IBM Internet Security Systems

IBM Proventia Management SiteProtector Installation Guide

Version 2.0, Service Pack 8.0

Note
Before using this information and the product it supports, read the information in "Notices" on page 57.

This edition applies to version 2.0, service pack 8.0 of the IBM Proventia Management SiteProtector systemand to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright IBM Corporation 1994, 2009.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

© Copyright IBM Corp. 1994, 2009

About this book

This book provides the information you need to install IBM® Proventia® Management SiteProtector.

Intended audience

This guide is for network or security administrators or any other individuals who are responsible for installing SiteProtector and managing network security. This guide assumes that you are familiar with network devices, including configuring firewalls and proxies, and configuring Microsoft SQL databases.

Prerequisite and related information

Use the following document for information about SiteProtector configuration options:

SiteProtector Scalability Guidelines

The following table describes the SiteProtector documents you use to configure SiteProtector after you install it:

Document	Contents
SiteProtector Configuration Guide	Contains information about configuring, updating, and maintaining SiteProtector
SiteProtector Policies and Responses Configuration Guide	Contains information about configuring policies and responses, including Central Responses
SiteProtector Information Center (Help)	Contains all the procedures that you need to use SiteProtector, including advanced procedures that might not be available in a printed user document

Locate all the SiteProtector documents as portable document format (PDF) files in the following places:

- The IBM ISS Web site at http://www.iss.net/support/documentation
- The Deployment Manager

Note: Documents must be manually downloaded to the Deployment Manager.

How to send your comments

Your feedback is important in helping to provide the most accurate and highest quality information. To submit any comments about this book or any other SiteProtector documentation, end your comments by e-mail to document@iss.net. Be sure to include the name of the book, the part number of the book, the version of SiteProtector, and if applicable, the specific location of the text that you are commenting on (for example, a page number or table number.)

© Copyright IBM Corp. 1994, 2009

Chapter 1. SiteProtector introduction

SiteProtector is a centralized management system that unifies management and analysis for network, server, and desktop protection agents and small networks or appliances. You can easily scale SiteProtector to provide security for large, enterprise-wide environments.

A SiteProtector system is a centralized management system that provides command, control, and monitoring capabilities for all of your IBM ISS products.

SiteProtector architecture

Components of SiteProtector when SiteProtector is installed on three systems. This is the recommended installation.

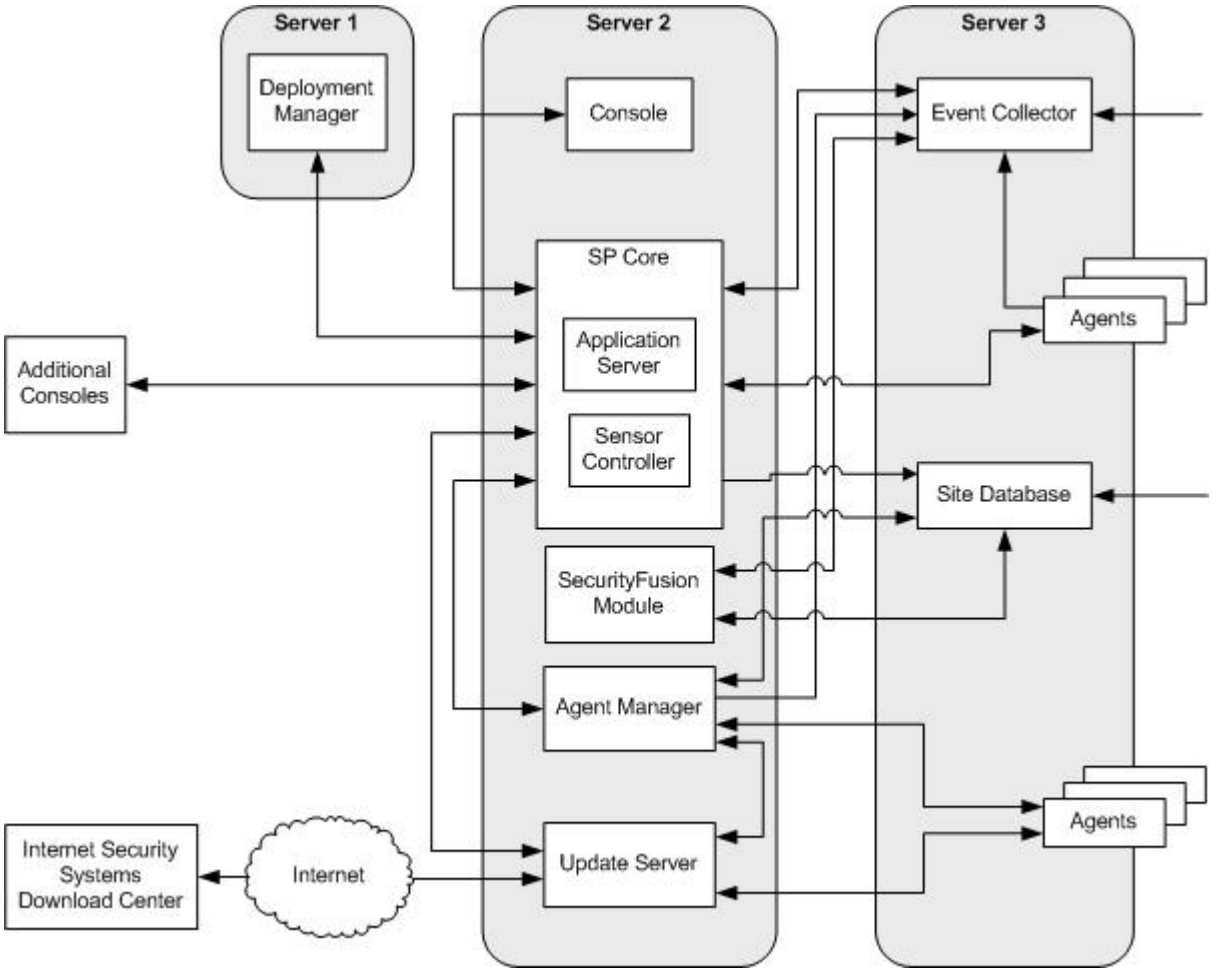


Figure 1. Components in a typical Site

Communication channels

SiteProtector system components use specific channels to communicate with each other and with other IBM ISS products. For a complete list of the ports used for communication, see the *Configuring Firewalls for SiteProtector System Traffic* document available at http://www.iss.net/support/documentation/.

© Copyright IBM Corp. 1994, 2009

SiteProtector components

This topic describes the functions of the SiteProtector components.

SiteProtector Component	Description
Agent Manager	The Agent Manager manages the command and control activities of the Desktop Protection agents and IBM ISS appliances. The Agent Manager also facilitates data transfer from agents to the Event Collector. The Agent Manager enables SiteProtector to collect and manage data from agents and components. An Agent Manager is installed with the Express and Recommended options.
Console	The SiteProtector Console is the main user interface for SiteProtector. You perform most SiteProtector functions, such as monitoring events, scheduling scans, generating reports, and configuring agents from the Console.
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 Archiver	The Event Archiver stores event data and improves performance by reducing the number of events the Site Database must store.
Event Collector	The Event Collector manages real-time events from sensors and vulnerability data from scanners.
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.
SecurityFusion™ Module	The SecurityFusion module increases your ability to quickly identify and respond to critical threats at your Site. Using advanced analysis techniques, the SecurityFusion module escalates high-impact attacks to help you focus on the most important attack activity.
Site Database	The SiteProtector database (Site 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 these components: • The Application Server, which enables communication between the SiteProtector Console and the Site Database. • The agent controller, which manages the command and control activities of agents, such as the command to start or to stop collecting events. • X-Press Update Server, which is a Web server that stores X-Press Updates (XPUs) after they have been downloaded from the IBM ISS Download center, and makes the XPUs 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, which is a read-only interface that provides easy access to SiteProtector for monitoring SiteProtector Event assets and security events.
X-Press Update Server	The X-Press Update Server is a Web server that stores X-Press Updates (XPUs) after they have been downloaded from the IBM ISS Download center, and makes the XPUs 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.

Add-on components

Add-on components available for SiteProtector provide additional protection and functions.

Note: The add-on components described here are separately licensed features available in SiteProtector.

SiteProtector Third Party Module

The SiteProtector Third Party Module retrieves data from third-party firewalls, enabling you to view firewall activity and to associate security events with specific firewalls.

SiteProtector reporting

Graphical summary and compliance reports provide the information managers need to assess the state of their security. Reports cover vulnerability assessment, attack activities, auditing, content filtering, Desktop, SecurityFusion and virus activity.

SiteProtector SecureSync Failover

The SiteProtector SecureSync Failover feature provides the user with information about how to configure SiteProtector for failover and how to recover SiteProtector after a complete failure.

Chapter 2. Hardware and software requirements

Each components of IBM Proventia Management SiteProtector has specific hardware and software requirements.

Important: The installation of some SiteProtector components requires 8dot3 short naming in the Windows FileSystem registry settings. If you have disabled short names in the registry settings on any servers on which you plan to install SiteProtector components, you must re-enable short names before installing SiteProtector.

System requirements for virtualization (VMware) support

The following table describes the system requirements for virtualization:

Component	Minimum Requirement
Virtualization	• VMware ESX Server 3.x • Microsoft Windows Server 2008 Hyper-V • Microsoft Virtual Server 2005

Note: All SiteProtector Components can be installed in a virtual environment, provided the virtual machines meet the requirements described in "System requirements for the SiteProtector Recommended option" on page 7 or "System requirements for the SiteProtector Express option" on page 6.

System requirements for Deployment Manager

Deployment Manager is a Web-based installer application that allows you to install:

- SiteProtector using the Recommended or Express option
- SiteProtector components individually
- Add-on SiteProtector products
- Other IBM ISS products

The following table describes the system requirements for the Deployment Manager:

Component	Minimum Requirement
Processor	400 MHz Pentium II 3.0 GHz Pentium 4 (recommended)
Operating system	SiteProtector supports both 32- and 64-bit versions of the following Windows operating systems: • Windows Server 2008 Standard • Windows Server 2008 Enterprise • Windows Server 2003 with Service Pack 2 • Windows Enterprise Server 2003 with Service Pack 2 **Note:** You must run SiteProtector and its components on an NTFS formatted partition. FAT and FAT32 partitions do not allow you to harden your system properly. **Note:** Refer to Knowledgebase article 3145 for more information about Windows Firewall.

© Copyright IBM Corp. 1994, 2009

Component	Minimum Requirement
RAM	256 MB 1 GB (recommended)
Free hard disk space	9 GB 40 GB (recommended)
Third-party software (included)	• IBM Java Runtime Environment (JRE), Version 1.6.0 SR 3
Third-party software not included	• Adobe Reader 8.0 or later http://www.adobe.com/products/acrobat/readstep2.html • Internet Explorer 7.0 or later http://www.microsoft.com/windows/internet-explorer/default.aspx • For the latest updates for Windows operating system software and Windows-based hardware, go to the Microsoft Update Web site at http://www.windowsupdate.com
Static IP address?	Yes

System requirements for the SiteProtector Express option

The following table describes the system requirements for the Express option:

Component	Minimum Requirement
Processor	1 GHz Pentium III Dual 3.0 GHz Pentium 4 (recommended)
Operating system	SiteProtector supports both 32- and 64-bit versions of the following Windows operating systems: • Windows Server 2008 Standard • Windows Server 2008 Enterprise • Windows Server 2003 with Service Pack 2 • Windows Enterprise Server 2003 with Service Pack 2 **Note:** You must run SiteProtector and its components on an NTFS formatted partition. FAT and FAT32 partitions do not allow you to harden your system properly. **Note:** Refer to Knowledgebase article 3145 for more information about Windows Firewall.
RAM	1 GB 2 GB (recommended)
Free hard disk space	8 GB 70 GB (recommended)
Screen resolution	1024 by 768 pixels
Third-party software (included)	• IBM Java Runtime Environment (JRE), Version 1.6.0 SR 3

Component	Minimum Requirement
Third-party software not included	• SQL Server 2008 Enterprise Edition • SQL Server 2008 Standard Edition • SQL Server 2008 64-bit • SQL Server 2005 Enterprise Edition, Service Pack 2 or later • SQL Server 2005 Standard Edition, Service Pack 2 or later • SQL Server 2005 64-bit, Service Pack 2 or later • SQL Server 2008 Express Edition • Internet Explorer 7.0 or later http://www.microsoft.com/windows/internet-explorer/default.aspx • Adobe Reader 8.0 or later http://www.adobe.com/products/acrobat/readstep2.html • For the latest updates for Windows operating system software and Windows-based hardware, go to the Microsoft Update Web site at http://www.windowsupdate.com
Static IP address?	Yes
Other requirements	Additional memory and disk space, depending upon various factors, such as the following items: • Number of views • Number of assets • Number of agents • Number of simultaneous users • Type of policies implemented on agents • Implementation of the SecurityFusion module • Amount of data to be stored on server

System requirements for the SiteProtector Recommended option

The Recommended option in Deployment Manager installs SiteProtector in two parts, and on two different computers:

First Computer	Second Computer
Installs Site Database	Installs Application Server (including X-Press Update Server)
Installs Event Collector	Installs Agent Manager
	Installs SecurityFusion module
	Installs Console (including Event Viewer)

Requirements for the first computer

The following table describes the system requirements for the computer you want to install the Database and Event Collector on:

Component	Minimum Requirement
Processor	Dual 1 GHz Pentium III Dual 3.0 GHz Pentium 4 (recommended)
Operating system	• Windows Server 2008 Standard • Windows Server 2008 Enterprise • Windows Server 2003 with Service Pack 2 • Windows Enterprise Server 2003 with Service Pack 2 **Note:** You must run SiteProtector and its components on an NTFS formatted partition. FAT and FAT32 partitions do not allow you to harden your system properly. **Note:** Refer to Knowledgebase article 3145 for more information about Windows Firewall.
RAM	2 GB (recommended)
Free hard disk space	18 GB 70 GB (recommended)
Third-party software (included)	• IBM Java Runtime Environment (JRE), Version 1.6.0 SR 3
Third-party software not included	• SQL Server 2008 Enterprise Edition • SQL Server 2008 Standard Edition • SQL Server 2008 64-bit • SQL Server 2005 Enterprise Edition, Service Pack 2 or later • SQL Server 2005 Standard Edition, Service Pack 2 or later • SQL Server 2005 64-bit, Service Pack 2 or later • Internet Explorer 7.0 or later http://www.microsoft.com/windows/internet-explorer/default.aspx • For the latest updates for Windows operating system software and Windows-based hardware, go to the Microsoft Update Web site at http://www.windowsupdate.com
Static IP address?	Yes
Other requirements	Additional memory and disk space, depending upon various factors, such as the following items: • Number of assets • Number of agents • Number of simultaneous users • Type of policies implemented on agents • Implementation of the SecurityFusion module • Amount of data to be stored on server

Requirements for the second computer

The following table describes the system requirements for the computer you want to install the following components on:

- Application Server (including X-Press Update Server)

- Console (including Event Viewer)
- Agent Manager
- SecurityFusion Module

Component	Minimum Requirement
Processor	1 GHz Pentium III 3.0 GHz Pentium 4 (recommended)
Operating system	SiteProtector supports both 32- and 64-bit versions of the following Windows operating systems: • Windows Server 2008 Standard • Windows Server 2008 Enterprise • Windows Server 2003 with Service Pack 2 • Windows Enterprise Server 2003 with Service Pack 2 **Note:** You must run SiteProtector and its components on an NTFS formatted partition. FAT and FAT32 partitions do not allow you to harden your system properly. **Note:** Refer to Knowledgebase article 3145 for more information about Windows Firewall.
RAM	1 GB (recommended)
Free hard disk space	18 GB 40 GB (recommended)
Screen resolution	1024 by 768 pixels
Third-party software (included)	• IBM Java Runtime Environment (JRE), Version 1.6.0 SR 3
Third-party software not included	• Adobe Reader 8.0 or later http://www.adobe.com/products/acrobat/readstep2.html • Internet Explorer 7.0 or later http://www.microsoft.com/windows/internet-explorer/default.aspx • For the latest updates for Windows operating system software and Windows-based hardware, go to the Microsoft Update Web site at http://www.windowsupdate.com
Static IP address?	Yes
Other requirements	Additional memory and disk space, depending upon various factors, such as the following items: • Number of views • Number of assets • Number of agents • Number of simultaneous users • Type of policies implemented on agents

Note: Testing found that the allocation of resources when using Microsoft Virtual Server 2005 affects the overall performance of SiteProtector more than instances not using Virtual Server 2005. For example, on a single processor unit where the base OS and a single virtual instance were running, SiteProtector performed much slower than it did on a hardware instance meeting the specifications of only the virtual instance. Therefore, consider providing additional resources when using Virtual Server 2005.

Systems requirements for the Console or Event Viewer

The following table describes the system requirements for a single Console or a single Event Viewer:

Component	Minimum Requirement
Processor	400 MHz Pentium II 2.4 GHz Pentium 4 (recommended)
Operating system	SiteProtector supports both 32- and 64-bit versions of the following Windows operating systems: • Windows Vista Business • Windows Vista Enterprise • Windows Server 2008 Enterprise • Windows Server 2008 Standard • Windows Server 2003 with Service Pack 2 • Windows Enterprise Server 2003 with Service Pack 2 • Windows XP with Service Pack 1 or later **Note:** You must run SiteProtector and its components on an NTFS formatted partition. FAT and FAT32 partitions do not allow you to harden your system properly. **Note:** Refer to Knowledgebase article 3145 for more information about Windows Firewall.
RAM	512 MB 1 GB (recommended)
Free hard disk space	4 GB 20 GB (recommended)
Screen resolution	1024 by 768 pixels
Color Setting	High Color (16 bit)
Static IP address?	No
Third-party software (included)	• IBM Java Runtime Environment (JRE), Version 1.6.0 SR 3
Third-party software not included	• Internet Explorer 7.0 or later http://www.microsoft.com/windows/internet-explorer/default.aspx • Adobe Reader 8.0 or later http://www.adobe.com/products/acrobat/readstep2.html • For the latest updates for Windows operating system software and Windows-based hardware, go to the Microsoft Update Web site at http://www.windowsupdate.com **Note:** The first time you click **Help** in the SiteProtector Console, you might receive a "Certificate Error" in Internet Explorer. To avoid this error in the future, install the security certificate generated by the Application Server. For more information, go to the Microsoft Support Web site: http://support.microsoft.com/kb/931850

System requirements for a Web Console

The following table describes the system requirements for the SiteProtector Web Console:

Component	Minimum Requirement
Third-party software not included	• Windows Internet Explorer 7.0 or Internet Explorer 6.0 with Service Pack 1 or later • Java J2SE Runtime Environment 5.0 (1.5.0) or later
Operating system	SiteProtector supports both 32- and 64-bit versions of the following Windows operating systems: • Windows Server 2008 Enterprise • Windows Server 2008 Standard • Windows Server 2003 with Service Pack 2 • Windows Enterprise Server 2003 with Service Pack 2 • Windows XP with Service Pack 1 or later • Windows Vista Business • Windows Vista Enterprise **Note:** Refer to Knowledgebase article 3145 for more information about Windows Firewall.

System requirements for the Event Archiver

The following table describes the system requirements for the Event Archiver:

Component	Minimum Requirement
Processor	1 GHz Pentium III 2.4 GHz Pentium 4 (recommended)
Operating system	• Windows Server 2008 Standard • Windows Server 2008 Enterprise • Windows Server 2003 with Service Pack 2 • Windows Enterprise Server 2003 with Service Pack 2 **Note:** You must run SiteProtector and its components on an NTFS formatted partition. FAT and FAT32 partitions do not allow you to harden your system properly. **Note:** Refer to Knowledgebase article 3145 for more information about Windows Firewall.
RAM	256 MB 1 GB (recommended)
Free hard disk space	9 GB 20 GB (recommended)
Third-party software not included	• For the latest updates for Windows operating system software and Windows-based hardware, go to the Microsoft Update Web site at http://www.windowsupdate.com
Static IP address?	Yes

Component	Minimum Requirement
Other requirements	Additional memory and disk space, depending upon various factors, such as the following items: • Number of agents or appliances • Number of simultaneous users • Type of policies implemented on agents or appliances • Implementation of the SecurityFusion module • Event logging

System requirements for the Event Collector or Agent Manager

The following table describes the system requirements for a single Event Collector or a single Agent Manager:

Component	Minimum Requirement
Processor	1 GHz Pentium III 2.4 GHz Pentium 4 (recommended)
Operating system	• Windows Server 2008 Standard • Windows Server 2008 Enterprise • Windows Server 2003 with Service Pack 2 • Windows Enterprise Server 2003 with Service Pack 2 **Note:** You must run SiteProtector and its components on an NTFS formatted partition. FAT and FAT32 partitions do not allow you to harden your system properly. **Note:** Refer to Knowledgebase article 3145 for more information about Windows Firewall.
RAM	256 MB 1 GB (recommended)
Free hard disk space	4 GB 20 GB (recommended)
Third-party software (included)	• IBM Java Runtime Environment (JRE), Version 1.6.0 SR 3
Third-party software not included	• For the latest updates for Windows operating system software and Windows-based hardware, go to the Microsoft Update Web site at http://www.windowsupdate.com
Dedicated system?	Yes
Static IP address?	Yes
Other requirements	Additional memory and disk space, depending upon various factors, such as the following items: • Number of agents or appliances • Number of simultaneous users • Type of policies implemented on agents or appliances • Implementation of the SecurityFusion module • Event logging

System requirements for the X-Press Update Server

The following table describes the system requirements for X-Press Update Server:

Component	Minimum Requirement
Processor	400 MHz Pentium II 2.4 GHz Pentium 4 (recommended)
Operating system	• Windows Server 2008 Standard • Windows Server 2008 Enterprise • Windows Server 2003 with Service Pack 2 • Windows Enterprise Server 2003 with Service Pack 2 **Note:** You must run SiteProtector and its components on an NTFS formatted partition. FAT and FAT32 partitions do not allow you to harden your system properly. **Note:** Refer to Knowledgebase article 3145 for more information about Windows Firewall.
RAM	256 MB 1 GB (recommended)
Free hard disk space	9 GB 20 GB (recommended)
Third-party software not included	• For the latest updates for Windows operating system software and Windows-based hardware, go to the Microsoft Update Web site at http://www.windowsupdate.com
Static IP address?	Yes

System requirements for the Third Party Module

The following table describes the system requirements for the Third Party Module.

Component	Minimum Requirement
Operating system	• Microsoft Windows Server/Enterprise Server 2003 with R2/Service Pack 1 or later • Windows 2000 Server with Service Pack 4 or later • Windows 2000 Advanced Server with Service Pack 4 or later • Windows 2000 Professional with Service Pack 4 or later
Third-party software not included	• Sun Java 2 Runtime Environment (JRE), Standard Edition, Version 1.4.1 **Note:** Do not uninstall earlier versions of JRE. If you do, you will have to reinstall JRE 1.4.1. Versions 1.4.1_01 and 1.4.1_02 are not supported.

System requirements for the SecurityFusion module

The following table describes the system requirements for the SecurityFusion module:

Component	Minimum Requirement
Processor	800 MHz Pentium III 2.4 GHz Pentium 4 (recommended) **Note:** The Pentium III processor does not exclude other processors, but acts as a guide for expected performance level. For example, support is available for 32-Bit Operating Systems running on Intel Xeon processors with EM64T (64-Bit) support. SiteProtector installed on a 64-Bit Operating System is currently not supported.
Operating system	• Windows Server 2008 Standard • Windows Server 2008 Enterprise • Windows Server 2003 with Service Pack 2 • Windows Enterprise Server 2003 with Service Pack 2 **Note:** Refer to Knowledgebase article 3145 for more information about Windows Firewall.
RAM	512 MB 1 GB (recommended)
9 GBFree hard disk space	9 GB 20 GB (recommended)
Third-party software (included)	• IBM Java Runtime Environment (JRE), Version 1.6.0 SR 3
Dedicated system?	Yes
Static IP address?	Yes
Virtualization	• VMware ESX Server 3.x. 4.x • Microsoft Windows Server 2008 Hyper-V • Microsoft Virtual Server 2005
Other requirements	Additional memory and disk space, depending upon various factors, such as the following items: • Number of simultaneous users • Number of agents or appliances • Type of policies implemented on agents or appliances

Chapter 3. Planning to install SiteProtector

Installation options

SiteProtector installation options are suited for many environments.

The following table describes the SiteProtector installation options.

Installation Option	Description
Express	Installs a streamlined version of SiteProtector on one computer. The Express option is intended for small environments and for evaluation purposes.
Recommended	Installs SiteProtector on two computers, which can provide better performance in large environments. You can add additional components without having to reinstall or significantly reconfigure your base installation.
Clustered SQL	Installs SiteProtector for Clustered SQL
Windows Authentication	Installs SiteProtector using Windows Authentication

An Event Collector, an Agent Manager, and a SiteProtector Console are included with the installation. The Event Collector and Agent Manager communicates with the Site Database and the Application Server, and the SiteProtector Console communicates with the Application Server.

Scalability Guidelines

Use this information to assist you when planning an initial deployment of SiteProtector or when expanding an existing configuration to meet increased performance demands.

Deployment scenarios

This topic suggests deployment scenarios for small, medium, and large network. Each deployment scenario has different hardware and software requirements. Consider these scenarios as you plan how you will install and configure SiteProtector.

Small network

This scenario requires one to two systems.

System one
Install SiteProtector using the express option.

Medium network

This scenario requires three to four systems.

System one
Use the recommended installation option to install the Site Database and the Event Collector.

System two
Use the recommended installation option to install the Application Server, Agent Manager, X-Press Update Server, SecurityFusion Module, and Console.

© Copyright IBM Corp. 1994, 2009

System three
Install additional Agent Manager and Event Collector components.

Large network

This scenario requires four to five systems.

System one
Use the recommended installation option to install the Site Database and the Event Collector.

System two
Use the recommended installation option to install the Application Server, Agent Manager, X-Press Update Server, SecurityFusion Module, and Console.

System three
Install additional Agent Manager and Event Collector components.

System four
Install additional Agent Manager and Event Collector components.

Recommendations

This topic gives recommendations for hardware, software, and free disk space. The recommendations are based on typical customer environments and might not apply to your specific environment.

Important: This document provides sizing criteria for events and heartbeats. Do not exceed the average events per day or the maximum heartbeats per day regardless of the number of sensors in your configuration.

Hardware and software

Hardware and software recommendations are based on the following items:

Item	Description
Maximum events per day for the site	This number represents the maximum number of events processed per day throughout the entire site. The recommendations in this guide assume that the total number of events per day in your entire site will not consistently exceed the number in this column.
Maximum heartbeats per day	This number represents the maximum number of heartbeats the database processes per day throughout your entire site. The recommendations in this guide assume that the total number of events per day in your entire site will not consistently exceed the number in this column.

Free hard disk space

Free hard disk space recommendations are based on the following:

- expected event volume
- space required to store event data for 30 days
- space required to perform periodic database maintenance

Database layout

For information about the layout of your database files, go to the Microsoft SQL Web site at: http://www.microsoft.com/sql/

Performance considerations

If the average events per day and the maximum heartbeats per day in your site are consistently higher than the following guidelines, your site can experience performance problems regardless of the number of agents you are using. Potential problems include the following:

- The console may become slow or unresponsive.
- The database may become temporarily unable to accept new events until the activity drops to within the constraints for your configuration.
- The database may process events at a very slow rate until the activity drops to within the constraints for your configuration.

If the activity in your environment exceeds the constraints for your deployment size, consider using the following guidelines to scale your deployment.

Factors that impact performance

Several factors can impact the overall performance and responsiveness of SiteProtector:

- multiple console operations
- long-running analysis queries
- report generation
- fusion analysis
- attack patterns
- maintenance operations

Event Collector and Agent Manager setup

For medium and large deployments, IBM ISS recommends that you install Events Collectors and Agent Managers on the same computer. The system requirements for installing the Agent Manager on a dedicated system also apply to Event Collector and Agent Managers that share the same computer. For more information about Agent Manager requirements, refer to the *SiteProtector System Requirements*.

When to use multiple Agent Managers and Event Collectors

Multiple Event Collector and Agent Manager pairs are required to accommodate the increased bandwidth that is needed during agent updates, including providing redundancy. However, increasing the number of Agent Manager or Event Collectors does not increase the event and heartbeat limits stated in this document.

For Medium and Large Deployments

To optimize performance, the Event Collector installed on the database server should only be used for redundancy purposes. This allows for server resources to be dedicated to the database service, which may improve performance.

To optimize performance, the Agent Manager on the application server should only be used for redundancy purposes. This allows for server resources to be dedicated to the application server services, which can improve performance.

Update Servers for Proventia Desktop 9.0

Version 9.0 of Proventia Desktop includes signature-based antivirus and anti-spyware scanning, which requires frequent updates to virus definitions. To ensure that you can accommodate these updates, see the knowledge base article *How many Update Servers will I need to support Proventia Desktop 9.0 Agents?* (Answer ID 3830) at http://iss.custhelp.com/cgi-bin/iss.cfg/php/enduser/std_adp.php?p_faqid=3830.

Small deployment

A small deployment of SiteProtector can be installed on a single computer.

Environment

A small deployment is appropriate in the following environment:

Deployment Type	Maximum Events Per Day	Maximum Heartbeats Per Day	Recommended Number of Event Collectors and Agent Managers
Small	50,000	1,000[a]	1[b]

[a] Assumes no more than 500 Proventia Desktop or RealSecure Desktop Agents.

[b] See "When to use multiple Agent Managers and Event Collectors."

Hardware and software

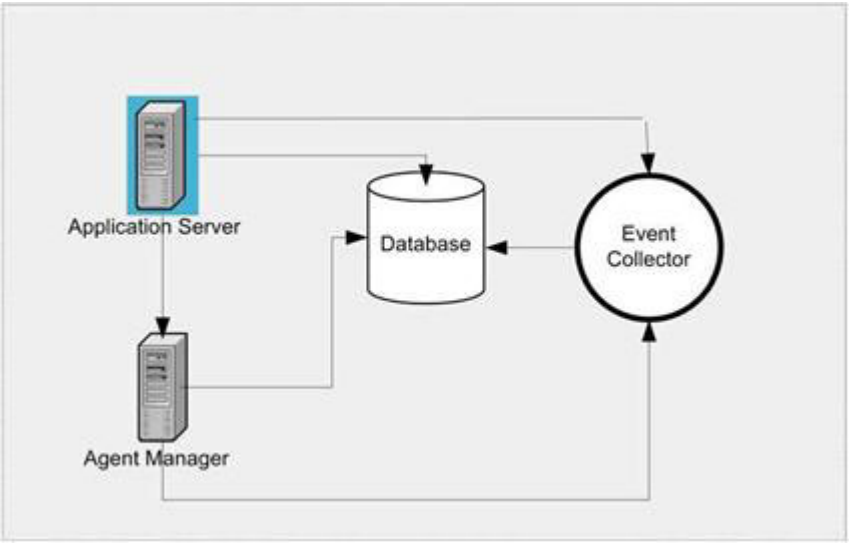
The following table gives hardware and software recommendations for a small deployment:

Item	Recommendation
processor	(2) 2.4 GHz Xeon
operating system	Windows Server 2008
SQL Server	2008
RAM	2 GB
free hard disk space	36-73 GB

Note: Please see *SiteProtector System Requirements* for minimum requirements and a list of all supported operating systems and database servers.

Diagram

The following figure illustrates the small deployment diagram:



Medium deployment

A medium deployment of SiteProtector can be installed on four or more computers:

Computer	Components
1	Application Server
2	Database
3 and 4	Event Collector
	Agent Manager

Environment

A medium deployment is appropriate in the following environment:

Deployment Type	Maximum Events Per Day	Maximum Heartbeats Per Day	Recommended Number of Event Collectors and Agent Managers
Medium	2,500,000	100,000[a]	2[b]

[a] Assumes no more than 15,000 Proventia Desktop or 10,000 RealSecure Desktop Agents.

[b] See "When to use multiple Agent Managers and Event Collectors."

Hardware and software

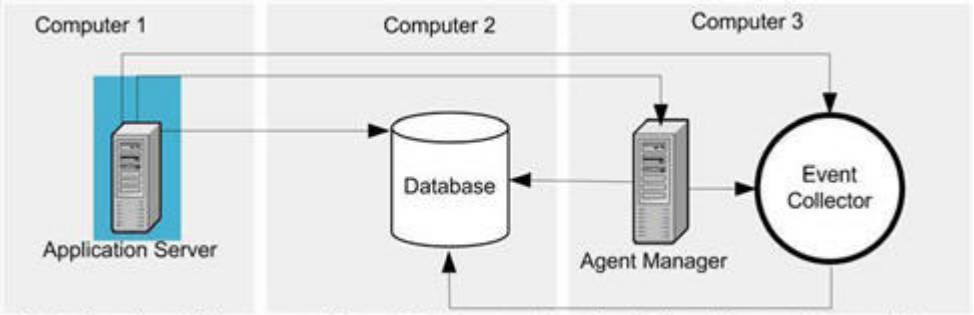
The following table gives hardware and software recommendations for the medium deployment:

Computer	Item	Recommendation
1 (Application Server)	processor	(1) 2.4 GHz Xeon
	operating system	Windows Server 2008
	RAM	2 GB
	free hard disk space	36 GB
2 (Database)	processor	(2) 3.0 GHz Xeon
	operating system	Windows Server 2008
	SQL Server	SQL Server 2008
	RAM	4 GB
	free hard disk space	73 to 438 GB as follows: • 15K RPM SCSI disk • RAID configuration • multiple controllers
3 and 4 (Event Collector/Agent Manager)	processor	2.4 GHz Xeon Intel Pentium 4
	operating system	Windows Server 2008
	RAM	1 GB
	free hard disk space	36 GB

Note: See Chapter 2, “Hardware and software requirements,” on page 5 for minimum requirements and a list of all supported operating systems and database servers.

Diagram

The following diagram illustrates a medium deployment:



Note: More Agent Managers and Event Collectors can be added to the deployment as needed.

Large deployment

A large deployment of SiteProtector can be installed on five or more computers:

Computer	Components
1	Application Server
2	Database
3, 4, and 5	Event Collector
	Agent Manager

Environment

A large deployment is appropriate in the following environment:

Deployment Type	Maximum Events Per Day	Maximum Heartbeats Per Day	Recommended Number of Event Collectors and Agent Managers
Large	5,000,000	300,000[a]	5[b]

[a] Assumes no more than 50,000 Proventia Desktop or 25,000 RealSecure Desktop Agents.

[b] See "When to use multiple Agent Managers and Event Collectors."

Hardware and software

The following table gives hardware and software recommendations for the large deployment:

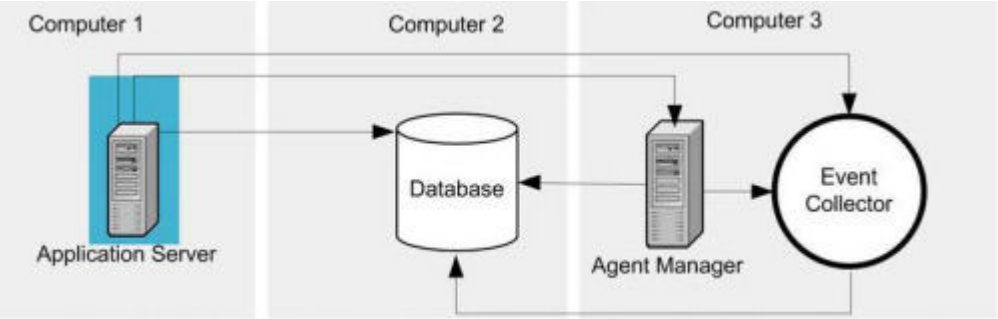
Computer	Item	Recommendation
1 (Application Server)	processor	(2) 3.2Ghz Xeon with 2 MB cache
	operating system	Windows Server 2008
	RAM	2 GB
	free hard disk space	36 GB

Computer	Item	Recommendation
2 (Database)	processor	(4) 3.2Ghz Xeon with 2 MB cache
	operating system	Windows Server 2008
	SQL Server version	SQL Server 2008
	RAM	8 GB
	free hard disk space	143-730 GB with the following specifications: • 15K RPM SCSI disk • RAID configuration • multiple controllers
3, 4, and 5 (Event Collector/Agent Manager)	processor	2.4 GHz Xeon Intel Pentium 4
	operating system	Windows Server 2008
	RAM	1 GB
	free hard disk space	36 GB

Note: Please see *SiteProtector System Requirements* for minimum requirements and a list of all supported operating systems and database servers.

Diagram

The following illustrates the large deployment diagram:



Multiple-site deployment

If your current configuration is too large, consider dividing it into several smaller sites. Use the guidelines and requirements for the small, medium, and large deployments described in this topic to help you choose the best deployment for each site.

The multiple-site deployment consists of several large deployments that report to a Site Summary instance. Use the multiple-site deployment if the following conditions apply:

- the sizing criteria for your configuration exceeds the numbers specified in the large deployment
- your configuration is distributed over a large geographic area

Installation considerations

Miscellaneous installation information

Additional requirements

In addition to meeting the system requirements, you must also meet the following requirements:

- Install SiteProtector on a dedicated computer.
- Do not use the SiteProtector computer as a DNS server or a proxy server.
- Do not install SiteProtector on systems that have been set up as primary or backup domain controllers.

Express installation domain names

You must use a fully-qualified domain name of up to 64 characters during the express installation.

Encryption key archives

You can archive encryption keys for the following components:

- Agent Manager
- X-Press Update Server (stand-alone version)

When you install or uninstall these components, you are prompted to specify an archive directory. Specify a non-local location, preferably on a removable medium. Encryption key archives can simplify disaster recovery if your server fails. If you do not archive encryption keys, these certificates are deleted if you uninstall the components that are using these keys. You then must redistribute certificates to the clients that communicate with this server. Redistributing server certificates can require significant time and effort if, for example, the server is an Agent Manager that must communicate with thousands of Desktop agents. This only applies if you are requiring your clients to validate certificates from this server ("Explicit Trust" or First "Time Trust" options).

Guidelines for selecting cryptographic providers

When you install the Deployment Manager, RSA is selected as the default cryptographic provider for all SiteProtector communication. RSA is the default provider for Microsoft operating systems, and it is supported by all IBM ISS products.

Important: The installation program gives you the option to select non-default cryptographic providers if they are installed on your computer. Non-default cryptographic providers are not supported. You are responsible for configuring these providers and making sure that they are compatible with agents and components that are communicating with SiteProtector.

Multiple IP addresses and hard drives

If you have multiple IP addresses or hard drives:

- Multiple IP addresses: You must select the IP address that clients (components on other computers) will use to communicate with the computer.
- Multiple hard drives: You must specify a hard drive.

Manually adding users to the database

To manually add users into SQL Server and the Site Database, use the Domain\Username format. Failure to do so can result in user conflicts during component installation. To use NT Authentication, you must manually add users before installing SiteProtector components.

Microsoft Windows Server 2003/2008

If you are running Microsoft Windows Server 2003/2008:

- Disable the hardened download option. By default, Microsoft Windows Server prevents you from opening program files from a browser. The installation program prompts you to save the files and run them on your local drive. To run the installation program from a remote location you must disable this security setting.
- Add the following sites to your list of trusted sites before you download files from the IBM ISS Download Center:
  - https://www.iss.net
  - http://www.iss.net

Windows Terminal Server

Due to an installation limitation with the Windows 2003 Terminal Server, you might need to use the Windows Add/Remove Programs control to install SiteProtector components if you use the Deployment Manager. To run all installation programs, you must download the installation application, rather than run it from the remote server.

Note: Disable font smoothing on Windows 2008 Terminal Series.

SQL Server Cluster

The SiteProtector Database is the only SiteProtector component that you can install on a SQL Server Cluster.

Locating Installation Programs

SiteProtector provides stand-alone programs for basic installation packages, add-on components, and modules. You can access these programs from several sources.

Stand-alone programs

You can use stand-alone programs to install SiteProtector components separately from the Deployment Manager. Because these files are not installed from a central location, you might need to enter additional information if you use them.

Locations of installation programs

You can access installation programs from the following locations:

Source	Description
Deployment Manager	The Deployment Manager provides a central location for downloading installation programs and can ensure that communication between SiteProtector components is configured correctly. IBM ISS recommends that you run all installation programs from the Deployment Manager. To use the Deployment Manager to its full potential, you must install it on your network.
IBM ISS product DVD	The IBM ISS product DVD contains stand-alone installation programs and includes the Deployment Manager.

Source	Description
IBM ISS Download Center	The IBM ISS Download Center provides the most up-to-date versions of the Deployment Manager and Express installation programs. The IBM ISS Download Center is available from the IBM ISS Web site at http://www.iss.net/download/

Information generated by the installation programs

The installation programs generate log files that contain information about the installation process. Also, a unique identification number is assigned to each SiteProtector installation performed from Deployment Manager. Use this information for troubleshooting installation problems or when communicating with IBM ISS Customer Support.

Log files

Installation programs generate a log file for each SiteProtector component you install. The installation programs also create a detailed log file for each bulk copy of data loaded into a particular table on the Site Database. The installation programs prompt you to view these logs when the installation program is complete if any errors or warnings have occurred.

Deployment Manager Identification number

A unique identification number is assigned to each SiteProtector installation performed from Deployment Manager. This number is for tracking purposes. A new identification number is assigned when you restart the installation process.

Note: To view this identification number, click Cancel to stop the installation program. The identification number then appears on the main page.

Preparing to install SiteProtector

Before you install SiteProtector, you need to harden security and implement measures to ensure that the systems on which you will install SiteProtector are secure.

Security considerations

Before you install a SiteProtector component on a system, consider the ways in which you can harden the system security, such as enabling screen savers or limiting the number of installed applications.

You can increase the security of systems by implementing the following measures:

- Enable screen savers with password authorization. This will help prevent unauthorized use of SiteProtector.
- Limit the number of application that are installed on a SiteProtector system.

Screen savers

Follow these guidelines when you enable screen savers:

- Use a screen saver that has a blank screen. Blank screen savers do not use as much CPU or memory as other screen savers.
- Set a short time-out period.
- Protect screen savers with passwords.

Tip: Lock the system when it is unattended, to prevent unauthorized access.

Limit the number of applications

Do not install additional applications on systems where you will install SiteProtector components, if possible. Additional applications can introduce security risks.

Preparing the Site Database system

Microsoft SQL Server software is a powerful database query application that helps organize and maintain up-to-date SiteProtector event information. However, SQL Server can make your system vulnerable to certain types of attacks. Before you install SiteProtector on the Site Database system (or another system where SQL Server is installed), ensure that the system has been properly prepared.

Procedure

1. Apply the latest updates for Microsoft Windows. You can download the updates from the Microsoft Web site at http://www.microsoft.com.
2. Harden the security of SQL Server.

Preparing systems on which you will install a SiteProtector component

Before you install SiteProtector components, ensure that the system has been properly prepared.

Procedure

1. Install Microsoft service packs and hotfixes.
2. Ensure that the latest version of Microsoft Internet Explorer and all related patches are installed.
3. Ensure that a screen saver with password authorization is enabled.

Installing Microsoft updates

To correct potential security flaws, update Microsoft Windows operating systems with the latest service packs, hotfixes, and security patches. When you apply updates, follow best practices, such as quality assurance testing and performing change control.

Microsoft updates

Microsoft provides different types of updates: service packs. hot fixes, and security patches.

Service pack
Cumulative updates that correct known problems and provide tools, drivers, and updates that extend product functionality.

Hotfix Code patches for products that are provided to individual customers when they experience problems. Groups of hotfixes that undergo more rigorous testing are periodically incorporated into service packs.

Security patches
Code patches that are similar to hotfixes, but actually eliminate security vulnerabilities. Install security patches as soon as possible because they protect your configuration against viruses and attackers.

Downloading Microsoft updates

About this task

Download the latest Microsoft patches from the Microsoft Web site (http://www.microsoft.com). Click "Microsoft Update" on the main page under Product Resources. You can also download the Critical Updates Package notification service from this Web site. After you install this service, it automatically notifies you about critical updates.

Managing Microsoft updates

About this task

Microsoft provides several utilities to manage updates if you do not have access to the Internet. Use the utilities described in the following table to determine which updates to download and how to manage these updates after you have installed them on your computer:

Utility	Description
Hfnetcheck	Identifies any hotfixes that have not been applied to your specific computer **Tip:** Run this utility in verbose mode (-v suffix).
Qchain	Verifies that hotfixes were installed in the correct order **Tip:** Run Qchain with the -z suffix.
Qfecheck	Verifies that hotfixes were installed properly **Tip:** Run this utility in verbose mode (-v suffix).

Installation checklists

This chapter provides a process overview and checklists to help ensure that you understand the tasks that are required at your Site and can perform them efficiently.

Recommendation

IBM ISS recommends that you make a copy of the checklists in this section and use them to keep track of your progress. Use the check boxes to either check off a completed task or to mark off a task that does not apply to your situation.

Pre-Installation Checklist

You must meet certain requirements and complete several setup tasks before you install SiteProtector. This topic provides a checklist to help you complete these tasks.

Checklist

The following table provides a checklist to ensure that you perform all the tasks required before you install SiteProtector:

✓	Task
☐	Purchase licenses for the agents that you plan to add to SiteProtector and have the license files available for the installation. **Note:** If you have not received these files, send an e-mail to mailto://licenses@iss.net.
☐	Verify that the computers you will be using meet the system requirements.
☐	Obtain administrator privileges on each computer where SiteProtector components will be installed, including administrator privileges for SQL Server.
☐	Decide which installation option you want to use.
☐	Read the readme document that applies to the SiteProtector release that you are installing.
☐	Install the required third-party software, and the latest patches. See the *SiteProtector System Requirements* for a list of required third-party software.
☐	Harden Windows and SQL Server software.

✓	Task
☐	If you install SiteProtector on the Windows 2003 operating system, then add the following sites to your list of trusted sites: • https://www.iss.net • http://www.iss.net
☐	Set up your Internet connection on the Application Server using Internet Explorer.
☐	Develop a strategy for archiving encryption keys, such as storing them in a remote location or on removable media.

Information Required Checklist

This topic provides a checklist of information that you might need to complete the installation procedures in this guide. Review this checklist to make sure that the information is available before you begin the installation process.

Important: Additional information might be required for the specific program that you are installing. This information is listed in each topic.

Checklist

The following table provides a checklist of the information you need to have before you install SiteProtector:

✓	Information for the Installation Programs
☐	A unique name for your Site or components to distinguish them in a multi-Site or multi-component environment.
☐	The IP address or fully qualified domain name for each computer where SiteProtector is installed.
☐	The fully qualified SQL Server Name for the Site Database computer in one of the following formats: • *ComputerName* • *ComputerName\NamedInstance* • *ComputerName.DomainName.com* • *ComputerName.DomainName.com\NamedInstance*
☐	The computer drives where you want to install SiteProtector components if more than one drive is available.
☐	The URL of the Deployment Manager if you are installing from a Deployment Manager.
☐	If you have more than one network interface card on the computer, you must know which IP address other SiteProtector components will use to communicate with the component you are installing.

Installing the Express Option from Deployment Manager

The Express option from Deployment Manager installs SiteProtector on one computer.

Task overview

The following table provides an overview of the tasks you must complete to install the Express option from Deployment Manager:

Task	Description
1	Download the Deployment Manager installation file(s) from one of the following locations: • IBM ISS Download Center • IBM ISS product DVD

Task	Description
2	Install the Deployment Manager. During the installation, you must download the express installation package. The computers where you plan to install SiteProtector must have network access to the Deployment Manager.
3	Install the Express option on the Deployment Manager.
4	Verify that the TCP/IP protocol is enabled on the computer where you are installing SiteProtector.
5	Install optional modules. • For information about configuring Event Archiver, see the *SiteProtector Configuration Guide*. • For information about installing and configuring Third Party Modules, see the *SiteProtector Third Party Module Guide*.

Installing the Express Option without the Deployment Manager

The Express option installs SiteProtector on one computer.

Task overview

The following table provides a checklist of the tasks you must complete to install the Express option:

✓	Task	Description
☐	1	Download the Express option from the IBM ISS Download Center or the IBM ISS product DVD.
☐	2	Install SiteProtector using the Express option.
☐	3	Install optional modules by downloading them from the IBM ISS Download Center or access the installation files on the IBM ISS product DVD. • For information about configuring Event Archiver, see the *SiteProtector Configuration Guide*. • For information about installing and configuring Third Party Modules, see the *SiteProtector Third Party Module Guide*. .

Recommended Option Tasks

The Recommended option installs SiteProtector on more than one computer. This option is available only from the Deployment Manager.

Task Overview

The following table provides a checklist of the tasks you must complete to install the Recommended option:

Task	Description
1	Access the Deployment Manager installation files from one of the following locations: • IBM ISS Download Center • IBM ISS product DVD
2	Install the Deployment Manager. The computers where SiteProtector is installed must have network access to the Deployment Manager.
3	Install the Site Database and the Event Collector on one computer.
4	Install the Application Server, SiteProtector Core, Agent Manager, XPress Update Server, and the SiteProtector Console on the other computer.

Task	Description
5	Install optional X-Press Update Servers.
6	Install optional modules. • For information about configuring Event Archiver, see the *SiteProtector Configuration Guide*. • For information about installing and configuring Third Party Modules, see the *SiteProtector Third Party Module Guide*.

Post-Installation Tasks

These tasks help ensure that SiteProtector components can communicate securely. You perform these tasks after you install SiteProtector, and the optional modules, but before you configure SiteProtector

Task Overview

The following table provides a list of optional post-installation tasks:

Task	Description
1	Secure database communications.
2	Enable communication through firewalls. See *Configuring Firewalls for IBM SiteProtector Traffic* (http://documents.iss.net/literature/SiteProtector/ConfiguringFirewallsSPTraffic20SP70.pdf).

Next steps

After you install SiteProtector, you must complete the SiteProtector setup process. During this process, you will perform all the tasks required to use SiteProtector for the first time, such as the following:

- Add licenses/tokens
- Configure SiteProtector agents
- Update SiteProtector agents
- Set up SiteProtector users and permissions
- Set up groups for network assets
- Set up other IBM ISS products to work with SiteProtector
- Configure security policies and responses
- Add network assets to SiteProtector

For information and instructions to guide you through this process, see the *SiteProtector Configuration Guide* and the *SiteProtector Policies and Responses Configuration Guide*.

Advanced Database Platform Tasks

This topic provides task overview information for the procedures you must perform to install SiteProtector using either SQL Server Cluster or 64-bit the SQL Server.

Task Overview

The following table provides a list of SQL platform installation tasks:

Task	Description
1	Access the package installation files from the IBM ISS product DVD.
2	Install the Site Database.

Task	Description
3	Install the Event Collector, Agent Manager, and the SiteProtector Console.
4	Install the Application Server, Agent Manager, and Console.
5	Install optional additional components.
6	Install optional modules. • For information about configuring Event Archiver, see the *SiteProtector Configuration Guide*. • For information about installing and configuring Third Party Modules, see the *SiteProtector Third Party Module Guide*.

SiteProtector Package Installation Task

This topic provides a task overview for the procedures you must perform to install the individual SiteProtector packages.

Use this method if you plan to perform the following tasks:

- Authenticate Windows NT on the SQL Server Database
- Install in a SQL Server cluster environment
- Install the SiteProtector components in a configuration other than the recommended or express options

Task Overview

The following table provides a checklist of Windows NT authentication installation tasks:

Task	Description
1	Access the package installation files from the IBM ISS product DVD.
2	Install the Site Database.
3	Install packages in the following order: 1. Event Collector 2. Application Server 3. Agent Manager 4. Console
4	Install optional modules. • For information about configuring Event Archiver, see the *SiteProtector Configuration Guide*. • For information about installing and configuring Third Party Modules, see the *SiteProtector Third Party Module Guide*.

Chapter 4. Installing SiteProtector

This chapter describes the options and procedures for installing SiteProtector.

Installing the Deployment Manager

After you have installed the Deployment Manager, you can use it to deploy SiteProtector and IBM ISS software to other systems on your network.

Downloading the installation files for the Deployment Manager

Download SiteProtector installation files from the IBM Internet Security Systems Download Center.

Procedure

1. In Internet Explorer, type the address of the Download Center: http://www.iss.net/download/.
2. In the Business Security Products section, click **Sign in to the Download Center**. The Sign in to Downloads page appears.
3. Enter the **User ID** and **Password**, and then click **Sign In**. The Download Center page appears.
4. In the Select a Product menu, select **SiteProtector**.
5. Click **Go**. The SiteProtector Downloads for Existing Customers page appears.
6. Click the **Full Installs** tab.
7. Click **Continue** on **SiteProtector 2.0 Service Pack 8**. The License Agreement window appears.
8. Review the license agreement, click **I Agree**, and click **Submit**. The File Download window appears.
9. Click **Download** on **Deployment Manager 8.1 for SiteProtector 2.0 Service Pack 8**.
10. Save the file to your computer.

Running the installation program for the Deployment Manager

Procedure

1. Run the program file.
2. Follow the instructions on the screens to complete the installation.

Results

Now that you have installed the Deployment Manager, you can use it to install modules, components, and agents. You can access the Deployment Manager from any system on the network that has access to it.

Starting the Deployment Manager

This topic provides a procedure for starting the Deployment Manager.

Procedure

1. Open Internet Explorer on the computer where you want to install a component.
2. In the **Address** box, type the location of the Deployment Manager in the following format: `https://ip_address_or_server_name:3994/deploymentmanager/index.jsp` . The Deployment Manager Main Menu appears.

   Tip: Add the address of your Deployment Manager to your Favorites list so that you can get to it quickly when you install additional applications.

© Copyright IBM Corp. 1994, 2009

Installing the express option

The express option installs a version of SiteProtector that you can use for evaluation purposes or a small environment. It includes all default SiteProtector components, except for the Deployment Manager. You can install the express option either from the Deployment Manager or the Download Center.

Preparing to install the express option

About this task

The Express option lets you use an existing SQL Server database on your computer. If an existing SQL Server database on your computer is not up-to-date, you must perform one of the following actions, and then run the Express installation again:

- Upgrade the database to the minimum requirements.
- Uninstall the database instance that does not meet the minimum requirements.

Do the following before you install the Express option:

- Download and install the SiteProtector Express Setup program file from the IBM ISS Download Center or use Deployment Manager to perform the Express installation.
- If you have two or more SQL Server instances on this computer, then you must select the instance where you want to install the Site Database.
- If you want to install a version of SQL Server in a language other than English, you must install it first, and then run the Express installation.

Enabling SQL Server Express communication over TCP/IP

About this task

By default, the SQL Server 2008 Express database is not configured to communicate over the TCP/IP protocol. If you are installing a Site Database that uses SQL Server Express, then you must enable the TCP/IP protocol before the Site Database can function properly.

Procedure

1. On the Start menu, click **All Programs** → **Microsoft SQL Server 2008** → **Configuration Tools** → **SQL Server Configuration Manager**.
2. Click **SQL Server 2008 Services**.
3. Expand the **SQL Server 2008 Network Configuration** node, and then select **Protocols for MSSQLServer** ***(SQL Instance Name)***.
4. Right-click **TCP/IP**, and then click **Enable**.
5. Select **SQL Server 2008 Services** in the tree.
6. Right-click **SQL Server** ***(SQL Instance Name)***, and then click **Restart**.

Installing the express option from the Deployment Manager

Before you begin

If you do not have a SQL Server instance installed, you must install SQL Server Express before you continue.

Procedure

1. Open the Deployment Manager on the computer where you want to install the Express installation option, click **Install SiteProtector**, and then click **Express Installation**. The Prerequisites page appears.

2. Verify that the remaining prerequisites for the SiteProtector Express installation option are installed on your computer, and then click **Next**.
3. Review the terms of the license agreement, and then click **I Accept**. The Prepare to Install page appears.
4. Review the information, and then click **Install**. The File Download window appears.
5. Click **Open**.

   Note: If security settings prevent you from opening this file, click Save and run this file locally.
6. Type the name of the Site you are creating, and then click **Next**.

   Tip: Choose a meaningful name to distinguish this Site from others in a multi-site environment.
7. If the SQL Server window appears, select the SQL Server instance where you are installing the Site Database, and then click **Next**.
8. In the Encryption Key Archival window, type the **Folder** location, and then click **Next**. Specify a folder on a non-local medium, such as a network or Zip drive.
9. In the InstallShield Wizard Complete window, click **Finish**.

   Note: By default, the installation program automatically creates and places a SiteProtector Console icon in the desktop folder. If you do not want a SiteProtector Console icon to be created, clear the check box.

Installing the express option from the Download Center

Before you begin

If you do not have a SQL Server instance installed, you must install SQL Server Express before you continue.

Procedure

1. Run the `SiteProtectorExpress-Setup.exe` file. The Welcome window appears.
2. Click **Next**. The License Agreement window appears.
3. Review the terms of the license agreement, click **I accept**, and then click **Next**. The Choose Destination Location window appears.
4. Select the default folder or select a folder in the Open window, and then click **Next**. The Site name window appears.
5. Type the name of the Site you are creating, and then click **Next**.

   Tip: Choose a meaningful name to distinguish this Site from others in a multi-site environment.
6. If the SQL Server window appears, select the SQL Server instance where you are installing the Site Database, and then click **Next**.
7. In the Encryption Key Archival window, type the **Folder** location, and then click **Next**. Specify a folder on a non-local medium, such as a network or Zip drive.
8. In the InstallShield Wizard Complete window, click **Finish**.

   Note: By default, the installation program automatically creates and places a SiteProtector Console icon in the desktop folder. If you do not want a SiteProtector Console icon to be created, clear the check box.

Installing the recommended option

You can use the Deployment Manager to install SiteProtector using the recommended option. This is a two-part process; first you install the Site Database and the Event Collector, and then you install the Application Server, Agent Manager, X-Press Update Server, and a Console.

Installing the Site Database and the Event Collector

Procedure

1. Open the Deployment Manager on the computer where you want to install the Site Database and the Event Collector, and then click **Install SiteProtector**. The Installation Options page appears.
2. Click **Recommended Installation**. The Choose Recommended Installation Part 1 or 2 page appears.
3. Click **Part 1: Install Site Database and Event Collector on first computer**. The Prerequisites page appears.
4. Ensure that the prerequisites for the SiteProtector Recommended installation option are installed on your computer, and then click **Next**. The Data File and Log File Information page appears.
5. Review the information, and then click **Next**. The Site Information page appears.
6. Type a Site name and the DNS name or IP address of the computer where the Application Server will be installed in Part 2, and then click **Next**. The Prepare to Install page appears.
7. Review the information, and then click **Install**. The File Download window appears.
8. Click **Open**.

   Note: If security settings prevent you from opening this file, click **Save**, and then run this file locally.
9. Click **Yes** in the Security Warning window to install and run SiteProtector. When the installation is complete, a message appears, indicating that the installation was successful.

Install the Application Server, Agent Manager, X-Press Update Server, and a Console

Procedure

1. Open the Deployment Manager on the computer where you want to install Part 2.
2. Click **Install SiteProtector**. The Installation Options page appears.
3. Click **Recommended Installation**. The Choose Recommended Installation Part 1 or 2 page appears.
4. Click **Part 2: Install Application Server, Agent Manager, X-Press Update server, and Console on second computer**. The Prerequisites page appears.
5. Ensure that the prerequisites for the SiteProtector Recommended installation option are installed on the computer, and then click **Next**. The SQL Server Information page appears.
6. Enter the name of the SQL Server where the Site Database is installed, and then click **Next**. The Prepare to Install page appears.
7. Review the information, and then click **Install**. The File Download window appears.
8. Click **Open**, and then click **OK**.

   Note: If security settings prevent you from opening this file, click **Save**, and then run this file locally.
9. Click **Yes** on the Security Warning window to install and run SiteProtector. The SSL certificate window appears.
10. In the **Folder** box, type a location where you want to archive encryption keys, and then click **Next**.

    Note: IBM ISS strongly recommends that you specify a folder on a non-local medium, such as a network or Zip drive.
11. Click **Next**.

Note: By default, the installation program automatically creates and places an IBM ISS icon in the desktop folder. If you do not want an the IBM ISS icon to be created, clear the check box.
When the installation is complete, a message appears that indicates the installation was successful.

Installing SiteProtector on a SQL Server cluster

If the SQL Server cluster is running SQL Server Enterprise, you can install SiteProtector. The SQL Server cluster can use either SQL or Windows NT authentication; it cannot use implicit trust.

About this task

You must install the individual packages in the following order:

1. Site Database
2. Event Collector
3. Application Server
4. Agent Manager
5. Console
6. Other packages, such as the SecurityFusion Module or Event Archiver

Installing SiteProtector on a SQL Server cluster that uses SQL authentication

Procedure

1. Install the SSL certificate on all cluster nodes.

   Note: For more information about installing an SSL certificate, see one of the following Microsoft Web pages:
   - How to enable SSL encryption for SQL Server 2000 (http://support.microsoft.com/?kbid=276553) or with SQL Server 2005 (http://support.microsoft.com/kb/318605/en-us) with Certificate Server
   - How to enable SSL encryption for SQL Server 2000 or 2005 with Microsoft Management Console (http://support.microsoft.com/kb/316898/en-us)
2. Install the Site Database from the package.

   Important: Do not use the Deployment Manager. Do not install anything except the database on the computer where the clustered SQL is installed.
3. Install the Event Collector on a separate computer from the package or the Deployment Manager.
4. Open the Deployment Manager on the computer where you want to install the Application Server, Agent Manager, X-Press Update Server, and Console.

   Note: The Application Server requires the SSL certificate before it can communicate with the Site Database. The Application Server installation program verifies that you are installing it on a cluster platform and checks for the required SSL certificate. If the certificate is unavailable, SSL will be turned off.
5. Click **Install SiteProtector**. The Installation Options page appears.
6. Click **Recommended Installation**. The Choose Recommended Installation Part 1 or 2 page appears.
7. Click **Part 2: Install Application Server, Agent Manager, X-Press Update server, and Console on second computer**. The Prerequisites page appears.
8. Ensure that the prerequisites for the SiteProtector Recommended installation option are installed on the computer, and then click **Next**. The SQL Server Information page appears.
9. Enter the name of the SQL Server where the Site Database is installed, and then click **Next**. The Prepare to Install page appears.

10. Review the information, and then click **Install**. The File Download window appears.
11. Click **Open**, and then click **OK**.

    Note: If security settings prevent you from opening this file, click **Save**, and then run this file locally.
12. Click **Yes** on the Security Warning window to install and run SiteProtector. The SSL certificate window appears.
13. In the **Folder** box, type a location where you want to archive encryption keys, and then click **Next**.

    Note: IBM ISS strongly recommends that you specify a folder on a non-local medium, such as a network or Zip drive.
14. Click **Next**.

    Note: By default, the installation program automatically creates and places an IBM ISS icon in the desktop folder. If you do not want an the IBM ISS icon to be created, clear the check box.
    When the installation is complete, a message appears that indicates the installation was successful.

Installing SiteProtector on a SQL Server cluster that uses Windows authentication

About this task

- Do not use Deployment Manager to install Windows Authentication.
- All systems must be in the same domain and domain accounts must be used.

Procedure

1. Install the SSL certificate on all cluster nodes.

   Note: For more information about installing an SSL certificate, see one of the following Microsoft Web pages:
   - How to enable SSL encryption for SQL Server 2000 (http://support.microsoft.com/?kbid=276553) or with SQL Server 2005 (http://support.microsoft.com/kb/318605/en-us) with Certificate Server
   - How to enable SSL encryption for SQL Server 2000 or 2005 with Microsoft Management Console (http://support.microsoft.com/kb/316898/en-us)
2. Install the packages in the following order:
   a. Event Collector
   b. Application Server
   c. Agent Manager
   d. Console

   Note: For information about installing the individual packages for the SQL Cluster with Windows NT Authentication, see “Installing SiteProtector when using Windows NT authentication” on page 38.

Installing SiteProtector on a 64-bit platform

This topic provides information for installing SiteProtector on a Windows 64-bit or SQL Server 64-bit Enterprise platform.

About this task

- All systems must be in the same domain and domain accounts must be used.
- For a clustered installation, you cannot use implicit trust.

You must install the individual packages in the following order:

1. Site Database
2. Event Collector
3. Application Server
4. Agent Manager
5. Console
6. Other packages, such as the SecurityFusion Module or Event Archiver

Installing SiteProtector on a 64-bit platform that uses SQL authentication

Procedure

1. Install the Site Database from the package.

   Important: Do not use the Deployment Manager. Do not install anything except the database on the computer where the Windows 64-bit or SQL Server 64-bit platform is installed.
2. Install the Event Collector on a separate computer from the package or the Deployment Manager.
3. Open the Deployment Manager on the computer where you want to install the Application Server, Agent Manager, X-Press Update Server, and Console.
4. Click **Install SiteProtector**. The Installation Options page appears.
5. Click **Recommended Installation**. The Choose Recommended Installation Part 1 or 2 page appears.
6. Click **Part 2: Install Application Server, Agent Manager, X-Press Update server, and Console on second computer**. The Prerequisites page appears.
7. Ensure that the prerequisites for the SiteProtector Recommended installation option are installed on the computer, and then click **Next**. The SQL Server Information page appears.
8. Enter the name of the SQL Server where the Site Database is installed, and then click **Next**. The Prepare to Install page appears.
9. Review the information, and then click **Install**. The File Download window appears.
10. Click **Open**, and then click **OK**.

    Note: If security settings prevent you from opening this file, click **Save**, and then run this file locally.
11. Click **Yes** on the Security Warning window to install and run SiteProtector. The SSL certificate window appears.
12. In the **Folder** box, type a location where you want to archive encryption keys, and then click **Next**.

    Note: IBM ISS strongly recommends that you specify a folder on a non-local medium, such as a network or Zip drive.
13. Click **Next**.

    Note: By default, the installation program automatically creates and places an IBM ISS icon in the desktop folder. If you do not want an the IBM ISS icon to be created, clear the check box.
    When the installation is complete, a message appears that indicates the installation was successful.

Installing SiteProtector on a 64-bit platform that uses Windows NT authentication

About this task

Do not use Deployment Manager to install Windows Authentication.

Procedure

Install packages in the following order:

1. Event Collector
2. Application Server
3. Agent Manager
4. Console

Installing SiteProtector when using Windows NT authentication

When you install SiteProtector on a network that uses Windows NT authentication, you must install each component individually; you cannot use the Deployment Manager. You can get the component installation packages from the product DVD or from the Web site.

About this task

You must install the individual packages in the following order:

1. Site Database
2. Event Collector
3. Application Server
4. Agent Manager
5. Console
6. Other packages, such as the SecurityFusion Module or Event Archiver

Installing the Site Database

Before you begin

You need the following information:

- SQL Server name
- Site name

Note: If you plan to use Windows Domain Accounts to access the Site Database, you must configure the SQL Server and SQL Agent services to run as a Domain account with adequate rights to run SQL Server. For exact requirements, see the documentation for SQL Server.

Procedure

1. Download the component package from the Download Center or find the package on the SiteProtector Installation DVD.
2. Run the program file for the component.
3. Follow the instructions on the screens to complete the installation.

   Note: When you install the Event Collector, the Application Server, and the Agent Manager, you must supply the authentication credentials for a Windows NT user. Include the domain name with the user name. For example: SP_domain\SP_User_Name

Installing the Event Collector

Before you begin

You need the following information:

- SQL Server name
- Authentication credentials for a Windows NT user with permissions to run services
- Application Server name
- Any additional user names of Public Key Administrators for the server

You also must have the SiteProtector JRE installed before you install the Event Collector.

Procedure

1. Download the component package from the Download Center or find the package on the SiteProtector Installation DVD.
2. Run the program file for the component.
3. Follow the instructions on the screens to complete the installation.

   Note: When you install the Event Collector, the Application Server, and the Agent Manager, you must supply the authentication credentials for a Windows NT user. Include the domain name with the user name. For example: SP_domain\SP_User_Name

Installing the Application Server

Before you begin

You need the following information:

- SQL Server name
- Authentication credentials for a Windows NT user with permissions to run services
- Agent Manager location
- Agent Manager authentication account name and password

  Note: This creates an account on your X-Press Update server to interact with the Agent Manager.
- (Optional) SiteProtector group name
- Proxy information for the Internet
- Proxy information for the Agent Manager

You also must have SiteProtector JRE installed before you install the Event Collector.

Procedure

1. Download the component package from the Download Center or find the package on the SiteProtector Installation DVD.
2. Run the program file for the component.
3. Follow the instructions on the screens to complete the installation.

   Note: When you install the Event Collector, the Application Server, and the Agent Manager, you must supply the authentication credentials for a Windows NT user. Include the domain name with the user name. For example: SP_domain\SP_User_Name

Installing the Agent Manager

Before you begin

You need the following information:

- SQL Server name
- Authentication credentials for a Windows NT user with permissions to run services
- Application Server name
- Any additional Public Key Administrators user names for the server

You also must have SiteProtector JRE installed before you install the Event Collector.

Procedure

1. Download the component package from the Download Center or find the package on the SiteProtector Installation DVD.
2. Run the program file for the component.
3. Follow the instructions on the screens to complete the installation.

   Note: When you install the Event Collector, the Application Server, and the Agent Manager, you must supply the authentication credentials for a Windows NT user. Include the domain name with the user name. For example: SP_domain\SP_User_Name

Installing the Console

Before you begin

You need the following information:

- (Optional) URL for the Deployment Manager

Procedure

1. Download the component package from the Download Center or find the package on the SiteProtector Installation DVD.
2. Run the program file for the component.
3. Follow the instructions on the screens to complete the installation.

   Note: When you install the Event Collector, the Application Server, and the Agent Manager, you must supply the authentication credentials for a Windows NT user. Include the domain name with the user name. For example: SP_domain\SP_User_Name

Chapter 5. Installing additional components

Additional component overview

The following figure shows the dependencies among the components. Additional components installed after the initial installation are represented with dashed lines in the following figure:

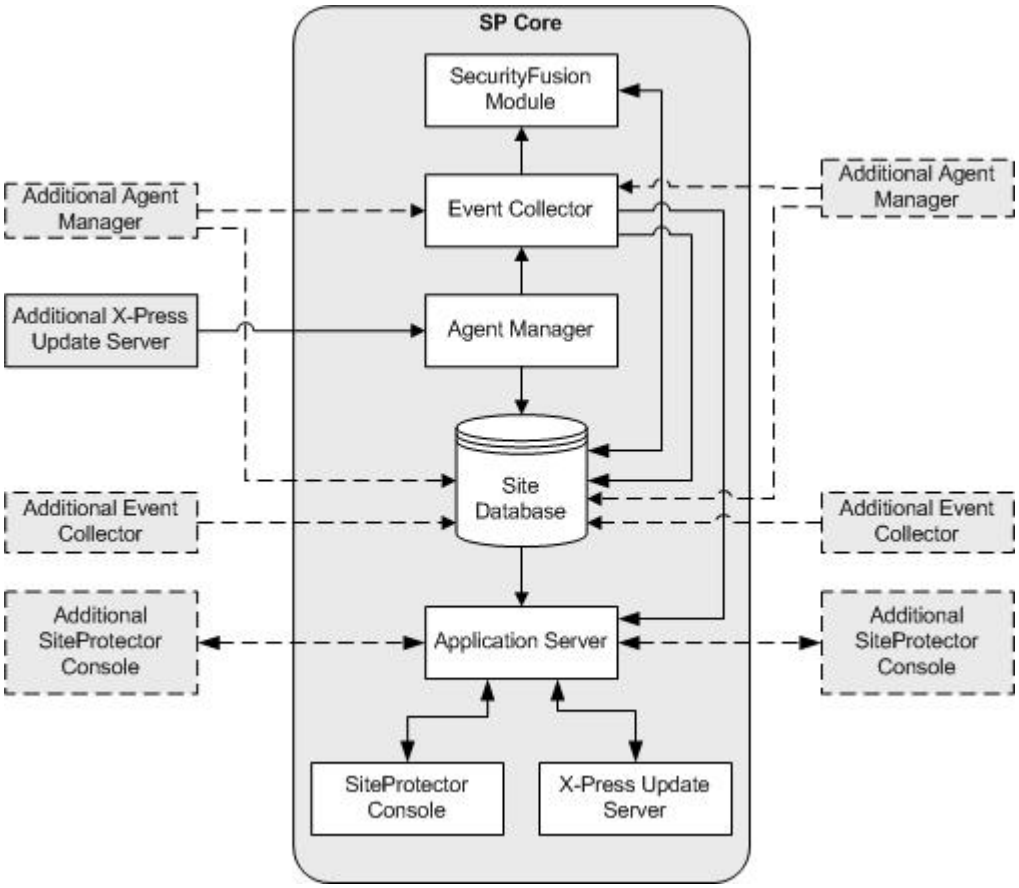


Figure 2. SiteProtector components and flow of events

The following table provides a list of additional components that you might want to install and briefly describes why you might want to install them.

Component	Reason to Install Additional
Agent Manager	• Provide scaling for a large number of agents • Network is partitioned into different geographical locations
Console	Provide multiple users their own Console for monitoring SiteProtector.
Event Collector	Support more agents than you can with your current Event Collector(s). One Event Collector is installed with the Express and Recommended options

© Copyright IBM Corp. 1994, 2009

Component	Reason to Install Additional
Event Viewer	Monitor events on a computer that does not have any other SiteProtector components installed on it.
Event Archiver	Store event data and improve performance by reducing the number of events the Site Database must store.
X-Press Update Server	Cluster X-Press Update Servers to improve performance and provide fail over.

Installing an additional Console

After installing SiteProtector, you might want to install additional SiteProtector Consoles. This enables multiple users to monitor SiteProtector remotely. When you install an additional SiteProtector Console, an additional Event Viewer also is automatically installed.

Procedure

1. Access the Deployment Manager. The Deployment Manager Main Menu appears.
2. Click **Install Additional SiteProtector Console**. The Prerequisites page appears.
3. Ensure that the prerequisites for the SiteProtector Additional SiteProtector Console installation option are installed on your computer, and then click **Next**. The Prepare to Install page appears.
4. Review the information, and then click **Install**. The File Download window appears.
5. Click **Open**.

   Note: If security settings prevent you from opening this file, click Save, and then run this file locally. The Results window appears. When the installation is complete, a summary appears, indicating that the installation was successful. The Additional SiteProtector Console Installation Complete page appears.

Installing an additional Event Collector

Consider installing an additional Event Collector to support additional agents in your environment. After you install an additional Event Collector, you need to redirect agents to it.

Procedure

1. Access the Deployment Manager. The Deployment Manager Main Menu appears.
2. Click **Install SiteProtector**. The Installation Options page appears.
3. Click **Additional Event Collector Installation**. The Prerequisites page appears.
4. Ensure that the prerequisites for the additional SiteProtector Console installation are installed on your computer, and then click **Next**. The SQL Server Information page appears.
5. Enter the name of the SQL Server where the Site Database was installed and the name of the computer where the Application Server is, or will be, installed, and then click **Next**. The Prepare to Install page appears.
6. Review the information, and then click **Install**. The File Download window appears.
7. Click **Open**, and then click **OK**.

   Note: If security settings prevent you from opening this file, click Save, and then run this file locally. The Download Complete dialog appears.
8. Click **Yes** on the Security Warning window to install and run SiteProtector. When the installation is complete, a summary appears, indicating that the installation was successful. The Additional Event Collector Installation Complete page appears.
9. Redirect agents to Event Controllers:

a. Select the agent.
b. Select **Action → Configure Agents → Assign Event Collector**. The Assign Event Collector window appears.
c. Select the Event Collector, and then click **OK**.

Installing an additional Agent Manager

Consider installing an additional Agent Manager if your environment either contains a large number of agents or if your environment is partitioned into different geographic locations. Each instance of Agent Manager must be installed on a separate system.

About this task

If your environment uses Network Address Translation (NAT), consider assigning a custom IP address to the Agent Manager when the installation program prompts you to enter an IP address. You must select the option that disables the list of IP addresses that are currently assigned to the network interface card (NIC), and then type the IP address in the **Custom IP address** field.

Procedure

1. Access the Deployment Manager. The Deployment Manager Main Menu appears.
2. Click **Install SiteProtector**. The Installation Options page appears.
3. Click **Additional Agent Manager Installation**. The Prerequisites page appears.
4. Ensure that the prerequisites for the Agent Manager installation option are installed on your computer, and then click **Next**. The SQL Server Information page appears.
5. Enter the name of the SQL Server where the Site Database was installed and the name of the computer where the Application Server is, or will be, installed, and then click **Next**. The Prepare to Install page appears.
6. Review the information, and then click **Install**. The File Download window appears.
7. Click **Open**, and then click **OK**.

   Note: If security settings prevent you from opening this file, click Save, and then run this file locally. The Download Complete window appears.
8. Click **Yes** on the Security Warning window to install and run SiteProtector. When the installation is complete, a summary appears, indicating that the installation was successful. The Additional Agent Manager Installation Complete page appears.

Installing an additional Event Viewer

You can install an Event Viewer on a system without other SiteProtector components installed, if you can connect to another Event Logger. This enables near real-time access to security event information. (The express and recommended installation options automatically install an Event Viewer on the same system as the Console.)

Procedure

1. Access the Deployment Manager. The Deployment Manager Main Menu appears.
2. Click **Install Additional SiteProtector Event Viewer**. The Prerequisites page appears.
3. Ensure that the prerequisites for the additional Event Viewer installation option are installed on your computer, and then click **Next**. The Prepare to Install page appears.
4. Review the information, and then click **Install**. The File Download window appears.
5. Click **Open**.

Note: If security settings prevent you from opening this file, click **Save**, and then run this file locally. When the installation is complete, a summary appears, indicating that the installation was successful. The Stand-alone Event Viewer Installation Complete page appears.

Installing the Event Archiver

To archive event data and improve database performance, you can install the Event Archiver. This component reduces the number of events that the Site Database must store. (The Event Archiver is not included in all SiteProtector pricing plans.)

Before you begin

You need the following information:

- Host name or IP address of the system where Agent Manager is installed
- Application Server name
- (Optional) Account name and password for Agent Manager
- (Optional) SiteProtector group name

Procedure

1. Download the Event Archiver package.
2. Run the program file.
3. Review the terms of the license agreement, and then click **I Accept**.
4. Follow the instructions on the screen to complete the installation.

Chapter 6. Troubleshooting installation problems

Troubleshooting an unsuccessful recommended installation

About this task

Tthe process of fixing an unsuccessful installation is easier to understand if you know how the SiteProtector recommended installation works:

- The installation program only installs components that are not already installed on the system.
- If the installation of the Site Database fails, the installation program does not install any other components.
- If the installation of a component other than the Site Database fails, the installation program continues to install the other selected components.

To fix an unsuccessful Recommended installation, you must reinstall the components:

- For the Site Database, uninstall each SiteProtector component (except for the Deployment Manager), and then reinstall them.

  CAUTION:
  If you reinstall only the Site Database, SiteProtector does not return to its pre-installation state.
- For each component except the Site Database, run the installation program for that component again.
- If the installation of multiple components failed, be sure to reinstall the components in the correct order.

Installation problems

This section contains information about common installation problems and how to solve them.

Deployment Manager Not Found messages are displayed

The menu frames for the Deployment Manager are visible, but the pages display “Not Found” messages. This can happen when the SiteProtector Web service is running, but the SiteProtector Application Server service is stopped on the computer where the Deployment Manager is installed.

Start the SiteProtector Application Server service on the computer where the Deployment Manager is installed.

issApp login already exists

While installing the Application Server, an error states that the Application Server login issApp already exists, and then the installation process is terminated.

Problem

This typically occurs when you attempt to install the Application Server over an unsuccessful uninstallation. If the Application Server service or Sensor Controller service cannot be stopped during the uninstallation process, the issApp login is still in use and cannot be deleted from the Site Database.

Solution

1. Make sure both services (or applications, if running as such) are stopped.
2. Use SQL Server 2005 Management Studio or SQL Server 2008 Management Studio to manually delete the existing issApp login, which is located in the `/Security/Logins` folder for the Site Database.

© Copyright IBM Corp. 1994, 2009

Event Collector login cannot be deleted

While uninstalling the event collector, an error states that the `EventCollector_<machine>` login cannot be deleted because the service is running, and then the uninstallation process is terminated.

Perform one of the following tasks:

- If you are uninstalling the Site Database, uninstall the database, and then repeat the uninstallation process for the Event Collector.
- If you are not uninstalling the Site Database, stop the issDaemon service, and then repeat the Event Collector uninstallation process. If the uninstallation process proceeds, but you are warned that the login still exists, use the SQL Server 2005 Management Studio or the SQL Server 2008 Management Studio to manually delete the existing **EventCollector_<computer>** login, located in the `/Security/Logins` folder for the Site Database.

Related tasks

"Uninstalling a SiteProtector component" on page 47

You cannot stop the Event Collector

You have removed the Application Server and the Console, but can't stop the Event Collector.

Perform one of the following tasks:

- Remove the Site Database.
- If you aren't removing the Site Database, contact IBM ISS Technical Support for assistance with manually stopping the event collector.

Related tasks

"Uninstalling a SiteProtector component" on page 47

Database is in use

While uninstalling the Site Database, an error states that the database is in use.

Use the SQL Server 2005 Management Studio or SQL Server 2008 Enterprise Manager to manually stop all processes associated with the Site Database, and then uninstall the database.

Related tasks

"Uninstalling a SiteProtector component" on page 47

Chapter 7. Uninstalling

Uninstalling a SiteProtector component

Procedure

1. Click **Start** on the taskbar, and then select **Programs** → **ISS** → **SiteProtector** → **Uninstall SiteProtector**. The Select Components dialog appears.
2. Select the component(s) to remove, and then click **Uninstall**. A message lists the selected component(s).
3. Click **Yes**.
4. If the SQL Login Password window appears, perform one of the following actions:
   - If you have not removed the database, type the SQL log-on user ID and password.
   - If you have not removed the database, or if the component cannot connect to the database for a reason other than an incorrect password, select the **Do not connect to the database** check box.
5. If the program does not remove a component successfully, perform one of the following actions:
   - If this is the first time that you tried to remove the component, go to Step 1 and attempt to uninstall the component again.
   - If you have tried to remove the component more than once, click Yes to view the log file, and then contact IBM ISS Technical Support if you need further assistance.
6. Click **OK**, and then restart your computer.

Related reference

"Event Collector login cannot be deleted" on page 46
While uninstalling the event collector, an error states that the `EventCollector_<machine>` login cannot be deleted because the service is running, and then the uninstallation process is terminated.

"You cannot stop the Event Collector" on page 46
You have removed the Application Server and the Console, but can't stop the Event Collector.

"Database is in use" on page 46
While uninstalling the Site Database, an error states that the database is in use.

Uninstalling SiteProtector

About this task

This topic explains how to remove SiteProtector completely. In most instances, you should remove all SiteProtector components at the same time. The order in which you remove the components is important.

Important: If you remove components through the Windows Control Panel, the uninstallation program automatically removes the components in the correct order.

If you remove components through the Start menu, you must remove them in the following order:

1. SiteProtector Console
2. X-Press Update Server
3. Agent Manager
4. Application Server
5. Event Collector
6. SecurityFusion Module
7. Site Database

© Copyright IBM Corp. 1994, 2009

8. Deployment Manager

If you installed SiteProtector on more than one computer, remove the components in order, computer-by-computer.

Procedure

1. Click **Start** on the taskbar, and then select **Programs** → **ISS** → **SiteProtector** → **Uninstall SiteProtector**.
2. Select all of the installed components, and then click **Uninstall**. The SiteProtector Installation message lists the components you selected to remove.
3. Click **Yes**. A message appears, indicating the success of removing the components.
4. If the program does not remove a component successfully, perform one of the following actions:
   - If this is the first time that you tried to remove the component, repeat Step 1 through Step 3 and attempt to remove the component again.
   - If you have tried to remove the component more than once, then click Yes to view the log file. Contact IBM ISS Technical Support if you need further assistance.
5. Click **OK**, and then restart your computer.

Chapter 8. Securing database communications

Communication between the Site Database and SiteProtector components is not automatically enabled. Because the Site Database contains sensitive information about the security of your network, consider encrypting and authenticating database communication using Secure Socket Layers (SSL).

Encryption protocols

You can use Secure Socket Layers (SSL) to secure communication between the Site Database and the SiteProtector components.

You can use the following encryption protocols to secure database communications:

SSL Secure Sockets Layer (SSL) encryption requires that you purchase certificates.

For more information, search the IBM ISS Knowledgebase for the article "How do I set up SiteProtector to use encryption for database communication?" (Answer ID 1824).

Enabling SSL encryption

You must manually enable SSL on the Event Collector, Application Server, Agent Manager, and SecurityFusion module, if the components are not installed on the same system as the Site Database.

SSL encryption considerations

Note: If you choose to use SSL, you must install the SQL Server's certificate on all the computers that will use SSL to access the Site Database.

Enabling SSL on the Event Collector

Before you begin

You must have the following privileges:

- SiteProtector Administrator privileges
- SA privileges on the Site Database

Procedure

1. On the computer where the Event Collector is installed, locate the ODBC data source for the module.

   Tip: It is named RSNTEvent Collector and is a system DSN.
2. Select the data source, click **Configure**, and then click **Next**.
3. Enter the login information to connect, click **Next**, and then click **Next** again.
4. Select **Use strong encryption for data**, and then click **Finish**.
5. On the summary window, click **Test Data Source** to ensure that everything is working properly.
6. If the test does not work, see the Microsoft article to determine what is wrong.
7. From a Site Protector Console, stop, and then restart the Event Collector.

© Copyright IBM Corp. 1994, 2009

Enabling SSL on the Application Server

Before you begin

You must have the following privileges:

- SiteProtector Administrator privileges
- SA privileges on the Site Database

Procedure

1. On the computer where the Application Server is installed, locate the ODBC data source for the module.

   Tip: It is named IssADReconciler and is a system DSN.
2. Select the data source, click **Configure**, and then click **Next**.
3. Enter the login information to connect, click **Next**, and then click **Next** again.
4. Select **Use strong encryption for data**, and then click **Finish**.
5. On the summary window, click **Test Data Source** to ensure that everything is working properly.
6. If the test does not work, see the Microsoft article to determine what is wrong.
7. From a Site Protector Console, stop, and then restart the ISS Application Server service.

Enabling SSL on the Agent Manager

Before you begin

You must have the following privileges:

- SiteProtector Administrator privileges
- SA privileges on the Site Database

Procedure

1. Locate the installation directory for the Agent Manager, and then open the RSSPDC.INI file in a text editor.
2. Find the property named **dbEncrypt**, and then set its value to "1."
3. Save, and then close the file.
4. From a Site Protector Console, stop, and then restart the Agent Manager.

   Note: If the Agent Manager fails to start because it cannot communicate with the Site Database, the system generates log errors. See the Microsoft article to determine what is wrong.

Enabling SSL on the SecurityFusion module

Before you begin

You must have the following privileges:

- SiteProtector Administrator privileges
- SA privileges on the Site Database

Procedure

1. In the SiteProtector Console, locate the SecurityFusion Module that you want to update.
2. Right-click the sensor, go to the SecurityFusion Module sub-menu, and then select **Edit Properties**. The property editor appears.

3. In the left side tree, select **Advanced Settings**.
4. On the tree, select **Encrypt communications with the RealSecure Site database using SSL**.
   CAUTION:
   See help before turning On.
5. Save the settings, and then close the property editor.
6. From a Site Protector Console, select the SecurityFusion Module to update, and then apply the modified policy to the sensor.

   Note: If the SecurityFusion Module fails to start because it cannot communicate with the Site Database, the system generates log errors. See the Microsoft article to determine what is wrong.

Appendix A. Supported agents and appliances

SiteProtector supports agents and appliances produced by IBM Internet Security Systems. This topic contains a list of supported products, complete with model and version information.

Product	Model	Version
Proventia Network Intrusion Detection System (IDS)	Network Gigabit	7.0
	Network Sensor	7.0
	Proventia A201	All models
	Proventia A604	All models
	Proventia A1204	
	Proventia AX604	
	Proventia AX1204	
Proventia Network IPS	G100	
	G200	
	G400	All models
	G1000	All models
	G1200	All models
	G2000	All models
Proventia Network IPS GX Models	GC1200	
	GX3002	
	GX4002	GX4002-C
	GX4004	GX4004-C
	GX5008	GX5008-C GX5008-CF
	GX5108	GX5108-C GX5108-CF
	GX5208	
	GX6116	

© Copyright IBM Corp. 1994, 2009

Product	Model	Version
Proventia Network Multi- Function Security	M10	
	M10e	
	M30	
	M30e	
	M50	
	M50A	
	M50Ae	
	M50e	
	MX0804	
	MX1004	
	MX3006	
	MX4006	
	MX5008	
	MX5010	
	MX5010A	
	MX5110	
	MX5110A	
Proventia Network Internet Scanner®		7.0 Service Pack 2
Proventia Network Anomaly Detection System	AD5003	
	AD5100	
	AD5200	
	AD5300	
Proventia Mail Security	MS1002	
	MS1002LP	
	MS3004	
	MS3004N	
	MS3004LP	
Proventia Network Enterprise Scanner	ES750	
	ES1500	
Proventia Desktop		8.0, 9.0, 10.0
Proventia Server for Linux		1.0
Proventia Server for Windows		1.0, 2.0
Server Sensor		7.0
Third Party Module		1.0

Appendix B. Technical support contacts

IBM Internet Security Systems (ISS) provides technical support through its Web site and by e-mail or telephone.

The IBM ISS Web site

The IBM Internet Security 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 can call or send an e-mail to the Americas office for help during off-hours.

Contact information

For contact information, go to the IBM Internet Security Systems Contact Technical Support Web page at http://www.ibm.com/services/us/iss/support/.

© Copyright IBM Corp. 1994, 2009

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:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, 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 Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites 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:

© Copyright IBM Corp. 1994, 2009

IBM Corporation
SiteProtector Project Management
C55A/74KB
6303 Barfield Rd.,
Atlanta, GA 30328
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 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 "Copyright and trademark information" at Copyright and trademark information 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

© Copyright IBM Corp. 1994, 2009

Readers' Comments — We'd Like to Hear from You

IBM Internet Security Systems
IBM Proventia Management SiteProtector
Installation Guide
Version 2.0, Service Pack 8.0

We appreciate your comments about this publication. Please comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. The comments you send should pertain to only the information in this manual or product and the way in which the information is presented.

For technical questions and information about products and prices, please contact your IBM branch office, your IBM business partner, or your authorized remarketer.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you. IBM or any other organizations will only use the personal information that you supply to contact you about the issues that you state on this form.

Comments:

Thank you for your support.

Send your comments to the address on the reverse side of this form.

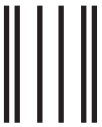
If you would like a response from IBM, please fill in the following information:

Name	Address
Company or Organization	
Phone No.	E-mail address

Readers' Comments — We'd Like to Hear from You

Cut or Fold
Along Line

Fold and Tape **Please do not staple** Fold and Tape



NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

International Business Machines Corporation
ATTN: Dept JP1A
6303 Barfield Road NE
Atlanta, GA
USA 30328-4233

Fold and Tape **Please do not staple** Fold and Tape

Cut or Fold
Along Line

Printed in USA