SP3001 appliance restarts and two boot options appear.
2. Select the **Restore to Factory Image** option, and then press ENTER.

   Note: This operation will overwrite all existing data on the application.
3. When you are prompted to confirm your choice, click **Yes**.
4. Read the IBM Security license agreement, and then click **Accept**.
5. When the Windows Setup window appears, type the Product Key in the boxes provided.
6. Click **Next**, and then verify that the "IBM Security SiteProtector SP3001" is displayed on the LCD.

   Note: It may take several minutes for this message to appear.
7. Refer to the following procedures in the listed chapters to reconfigure the SiteProtector SP3001 appliance:
   - Chapter 3, "Connecting and configuring the SiteProtector SP3001 appliance," on page 11
   - Chapter 4, "Configuring the SiteProtector Console," on page 17

Appendix. Safety, environmental, and electronic emissions notices

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

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 provided power cord. Do not use the IBM 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

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:
The battery contains lithium. To avoid possible explosion, do not burn or charge the battery.

Do not:

- **Throw or immerse into water**
- **Heat to more than 100°C (212°F)**
- **Repair or disassemble**

Exchange only with the IBM-approved part. Recycle or discard the battery as instructed by local regulations. In the United States, IBM has a process for the collection of this battery. For information, call 1-800-426-4333. Have the IBM part number for the battery unit available when you call. (C003)

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)

Product handling information

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

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)

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

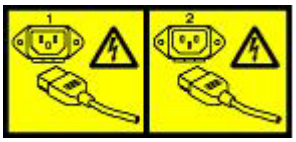
One or more of the following safety labels may apply to this product.

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. (L001)

DANGER

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



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 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

The following laser safety notices apply to this product:

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)**

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.

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 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.

Battery return program

This product contains a lithium battery. The battery must be recycled or disposed of properly. Recycling facilities may not be available in your area. For information on disposal of batteries outside the United States, go to http://www.ibm.com/ibm/environment/products/ batteryrecycle.shtm or contact your local waste disposal facility.

In the United States, IBM has established a return process for reuse, recycling, or proper disposal of used IBM sealed lead acid, nickel cadmium, nickel metal hydride, and other battery packs from IBM equipment. For information on proper disposal of these batteries, contact IBM at 1-800-426- 4333. Please have the IBM part number listed on the battery available prior to your call.

For Taiwan:

Please recycle batteries 廢電池請回收

For the European Union:

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

Batteries or packing for batteries are labeled in accordance with European Directive 2006/66/EC concerning batteries and accumulators and waste batteries and accumulators. The Directive determines the framework for the return and recycling of used batteries and accumulators as applicable throughout the European Union. This label is applied to various batteries to indicate that the battery is not to be thrown away, but rather reclaimed upon end of life per this Directive.

Les batteries ou emballages pour batteries sont étiquetés conformément aux directives européennes 2006/66/EC, norme relative aux batteries et accumulateurs en usage et aux batteries et accumulateurs usés. Les directives déterminent la marche à suivre en vigueur dans l'Union Européenne pour le retour et

le recyclage des batteries et accumulateurs usés. Cette étiquette est appliquée sur diverses batteries pour indiquer que la batterie ne doit pas être mise au rebut mais plutôt récupérée en fin de cycle de vie selon cette norme.

バッテリーあるいはバッテリー用のパッケージには、EU 諸国に対する廃電気電子機器指令 2006/66/EC のラベルが貼られています。この指令は、バッテリーと蓄電池、および廃棄バッテリーと蓄電池に関するものです。この指令は、使用済みバッテリーと蓄電池の回収とリサイクルの骨子を定めているもので、EU 諸国にわたって適用されます。このラベルは、使用済みになったとき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バッテリーに貼られています。

In accordance with the European Directive 2006/66/EC, batteries and accumulators are labeled to indicate that they are to be collected separately and recycled at end of life. The label on the battery may also include a symbol for the metal concerned in the battery (Pb for lead, Hg for the mercury, and Cd for cadmium). Users of batteries and accumulators must not dispose of batteries and accumulators as unsorted municipal waste, but use the collection framework available to customers for the return, recycling, and treatment of batteries and accumulators. Customer participation is important to minimize any potential effects of batteries and accumulators on the environment and human health due to potential presence of hazardous substances. For proper collection and treatment, contact your local IBM representative.

For California:

Perchlorate Material - special handling may apply. See http://www.dtsc.ca.gov/ hazardouswaste/ perchlorate.

The foregoing notice is provided in accordance with California Code of Regulations Title 22, Division 4.5, Chapter 33. Best Management Practices for Perchlorate Materials. This product, part, or both may include a lithium manganese dioxide battery which contains a perchlorate substance.

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 xvi IBM Internet Security Systems 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/ EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM 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 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
email: 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 89/336/EWG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EUMitgliedsstaaten 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 89/336/EWG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) vom 18. September 1998 (bzw. der EMC EG Richtlinie 89/336) für Geräte der Klasse A.

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EGKonformitätszeichen - CE - zu führen.

Verantwortlich für die Konformitätserklärung nach Paragraf 5 des EMVG ist die IBM Deutschland GmbH, 70548 Stuttgart.

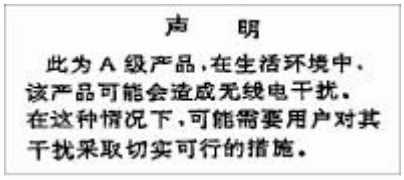
Informationen in Hinsicht EMVG Paragraf 4 Abs. (1) 4:

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

update: 2004/12/07

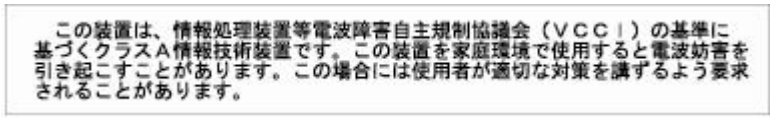
People's Republic of China Class A Compliance Statement:

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.

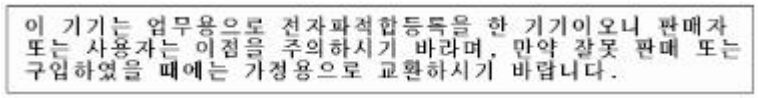


Japan Class A Compliance Statement:

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 xviii IBM Internet Security Systems domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.



Korean Class A Compliance Statement:



Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Office 4360
One Rogers Street
Cambridge, MA 02142
U.S.A

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Trademarks

IBM, the IBM logo, and ibm.com, and Lotus® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at www.ibm.com/legal/copytrade.shtml.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Index

Printed in USA