Installation Guide
Version 2.0, Service Pack 7.0
IBM Proventia® Management SiteProtector™

Installation Guide
Version 2.0, Service Pack 7.0
Trademarks and Disclaimer

IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. ADDME, Ahead of the Threat, BlackICE, Internet Scanner, Proventia, RealSecure, SecurePartner, SecurityFusion, SiteProtector, System Scanner, Virtual Patch, X-Force and X-Press Update are trademarks or registered trademarks of Internet Security Systems, Inc. in the United States, other countries, or both. Internet Security Systems, Inc. is a wholly-owned subsidiary of International Business Machines Corporation.

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

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

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.

Disclaimer: The information contained in this document may change without notice, and may have been altered or changed if you have received it from a source other than IBM Internet Security Systems (IBM ISS). Use of this information constitutes acceptance for use in an “AS IS” condition, without warranties of any kind, and any use of this information is at the user’s own risk. IBM Internet Security Systems disclaims all warranties, either expressed or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall IBM ISS be liable for any damages whatsoever, including direct, indirect, incidental, consequential or special damages, arising from the use or dissemination hereof, even if IBM Internet Security Systems has been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages, so the foregoing limitation may not apply.

Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by IBM Internet Security Systems. The views and opinions of authors expressed herein do not necessarily state or reflect those of IBM Internet Security Systems, and shall not be used for advertising or product endorsement purposes.

Links and addresses to Internet resources are inspected thoroughly prior to release, but the ever-changing nature of the Internet prevents IBM Internet
Security Systems, Inc. from guaranteeing the content or existence of the resource. When possible, the reference contains alternate sites or keywords that could be used to acquire the information by other methods. If you find a broken or inappropriate link, please send an email with the topic name, link, and its behavior to support@iss.net.
## Contents

**Trademarks and Disclaimer**  
iii

**Overview.**  
vii

How to Use SiteProtector Documentation  
viii

Getting Technical Support  
ix

**Chapter 1. Introduction to SiteProtector**  
1

What is SiteProtector?  
2

SiteProtector Architecture  
3

SiteProtector Component Descriptions.  
4

Add-on Components  
6

**Chapter 2. Requirements and Considerations**  
7

Requirements  
8

Locating Installation Programs  
9

Considerations for Running Installation Programs  
10

**Chapter 3. Installation Checklists**  
13

Pre-Installation Checklist  
14

Information Required Checklist  
15

Installing the Express Option from Deployment Manager  
16

Installing the Express Option without the Deployment Manager  
17

Recommended Option Tasks  
18

Post-Installation Tasks.  
19

Advanced Database Platform Tasks  
20

SiteProtector Package Installation Task  
21

**Chapter 4. Securing Third-Party Software**  
23

Security Measures for Microsoft SQL Server  
24

Security Measures for Third-Party Software  
25

Installing the Latest Microsoft Updates  
26

**Chapter 5. Installing SiteProtector**  
29

Installation Options  
30

Guidelines for Selecting Cryptographic Providers and Encryption Key Archives  
31

How to Implement Deployment Scenarios  
32

Installing the Deployment Manager  
34

Downloading the installation program  
35

Starting the Deployment Manager  
35

Installing the Express Option from the Deployment Manager  
36

Enabling MSDE database communication over TCP/IP  
37

Installing the Express option from the Deployment Manager  
37

Installing the Recommended Option  
39

Install the Site Database and the Event Collector  
39

Install the Application Server, Agent Manager, X-Press Update Server, and a Console  
40

Installing the Express Option from the Download Center  
41

Installing the Express Option  
42

Installing SiteProtector on a Clustered SQL Platform  
43

SiteProtector installation on a clustered SQL platform with SQL Authentication  
44

SiteProtector installation on a clustered SQL platform with Windows Authentication  
45

Installing SiteProtector on Microsoft Windows 64-bit, SQL Server 64-bit  
46

SiteProtector installation on a clustered SQL platform with SQL Authentication  
47

SiteProtector installation on a Windows 64-bit or SQL Server 64-bit platform with Windows Authentication  
48

Installing SiteProtector When Using Windows NT Authentication  
49

Installing a component  
51

**Chapter 6. Installing Additional Components**  
53

Component Overview.  
54

Installing an Additional SiteProtector Console  
56

Installing an Additional Event Collector.  
57

Installing an additional Event Collector.  
57

Redirecting agents to Event Collectors  
58

Installing an Additional Agent Manager.  
58

Installing an Agent Manager  
59

Installing an Additional SiteProtector Event Viewer.  
59

Installing the Event Archiver  
60
Overview

Introduction

The SiteProtector Installation Guide provides the information you need to install IBM Proventia Management SiteProtector.

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.
How to Use SiteProtector Documentation

This topic describes documents in the SiteProtector documentation suite.

Related publications

Use the following documents for information about SiteProtector configuration options:

- SiteProtector System Requirements
- SiteProtector Scalability Guidelines
- SiteProtector Supported Agents and Appliances

Additional publications

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

<table>
<thead>
<tr>
<th>Document</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>SiteProtector Configuration Guide</td>
<td>Contains information about configuring, updating, and maintaining SiteProtector</td>
</tr>
<tr>
<td>SiteProtector Policies and Responses</td>
<td>Contains information about configuring policies and responses, including Central Responses</td>
</tr>
<tr>
<td>SiteProtector Help</td>
<td>Contains all the procedures that you need to use SiteProtector, including advanced procedures that may not be available in a printed user document</td>
</tr>
</tbody>
</table>

Locating the publications

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](http://www.iss.net/support/documentation)
- The Deployment Manager

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

Licensing agreement

For licensing information on IBM Internet Security System products, [download the IBM Licensing Agreement from](http://www-935.ibm.com/services/us/iss/html/contracts_landing.html)
Getting Technical Support

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

The IBM ISS Web site


Hours of support

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

<table>
<thead>
<tr>
<th>Location</th>
<th>Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Americas</td>
<td>24 hours a day</td>
</tr>
<tr>
<td>All other locations</td>
<td>Monday through Friday, 9:00 A.M. to 6:00 P.M. during their local time, excluding IBM ISS published holidays</td>
</tr>
</tbody>
</table>

**Note:** If your local support office is located outside the Americas, you may call or send an email to the Americas office for help during off-hours.

Contact information

Chapter 1. Introduction to SiteProtector

This chapter introduces SiteProtector, SiteProtector architecture, and the components and agents that work with SiteProtector.

Terms to know

The following table describes the terms used for security products in this document:

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>agent</td>
<td>The generic term for all appliances; scanners; and network, server and desktop sensors</td>
</tr>
<tr>
<td>appliance</td>
<td>An inline security device on a network or gateway</td>
</tr>
<tr>
<td></td>
<td>Depending on the type of appliance, it can provide any combination of intrusion detection and prevention, antivirus, antispam, virtual private networking (VPN), Web filtering, and firewall functions.</td>
</tr>
<tr>
<td>scanner</td>
<td>An agent that scans assets for vulnerabilities and other security risks</td>
</tr>
<tr>
<td>sensor</td>
<td>An agent that monitors network traffic on the network and on servers to identify and, in some cases, stop attacks</td>
</tr>
</tbody>
</table>

Topics

“What is SiteProtector?” on page 2
“SiteProtector Architecture” on page 3
“SiteProtector Component Descriptions” on page 4
“Add-on Components” on page 6
What is SiteProtector?

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.

SiteProtector components and agents

The components and agents in a SiteProtector are categorized as follows:

<table>
<thead>
<tr>
<th>Component Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required and optional</td>
<td>Provide base functionality to accept, monitor, and analyze network events. Depending on your Site requirements, you may need to install more than one of some components.</td>
</tr>
<tr>
<td>Add-on components (purchased separately)</td>
<td>Provide additional security and management functions.</td>
</tr>
<tr>
<td>Agents (purchased separately)</td>
<td>Provide vulnerability scanning, intrusion detection and prevention, and integrated security.</td>
</tr>
</tbody>
</table>
SiteProtector Architecture

You can use one or more computers to install SiteProtector.

- If you use more than one computer, perform the Recommended installation.
- If you use one computer, perform the Express installation.

Illustration on three computers

The following figure shows the components of SiteProtector when SiteProtector is installed on three computers. This is the recommended installation:

Figure 1. Components in a typical Site
**SiteProtector Component Descriptions**

This topic describes the purpose of the SiteProtector components.

**Descriptions**

The following table describes the purpose of the SiteProtector components:

<table>
<thead>
<tr>
<th>SiteProtector Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Manager</td>
<td>The Agent Manager manages the command and control activities of the Desktop Protection agents and IBM ISS appliance. The Agent Manager also facilitates data transfer from agents to the Event Collector.</td>
</tr>
<tr>
<td>Console</td>
<td>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.</td>
</tr>
<tr>
<td>Databridges (optional)</td>
<td>Databridges accept data from earlier versions of agents and send them to the Event Collector in the proper format. Note: Only System Scanner Databridge is supported.</td>
</tr>
<tr>
<td>Deployment Manager (optional)</td>
<td>The Deployment Manager is a Web server that lets you install any of the SiteProtector components and agents on computers on your network.</td>
</tr>
<tr>
<td>Event Collector</td>
<td>The Event Collector manages real-time events from sensors and vulnerability data from scanners.</td>
</tr>
<tr>
<td>Event Viewer (optional)</td>
<td>The SiteProtector Event Viewer receives unprocessed events from the Event Collector to provide near real-time access to security data for troubleshooting.</td>
</tr>
<tr>
<td>Site Database</td>
<td>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).</td>
</tr>
<tr>
<td>SiteProtector Component</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SP Core</td>
<td>The SP core includes the following components:</td>
</tr>
<tr>
<td></td>
<td>• The Application Server, which enables communication between the SiteProtector Console and the Site Database.</td>
</tr>
<tr>
<td></td>
<td>• The agent controller, which manages the command and control activities of agents, such as the command to start or to stop collecting events.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• SiteProtector Web Access, which is a read-only interface that provides easy access to SiteProtector for monitoring SiteProtector Event assets and security events.</td>
</tr>
<tr>
<td>X-Press Update Server</td>
<td>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.</td>
</tr>
<tr>
<td>Event Archiver</td>
<td>The Event Archiver stores event data and improves performance by reducing the number of events the Site Database must store.</td>
</tr>
</tbody>
</table>
Add-on Components

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

SiteProtector SecurityFusion Module

The SiteProtector SecurityFusion Module greatly increases your ability to quickly identify and respond to critical threats on your Site. Using advanced correlation and analysis techniques, the Module identifies both high impact events and patterns of events that may indicate attacks.

Impact analysis: The Module correlates intrusion detection events with vulnerability assessment and operating system data and immediately estimates the impact of events.

Attack pattern recognition: The Module recognizes patterns of events that may indicate specific types of attacks, such as unauthorized scans, break-in attempts, and activity from a compromised host.

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. Requirements and Considerations

This chapter gives requirements and important considerations about the installation process.

Topics

“Requirements” on page 8
“Locating Installation Programs” on page 9
“Considerations for Running Installation Programs” on page 10
Requirements

This topic lists the requirements for installing SiteProtector.

System requirements

The SiteProtector System Requirements document for SiteProtector is available from the IBM ISS Web site at http://documents.iss.net/literature/SiteProtector/SPSystemRequirements20SP7.pdf.

Important: Download the system requirements to make sure you have the latest system requirements for each configuration option.

Other computer requirements

In addition to meeting the system requirements, you must also do the following:
• 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 Microsoft Windows 2000 Server and Microsoft Windows Server 2003 computers that have been set up as primary or backup domain controllers.

Enabling the TCP/IP protocol

You must enable the TCP/IP protocol on the Site Database if the Site Database uses MSDE.

Reference: See “Installing the Express Option from the Deployment Manager” on page 36.

Express installation domain names

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

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

Standalone programs

Standalone programs let you install SiteProtector components separately from the Deployment Manager. Because these files are not installed from a central location, you may have to enter additional information if you use them.

Locations of installation programs

You can access installation programs from the following locations:

<table>
<thead>
<tr>
<th>Source</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment Manager</td>
<td>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 fully utilize the Deployment Manager, you must install it on your network.</td>
</tr>
<tr>
<td>IBM ISS product DVD</td>
<td>The IBM ISS product DVD contains standalone installation programs and includes the Deployment Manager.</td>
</tr>
<tr>
<td>IBM ISS Download Center</td>
<td>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: <a href="http://www.iss.net/download/">http://www.iss.net/download/</a></td>
</tr>
</tbody>
</table>
Considerations for Running Installation Programs

The installation programs may require that you install certain software or perform tasks in a certain way. This topic provides lists of items you should consider before you install SiteProtector.

Encryption key archives

Many installation and uninstallation programs give you the option to archive private cryptographic keys. The archiving option only applies to encryption keys that are used by Agent Managers and standalone X-Press Update Servers. IBM ISS recommends that you archive these keys in a non-local location, preferably on a removable medium. If you do not archive encryption keys, these certificates are deleted if you uninstall the components that are using these keys. Encryption key archives can simplify disaster recovery if your server fails.

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

If you are running Microsoft Windows Server 2003:

- Disable the hardened download option – By default, Microsoft Windows Server 2003 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 2003 Terminal Server**

Due to an installation limitation with the Windows 2003 Terminal Server, you may have 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.

**SQL Server Cluster**

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

**Microsoft Windows 64-bit, SQL Server 64-bit**

The SiteProtector Database is the only SiteProtector component that you can install on a computer using Microsoft Windows 64-bit or SQL Server 64-bit.

**Information generated by the installation programs**

The installation programs generate the following information about the installation process. Use this information for troubleshooting or when communicating with IBM ISS Customer Support:

<table>
<thead>
<tr>
<th>Information Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log files</td>
<td>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.</td>
</tr>
<tr>
<td>Deployment Manager Identification number</td>
<td>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. <strong>Note:</strong> To view this identification number, click Cancel to stop the installation program. The identification number then appears on the main page.</td>
</tr>
</tbody>
</table>
Chapter 3. 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.

**Topics**

- “Pre-Installation Checklist” on page 14
- “Information Required Checklist” on page 15
- “Installing the Express Option from Deployment Manager” on page 16
- “Installing the Express Option without the Deployment Manager” on page 17
- “Recommended Option Tasks” on page 18
- “Post-Installation Tasks” on page 19
- “Advanced Database Platform Tasks” on page 20
- “SiteProtector Package Installation Task” on page 21
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:

<table>
<thead>
<tr>
<th>Task</th>
</tr>
</thead>
</table>
| ✔️ 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 email to mailto://licenses@iss.net |
| ✔️ Verify that the computers you will be using meet the system requirements in the [SiteProtector System Requirements document](http://documents.iss.net/literature/SiteProtector/SPSystemRequirements20SP7.pdf) |
| ✔️ 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.  
  The following information can assist you in making this decision:  
  • [SiteProtector System Requirements](http://documents.iss.net/literature/SiteProtector/SPSystemRequirements20SP7.pdf)  
  • [SiteProtector Scalability Guidelines](http://documents.iss.net/literature/SiteProtector/SPScalabilityGuide20SP7.pdf) |
| ✔️ 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](http://documents.iss.net/literature/SiteProtector/SPSystemRequirements20SP7.pdf) for a list of required third-party software. |
| ✔️ Harden Windows and SQL Server software.  
  See the following topics:  
  • "Security Measures for Microsoft SQL Server" on page 24  
  • "Security Measures for Third-Party Software" on page 25 |
| ✔️ 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](https://www.iss.net)  
  • [http://www.iss.net](http://www.iss.net) |
Task

- 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 may 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 may 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:

<table>
<thead>
<tr>
<th>Information for the Installation Programs</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐ A unique name for your Site or components to distinguish them in a multi-Site or multi-component environment.</td>
</tr>
<tr>
<td>☐ The IP address or fully qualified domain name for each computer where SiteProtector is installed.</td>
</tr>
<tr>
<td>☐ The fully qualified SQL Server Name for the Site Database computer in one of the following formats:</td>
</tr>
<tr>
<td>• ComputerName</td>
</tr>
<tr>
<td>• ComputerName\NamedInstance</td>
</tr>
<tr>
<td>• ComputerName.DomainName.com</td>
</tr>
<tr>
<td>• ComputerName.DomainName.com\NamedInstance</td>
</tr>
<tr>
<td>☐ The computer drives where you want to install SiteProtector components if more than one drive is available.</td>
</tr>
<tr>
<td>☐ The URL of the Deployment Manager if you are installing from a Deployment Manager.</td>
</tr>
<tr>
<td>☐ 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.</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1    | Download the Deployment Manager installation file(s) from one of the following locations:  
• IBM ISS Download Center  
• IBM ISS product DVD |
| 2    | Install the Deployment Manager.  
See [“Installing the Deployment Manager” on page 34](#). 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.  
See [“Installing the Express Option from the Deployment Manager” on page 36](#).  
Verify that the TCP/IP protocol is enabled on the computer where you are installing SiteProtector. |
| 4    | Install optional modules.  
• See [“Installing the Event Archiver” on page 60](#).  
• For information about installing and configuring SecurityFusion Module, see the *SiteProtector SecurityFusion Module 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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Download the Express option from the IBM ISS Download Center or the IBM ISS product DVD.</td>
</tr>
</tbody>
</table>
| 2    | Install SiteProtector using the Express option.  

See “Installing the Express Option from the Download Center” on page 41. |
| 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 installing the optional modules:  
• See “Installing the Event Archiver” on page 60.  
• For information about installing and configuring SecurityFusion Module, see the SiteProtector SecurityFusion Module 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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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.  
   See “Installing the Deployment Manager” on page 34.  
   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.  
   See “Installing the Recommended Option” on page 39. |
| 4    | Install the Application Server, SiteProtector Core, Agent Manager, XPress Update Server, and the SiteProtector Console on the other computer. |
| 5    | Install optional X-Press Update Servers.  
   See “Install the Application Server, Agent Manager, X-Press Update Server, and a Console” in “Installing the Recommended Option” on page 39.  
   Install optional additional components.  
   - See “Installing an Additional SiteProtector Console” on page 56.  
   - See “Installing an Additional Event Collector” on page 57.  
   - “Installing an Additional Agent Manager” on page 58.  
   - See “Installing an Additional SiteProtector Event Viewer” on page 59. |
| 6    | Install optional modules.  
   - See “Installing the Event Archiver” on page 60.  
   - For information about configuring Event Archiver, see the SiteProtector Configuration Guide.  
   - For information about installing and configuring SecurityFusion Module, see the SiteProtector SecurityFusion Module 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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Access the package installation files from the IBM ISS product DVD.</td>
</tr>
<tr>
<td>2</td>
<td>Install the Site Database.</td>
</tr>
<tr>
<td></td>
<td>See “Installing the Recommended Option” on page 39.</td>
</tr>
<tr>
<td>3</td>
<td>Install the Event Collector, Agent Manager, and the SiteProtector Console.</td>
</tr>
<tr>
<td></td>
<td>See “Installing the Recommended Option” on page 39.</td>
</tr>
<tr>
<td>4</td>
<td>Install the Application Server, Agent Manager, and Console.</td>
</tr>
<tr>
<td>5</td>
<td>Install optional additional components.</td>
</tr>
<tr>
<td></td>
<td>• See “Installing the Deployment Manager” on page 34.</td>
</tr>
<tr>
<td></td>
<td>• See “Install the Application Server, Agent Manager, X-Press Update Server, and a Console” in “Installing the Recommended Option” on page 39.</td>
</tr>
<tr>
<td></td>
<td>• See “Installing an Additional Event Collector” on page 57.</td>
</tr>
<tr>
<td></td>
<td>• See “Installing an Additional Agent Manager” on page 58.</td>
</tr>
<tr>
<td></td>
<td>• See “Installing an Additional SiteProtector Event Viewer” on page 59.</td>
</tr>
<tr>
<td>6</td>
<td>For information about installing the optional modules:</td>
</tr>
<tr>
<td></td>
<td>• See “Installing the Event Archiver” on page 60.</td>
</tr>
<tr>
<td></td>
<td>• For information about installing and configuring SecurityFusion Module, see the SiteProtector SecurityFusion Module Guide.</td>
</tr>
<tr>
<td></td>
<td>• For information about installing and configuring Third Party Modules, see the SiteProtector Third Party Module Guide.</td>
</tr>
</tbody>
</table>
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 NT authentication to the SQL Server Database
- Install in a SQL Server cluster environment
- Install the site database on 64-bit SQL Server
- 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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Access the package installation files from the IBM ISS product DVD.</td>
</tr>
</tbody>
</table>
| 2    | Install the Site Database.  
**See** [“Installing the Recommended Option” on page 39](#) |
| 3    | Install packages in the following order:  
1. Event Collector  
2. Application Server  
3. Agent Manager  
4. Console |
| 4    | For information about installing the optional modules:  
• See [“Installing the Event Archiver” on page 60](#)  
• For information about installing and configuring SecurityFusion Module, see the SiteProtector SecurityFusion Module Guide.  
• For information about installing and configuring Third Party Modules, see the SiteProtector Third Party Module Guide. |
Chapter 4. Securing Third-Party Software

Software that communicates over a network or over the Internet is vulnerable to security risks. Therefore, IBM ISS recommends that you harden your security and implement measures that help ensure that your security is maintained before you install SiteProtector. This chapter provides guidelines for hardening your security.

Important: This guide assumes that you have a new operating system installation, have not modified the security settings for your operating system, and have not previously installed IBM ISS software components.

Before you continue

Use the information from Chapter 2, “Requirements and Considerations,” on page 7 and Chapter 3, “Installation Checklists,” on page 13 to make sure that you choose the correct installation procedures to meet your Site requirements.

Topics

“Security Measures for Microsoft SQL Server” on page 24

“Security Measures for Third-Party Software” on page 25

“Installing the Latest Microsoft Updates” on page 26
Security Measures for Microsoft SQL Server

Microsoft SQL Server software is a powerful database query application that helps organize and maintain up-to-date event information in SiteProtector. However, SQL Server can make your computer vulnerable to certain types of attacks. Use this topic to improve the security of SiteProtector components that run SQL Server so that you can prevent these types of attacks.

Requirement

You must install SQL Server software on the Site Database.

Securing components that run SQL server

The following table provides recommendations for securing your system from SQL Server vulnerabilities:

<table>
<thead>
<tr>
<th>Security Measures Checklist</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐ Apply Microsoft’s latest patches for Microsoft Windows 2000 Server and Microsoft Windows Server 2003. You can download the patch from the Microsoft Web site:</td>
</tr>
<tr>
<td>☐ Harden the security of SQL Server. IBM ISS recommends that you harden SQL Server security.</td>
</tr>
</tbody>
</table>
Security Measures for Third-Party Software

This topic contains guidelines and procedures for hardening security on SiteProtector components.

Checklist

You can secure third-party software in the following ways:

<table>
<thead>
<tr>
<th>Security Measures Checklist</th>
</tr>
</thead>
<tbody>
<tr>
<td>☑ Install service packs and hotfixes.</td>
</tr>
<tr>
<td>Reference: &quot;Installing the Latest Microsoft Updates&quot; on page 26.</td>
</tr>
<tr>
<td>☐ Enable a screen saver with password authorization to prevent unauthorized use of SiteProtector.</td>
</tr>
<tr>
<td>☐ Secure Internet Explorer by installing the latest version of Microsoft Internet Explorer and all related patches on all computers on which SiteProtector is installed.</td>
</tr>
<tr>
<td>☐ Verify that additional applications are not installed on SiteProtector servers.</td>
</tr>
<tr>
<td>☑ Secure SiteProtector passwords.</td>
</tr>
</tbody>
</table>

Guidelines for 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 computer when it is unattended, to prevent unauthorized access.

Limit applications on a SiteProtector server

Do not install additional software applications on devices that run SiteProtector components unless it is absolutely necessary. Additional applications can introduce security risks.

Secure passwords

SiteProtector automatically generate passwords for the Event Collector, Agent Manager, and Application Server.
Installing the Latest Microsoft Updates

To correct potential security flaws, IBM ISS recommends that you update Microsoft Windows 2000 Server and Microsoft Windows Server 2003 with the latest service packs, hotfixes, and security patches. When you apply updates, Microsoft recommends that you follow best practices, such as quality assurance testing and performing change control. Refer to the Microsoft Web site for more information about these practices and how they apply to your environment.

Types of Microsoft updates

The following table describes Microsoft updates:

<table>
<thead>
<tr>
<th>Update Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service pack</td>
<td>Cumulative updates that correct known problems and provide tools, drivers, and updates that extend product functionality.</td>
</tr>
<tr>
<td>Hotfix</td>
<td>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.</td>
</tr>
<tr>
<td>Security patches</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Important**: Before you install SiteProtector, you must update Microsoft Windows 2000 Server and Microsoft Windows Server 2003 to meet the Service Pack level specified in the SiteProtector System Requirements document.

**Downloading updates directly to your computer**

Download the latest Microsoft patches from the Microsoft Web site [http://www.microsoft.com](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.
Using Windows utilities to manage updates

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:

<table>
<thead>
<tr>
<th>Utility</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hfnetcheck</td>
<td>Identifies any hotfixes that have not been applied to your specific computer</td>
</tr>
<tr>
<td></td>
<td>Tip: Run this utility in verbose mode (-v suffix).</td>
</tr>
<tr>
<td>Qchain</td>
<td>Verifies that hotfixes were installed in the correct order</td>
</tr>
<tr>
<td></td>
<td>Tip: Run Qchain with the -z suffix.</td>
</tr>
<tr>
<td>Qfecheck</td>
<td>Verifies that hotfixes were installed properly</td>
</tr>
<tr>
<td></td>
<td>Tip: Run this utility in verbose mode (-v suffix).</td>
</tr>
</tbody>
</table>
Chapter 5. Installing SiteProtector

This chapter describes the options and procedures for installing SiteProtector.

Before you continue

Review Chapter 2, “Requirements and Considerations,” on page 7 and Chapter 3, “Installation Checklists,” on page 13 to make sure that you choose the correct installation procedures to meet your Site requirements.

Topics

“Installation Options” on page 30

“Guidelines for Selecting Cryptographic Providers and Encryption Key Archives” on page 31

“How to Implement Deployment Scenarios” on page 32

“Installing the Deployment Manager” on page 34

“Installing the Express Option from the Deployment Manager” on page 36

“Installing the Recommended Option” on page 39

“Installing the Express Option from the Download Center” on page 41

“Installing SiteProtector on a Clustered SQL Platform” on page 43

“Installing SiteProtector When Using Windows NT Authentication” on page 49
**Installation Options**

SiteProtector installation options are suited for many environments. This topic describes the SiteProtector installation options.

**Description of the installation options**

The following table describes the SiteProtector installation options:

<table>
<thead>
<tr>
<th>Installation Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Express</td>
<td>Installs a streamlined version of SiteProtector on one computer. It includes an option for installing an MSDE database. The Express option is intended for small environments and for evaluation purposes. <strong>Note:</strong> The TCP/IP protocol must be enabled on the MSDE or SQL Server instance.</td>
</tr>
<tr>
<td>Recommended</td>
<td>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.</td>
</tr>
<tr>
<td>Clustered SQL</td>
<td>Installs SiteProtector for Clustered SQL</td>
</tr>
<tr>
<td>Windows Authentication</td>
<td>Installs SiteProtector using Windows Authentication</td>
</tr>
<tr>
<td>64-bit SQL</td>
<td>Install the site database on a 64-bit SQL Server database</td>
</tr>
</tbody>
</table>
Guidelines for Selecting Cryptographic Providers and Encryption Key Archives

Some installation programs require that you select cryptographic providers and encryption key archives. This topic provides background information and guidelines for selecting these options.

**Important:** SiteProtector does not encrypt or authenticate database communication. You must secure this communication manually. See Chapter 8, “Securing Database Communication,” on page 71.

**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.

**Guidelines for archiving encryption keys**

Certain installation programs give you the option to specify a directory, preferably on a removable medium, where a server’s private cryptographic keys are archived. If you do not archive encryption keys, and you uninstall the server, then you may have to redistribute certificates to clients that communicate with this server. This only applies if you are requiring your clients to validate certificates from this server (“Explicit Trust” or First “Time Trust” options). 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.

**Installation programs that archive encryption keys**

You can archive encryption keys for the following components. The installation programs prompt you to specify an archive directory anytime these components are installed or uninstalled:

- Agent Manager
- X-Press Update Server

**Note:** You cannot archive encryption keys for integrated X-Press Update Servers.
How to Implement Deployment Scenarios

The SiteProtector Scalability Guidelines document recommends several deployment scenarios to assist you in choosing the appropriate SiteProtector configuration. This topic provides guidelines for implementing these deployment scenarios.

Recommended and additional component installations

To implement a deployment scenario, you must use a combination of the installation procedures in this guide.

Important: Depending on your environment, you may be required to perform additional procedures.

How to implement deployment scenarios

The following table describes the deployment scenarios for small, medium, and large networks and the corresponding installation options for each of them in the Deployment Manager. Use this table to assist you as you plan your configuration:

<table>
<thead>
<tr>
<th>Deployment Scenario</th>
<th>Computers</th>
<th>Installation Options</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small</td>
<td>Computer 1</td>
<td>Use the Express option to install the following:</td>
<td>See “Installing the Express Option from the Deployment Manager” on page 36</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Console</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Application server</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Agent Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• X-Press Update Server</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Site Database</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Event Collector</td>
<td></td>
</tr>
<tr>
<td>Computer 2 (optional)</td>
<td></td>
<td>Install the SiteProtector SecurityFusion Module</td>
<td>See the SiteProtector SecurityFusion Module Guide.</td>
</tr>
<tr>
<td>Deployment Scenario</td>
<td>Computers</td>
<td>Installation Options</td>
<td>Reference</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------</td>
<td>----------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Medium</td>
<td>Computer 1</td>
<td>Install the Site Database and the Event Collector</td>
<td>See “Installing the Recommended Option” on page 39</td>
</tr>
<tr>
<td></td>
<td>Computer 2</td>
<td>Install Application Server, Agent Manager, X-Press Update Server, and Console on Second Computer</td>
<td>See “Installing the Recommended Option” on page 39</td>
</tr>
</tbody>
</table>
|                     | Computer 3 | Install additional Agent Managers and Event Collectors | • See “Installing an Additional Agent Manager” on page 58  
• See “Installing an Additional Event Collector” on page 57 |
|                     | Computer 4 (optional) | Install the SiteProtector SecurityFusion Module | See the SiteProtector SecurityFusion Module Guide. |
### Installing the Deployment Manager

#### About this task

The Deployment Manager lets you deploy and maintain SiteProtector and IBM ISS software from a central computer on your network. Use the Deployment Manager to install SiteProtector on one computer (Express installation), or install SiteProtector components on two computers (Recommended installation).

<table>
<thead>
<tr>
<th>Deployment Scenario</th>
<th>Computers</th>
<th>Installation Options</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Large</td>
<td>Computer 1</td>
<td>Install the Site Database and the Event Collector</td>
<td>See “Installing the Recommended Option” on page 39</td>
</tr>
<tr>
<td></td>
<td>Computer 2</td>
<td>Install Application Server, Agent Manager, X-Press Update Server, and Console on Second Computer</td>
<td>See “Installing the Recommended Option” on page 39</td>
</tr>
</tbody>
</table>
|                     | Computer 3      | Install additional Agent Managers and Event Collectors                                | • See “Installing an Additional Agent Manager” on page 58  
                                                                      • See “Installing an Additional Event Collector” on page 57 |
|                     | Computer 4      | Install additional Agent Managers and Event Collectors                                | • See “Installing an Additional Agent Manager” on page 58  
                                                                      • See “Installing an Additional Event Collector” on page 57 |
|                     | Computer 5 (optional) | Install the SiteProtector SecurityFusion Module                                      | See the SiteProtector SecurityFusion Module Guide. |
Installing the Deployment Manager is a two-task process:

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Download the installation program.</td>
</tr>
<tr>
<td>2</td>
<td>Install the Deployment Manager.</td>
</tr>
</tbody>
</table>

**Downloading the installation program**

**Procedure**

1. In Internet Explorer, type the address of the IBM ISS download Web site: [http://www.iss.net/downloads/](http://www.iss.net/downloads/) The Downloads page appears.
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, click **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 6**. 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 6.1 for SiteProtector 2.0 Service Pack 6**.
10. Save the file to your computer.
11. Run the program file.
12. Follow the instructions on the screens to complete the installation.

**Starting the Deployment Manager**

**About this task**

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 computer on the network that has access to it. 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.

---

**Installing the Express Option from the Deployment Manager**

**About this task**

The Express option provides a quick and easy way to install a version of SiteProtector that you can use with smaller configurations or for evaluation purposes. Use the background information and procedures in this topic to install an Express option with Deployment Manager.

Review the following topics to make sure that you are performing tasks correctly and have gathered the required information:

- “Installing the Express Option from Deployment Manager” on page 16
- “Information Required Checklist” on page 15

**SiteProtector components installed with this option**

The Express option installs all default SiteProtector components except for the Deployment Manager. The Express option lets you install a Microsoft Data Engine (MSDE) server or choose an existing SQL or MSDE server for the Site Database.

**MSDE option**

The MSDE option is a local data storage tool that is designed for smaller computer systems and not large enterprises. Consider using MSDE for evaluation purposes only.

**Important:** The Express option installs an English version of MSDE. If you want to install a localized version of MSDE, you must download it from the Microsoft Web site, and install it before you run the Express installation.

**If your SQL or MSDE database is out of date**

The Express option lets you use an existing SQL or MSDE database on your computer. If an existing SQL or MSDE database on your computer is not up-to-date, you must do one of the following, 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.

Important: If you intend to install an MSDE during the installation, you may be required to restart your computer. When the computer restarts and you log on, the installation automatically resumes.

**Enabling MSDE database communication over TCP/IP**

**Before you begin**

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 or MSDE instances on this computer, then you must choose the instance where you want to install the Site Database.
- If you want to install a non-English version of SQL Server or MSDE 2000, you must install it first, and then run the Express installation.

**About this task**

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

**Procedure**

1. Run the following program file:
   \programfiles\microsoft sql server\80\tools\bin\Svrnetcn.exe
2. Make sure that the Site Database you are configuring is selected in the **Instance(s) on this server** box.
3. Select the **General** tab.
4. Select **TCP/IP** in the Disabled protocols column, and then click **Enable**.
5. Click **OK**.
6. Restart the MSDE service.

**Installing the Express option from the Deployment Manager**

**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 or MSDE instance where you are installing the Site Database, and then click Next.

   **Note:** If a single SQL or MSDE instance is installed on this computer, the installation program installs the Site Database on this instance. If the program does not find a SQL or MSDE instance, then it installs an MSDE instance automatically.

8. Does a message appear stating that the installation program is installing an MSDE database?
   - If yes, click Yes, and then go to Step 9.
   - If no, then go to Step 10.

9. In the SA password window, type a password for the MSDE logon ID in the Password and Confirm Password fields, and then click OK.

   **Note:** The default user name for the MSDE database is sa.

10. In the Encryption Key Archival window, type the Folder location, 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.

   **Important:** The installation program may restart your computer twice so that it can install MSDE and MDAC components. When your computer restarts, log onto your computer. The installation program automatically resumes where it left off.

11. In the InstallShield Wizard Complete window, click Finish.
**Note:** By default, the installation program will automatically create and place 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**

**Before you begin**

Review the following topics to make sure that you are performing tasks in the correct order and have gathered the required information:
- [“Recommended Option Tasks” on page 18](#)
- [“Information Required Checklist” on page 15](#)

**About this task**

After you install the Deployment Manager, you can use it to install the Recommended option.

Installing the Recommended option is a two-task process:

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Install the Site Database and the Event Collector.</td>
</tr>
<tr>
<td>2</td>
<td>Install the Application Server, Agent Manager, X-Press Update Server, and a Console.</td>
</tr>
</tbody>
</table>

**Install 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**.

**Reference:** See [“Database Parameters,” on page 81](#).
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 will automatically create and place 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 the Express Option from the Download Center

About this task

The Express option provides a quick and easy way to install a version of SiteProtector that you can use in a small configuration or for evaluation purposes. Use the background information and procedures in this topic to install an Express option.

Review the following topics to make sure that you are performing tasks in the correct order and have gathered the required information:

- “Installing the Express Option without the Deployment Manager” on page 17
- “Information Required Checklist” on page 15

SiteProtector components installed with this option

The Express option installs all default SiteProtector components except for the Deployment Manager. The Express option lets you install a Microsoft Data Engine (MSDE) server or choose an existing SQL or MSDE server for the Site Database.

MSDE option

The MSDE option is a local data storage tool that is designed for smaller computer systems and not large enterprises. Consider using MSDE for evaluation purposes only.

Important: The Express option installs an English version of MSDE. If you want to install a localized version of MSDE, you must download it from the Microsoft Web site, and install it before you run the Express installation.

Existing SQL or MSDE databases that do not meet requirements

The Express option lets you use an existing SQL or MSDE database on your computer. If an existing SQL or MSDE database on your computer is not up-to-date, you must do one of the following 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

**Important:** If you intend to install an MSDE during the installation, you may be required to restart your computer. When the computer restarts and you log in, the installation automatically resumes where it left off.

**Installing the Express Option**

**Before you begin**

Do the following before you install the Express option:
• Download and install the SiteProtector Express Setup program file from the IBM ISS Download Center.
• If you have two or more SQL Server or MSDE instances on this computer, then you must choose the instance where you want to install the Site Database.
• If you want to install a non-English version of SQL Server or MSDE 2000, you must install it first, and then run the Express installation.

**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.
6. If the SQL Server window appears, select the SQL or MSDE instance where you are installing the Site Database, and then click Next.

**Note:** If a single SQL or MSDE instance is installed on this computer, the installation program installs the Site Database on this instance. If the program does not find a SQL or MSDE instance, then it installs an MSDE instance automatically.

7. Does a message appear stating that the installation program is installing an MSDE database?
   • If yes, click Yes, and then go to Step 8.
   • If no, then go to Step 9.
8. In the SA password window, type a password for the MSDE logon ID in the **Password** and **Confirm Password** fields, and then click OK.
Note: The default user name for the MSDE database is sa. Encryption Key Archival window appears.

9. In the Encryption Key Archival window, type the Folder location where you want to archive encryption keys preferably on a removable medium, and then click Next.

Important: The installation program may restart your computer twice so that it can install MSDE and MDAC components. When your computer restarts, log onto your computer. The installation program automatically resumes where it left off.

10. In the InstallShield Wizard Complete window, click Finish.

Note: By default, the installation program will automatically create and place 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 SiteProtector on a Clustered SQL Platform**

**Before you begin**

To install SiteProtector on a clustered SQL platform you must use an Enterprise SQL Server. SiteProtector does not work on a standard SQL Server platform.

When you install SiteProtector on a clustered SQL platform with Windows NT authentication, all computers must be in the same domain and domain accounts must be used.

Important: You cannot use implicit trust with the clustered installation.

**About this task**

This topic provides information for installing SiteProtector on a clustered SQL platform using either SQL or Windows NT authentication. The procedure for each type of authentication is different. Please refer to the procedure that applies to your system.

To install SiteProtector on a clustered SQL platform, install the individual packages in this sequence:

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Install the Site Database.</td>
</tr>
<tr>
<td>2</td>
<td>Install the Event Collector.</td>
</tr>
<tr>
<td>3</td>
<td>Install the Application Server.</td>
</tr>
</tbody>
</table>
SiteProtector installation on a clustered SQL platform with SQL Authentication

Procedure

1. Install the SSL certificate on all database 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](http://support.microsoft.com/?kbid=276553) or with SQL Server 2005
   - How to enable SSL encryption for SQL Server 2000 or 2005 with Microsoft Management Console

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.

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**. When the installation is complete, a message appears that indicates the installation was successful.

**SiteProtector installation on a clustered SQL platform with Windows Authentication**

**About this task**

**Note:** Do not use Deployment Manager to install Windows Authentication.

**Procedure**

1. Install the SSL certificate on all database 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](http://support.microsoft.com/?kbid=276553)  or with SQL Server 2005  
   - How to enable SSL encryption for SQL Server 2000 or 2005 with Certificate Server  

2. Install packaged in the following order:
   a. Event Collector
   b. Application Server
   c. Agent Manager
Note: For SQL 2000 only, 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, a message appears giving you the option to turn SSL communication off, retry the connection after adding the certificate to the cluster nodes, or exit the installation.

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 49.

Installing SiteProtector on Microsoft Windows 64-bit, SQL Server 64-bit

Before you begin

To install SiteProtector on a Windows 64-bit or SQL Server 64-bit platform you must use an Enterprise SQL Server. SiteProtector does not work on a standard SQL Server platform.

When you install SiteProtector on a Windows 64-bit or SQL Server 64-bit platform, all computers must be in the same domain and domain accounts must be used.

Important: You cannot use implicit trust with the clustered installation.

About this task

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

Note: You can only install the SiteProtector Database on a computer using Microsoft Windows 64-bit or SQL Server 64-bit.

To install SiteProtector on a Windows 64-bit or SQL Server 64-bit platform, install the individual packages in this sequence:

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Install the Site Database.</td>
</tr>
<tr>
<td>2</td>
<td>Install the Event Collector.</td>
</tr>
<tr>
<td>3</td>
<td>Install the Application Server.</td>
</tr>
<tr>
<td>4</td>
<td>Install the Agent Manager.</td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>5</td>
<td>Install the Console.</td>
</tr>
<tr>
<td>6</td>
<td>Install any other packages, such as the SecurityFusion Module (see the SiteProtector SecurityFusion Module Guide) or Event Archiver “Installing the Event Archiver” on page 60</td>
</tr>
</tbody>
</table>

**SiteProtector installation on a clustered SQL platform with 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.

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. When the installation is complete, a message appears that indicates the installation was successful.

SiteProtector installation on a Windows 64-bit or SQL Server 64-bit platform with Windows Authentication

About this task

Note: Do not use Deployment Manager to install Windows Authentication.

Procedure

Install packaged 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 from the DVD or from the Web site individually.

Important: Do not use Deployment Manager.

Task overview

You must install the individual packages in the following order:

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Install the Site Database.</td>
</tr>
<tr>
<td>2</td>
<td>Install the Event Collector.</td>
</tr>
<tr>
<td>3</td>
<td>Install the Application Server.</td>
</tr>
<tr>
<td>4</td>
<td>Install the Agent Manager.</td>
</tr>
<tr>
<td>5</td>
<td>Install the Console.</td>
</tr>
<tr>
<td>6</td>
<td>Install any other packages, such as the SecurityFusion Module (see the SiteProtector SecurityFusion Module Guide) or Event Archiver.</td>
</tr>
</tbody>
</table>

Site Database installation checklist

You need the following information to install the Site Database:

<table>
<thead>
<tr>
<th>✔️ Required Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>□ SQL Server name</td>
</tr>
<tr>
<td>□ Site name</td>
</tr>
</tbody>
</table>

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.

Event Collector installation checklist

You need the following information to install the Event Collector:

<table>
<thead>
<tr>
<th>✔️ Required Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>□ SQL Server name</td>
</tr>
</tbody>
</table>
**Required Information**

- 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

**Note:** You must have SiteProtector JRE installed before you install the Event Collector.

### Application Server installation checklist

You need the following information to install the Application Server:

- 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 (optional)

**Note:** This creates an account on your X-Press Update server to interact with the Agent Manager.

- SiteProtector group name (optional)
- Proxy information for the Internet
- Proxy information for the Agent Manager

**Note:** You must have SiteProtector JRE installed before you install the Event Collector.

### Agent Manager installation checklist

You need the following information to install the Agent Manager:

- 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
**Note:** You must have SiteProtector JRE installed before you install the Event Collector.

**Console installation checklist**

You need the following information to install the Console:

<table>
<thead>
<tr>
<th>✔️ Required Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐ Deployment Manager URL location (optional)</td>
</tr>
</tbody>
</table>

**Installing a component**

**Procedure**

1. Find the checklist for the component in this topic and make sure you have the required information.
2. Download the component package from the Download Center or find the package on the SiteProtector Installation DVD.
3. Run the program file for the component.
4. 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 6. Installing Additional Components

SiteProtector is a highly scalable application that allows you to add and reconfigure components as needed. Use the procedures in this chapter to install additional SiteProtector components and reconfigure agents so that they can report to these components.

Reference: For information about installing X-Press Update Servers and configuring X-Press Update Server groups, see the SiteProtector Configuration Guide.

Topics

"Component Overview" on page 54

"Installing an Additional SiteProtector Console" on page 56

"Installing an Additional Event Collector" on page 57

"Installing an Additional Agent Manager" on page 58

"Installing an Additional SiteProtector Event Viewer" on page 59

"Installing the Event Archiver" on page 60

"Removing and Reinstalling SiteProtector Components" on page 62
Component Overview

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.

SiteProtector components and flow of events

The shaded box in 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
Additional components to install

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

<table>
<thead>
<tr>
<th>Component</th>
<th>Reason to Install Additional</th>
</tr>
</thead>
</table>
| 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).                       |
| 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 failover.                 |

References

See the following documents for additional information about a particular component:

- For information about installing and configuring SecurityFusion Module, see the SiteProtector SecurityFusion Module Guide.
- For information about installing and configuring Third Party Module, see the SiteProtector Third Party Module Guide.
- For information about installing and configuring X-Press Update servers, see the SiteProtector Configuration Guide.
- For information about configuring Event Archiver, see the SiteProtector Configuration Guide.
Installing an Additional SiteProtector Console

Before you begin

Review the following topics to make sure that you are performing tasks correctly and have gathered the required information:

- "Recommended Option Tasks" on page 18
- "Information Required Checklist" on page 15

About this task

After you have installed SiteProtector, you may want to install additional SiteProtector Consoles. This option allows multiple users to monitor SiteProtector remotely.

Note: When you install an additional SiteProtector Console, an additional Event Viewer is automatically included in the installation.

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

Before you begin

Review the following topics to make sure that you are performing tasks correctly and have gathered the required information:

- "Recommended Option Tasks" on page 18
- "Information Required Checklist" on page 15

About this task

One Event Collector is installed with the Express and Recommended options. Use the procedures in this topic to install additional Event Collectors.

The more Event Collectors you have, the more agents SiteProtector can support.

Reference: See the SiteProtector Scalability Guidelines for recommendations on the number of Event Collectors per Site.

Installing an additional Event Collector is a two-task process:

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Install additional Event Collectors</td>
</tr>
<tr>
<td>2</td>
<td>Redirect agents</td>
</tr>
</tbody>
</table>

Installing an additional Event Collector

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.

Redirecting agents to Event Collectors

Procedure
1. Select the agent.
3. Select the Event Collector, and then click OK.

Installing an Additional Agent Manager

The Agent Manager allows SiteProtector to collect and manage data from agents and components. An Agent Manager is installed with the Express and Recommended options.

Requirement

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

Reference: See the SiteProtector Scalability Guidelines for recommendations about the number of Agent Managers per Site.

Installing additional Agent Managers

Reasons to install additional Agent Managers include the following:
• scaling for a large number of agents
• your network is partitioned into different geographical locations

Considerations for NAT environments

If you are installing the Agent Manager in an environment that 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 currently assigned to the Agent Manager’s network interface (NIC), and then type the IP address in the Custom IP address field.
Installing an Agent Manager

Before you begin
Review the following topics to make sure that you are performing tasks correctly and have gathered the required information:
- "Recommended Option Tasks" on page 18
- "Information Required Checklist" on page 15

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 SiteProtector Event Viewer

Before you begin
Review the following topics to make sure that you are performing tasks correctly and have gathered the required information:
- "Recommended Option Tasks" on page 18
- "Information Required Checklist" on page 15
About this task

The SiteProtector Event Viewer retrieves security events for security operators and security analysts to view for troubleshooting, providing near real-time access to security event information.

**Note:** The Express and Recommended installation options automatically install an Event Viewer on the same computer as the SiteProtector Console.

You can install an Event Viewer on a computer that doesn’t have any SiteProtector components installed on it, as long as you can connect to an Event Collector that is logging events that you want to monitor.

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

About this task

The Event Archiver component archives event data and improves database performance by reducing the number of events the Site Database must store.

**Note:** The Event Archiver is not included in all SiteProtector pricing plans. For more information, refer to the pricing plan that applies to your configuration.
Before you begin the installation, you must have the following information:

<table>
<thead>
<tr>
<th>Required Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name or IP of Agent Manager.</td>
</tr>
<tr>
<td>Application Server Name.</td>
</tr>
<tr>
<td>Account Name and Password for Agent Manager (optional).</td>
</tr>
<tr>
<td>SiteProtector Group Name (optional).</td>
</tr>
</tbody>
</table>

**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.
Removing and Reinstalling SiteProtector Components

This topic explains how to remove and reinstall individual SiteProtector components.

How to reinstall components

Remove and then reinstall components as follows:

- For each component except the Site Database, you can reinstall the component after you remove it.
- For the Site Database, you must first remove all the SiteProtector components that are installed, and then reinstall them.

CAUTION:
If you simply reinstall the Site Database, SiteProtector does not return to its pre-installation state.

About the SQL logon user ID

If a component cannot connect to the Site Database, you must supply a log-on user ID and password. If you are removing all SiteProtector components, you may be prompted up to three times for the user ID and password. The following are important points to remember about the SQL log on user ID:

- On most systems, the sa log-on is the only SQL log-on with the access rights required to run the SQL scripts that remove the programs.
- Select the Do Not Connect to the Database check box only if you have to. If the database is still installed and you select this check box, the component you are removing will not be unregistered from the database. This may cause problems if you are planning to reinstall this component without reinstalling the database.

Removing individual components

Put your short description here; used for first paragraph and abstract.

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, do one of the following:
   - 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 do one of the following:
   • 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.
Chapter 7. Troubleshooting

This chapter provides solutions to common installation problems and explains how to fix unsuccessful SiteProtector installations and remove SiteProtector completely.

**Topics**

“Issues Related to SiteProtector Installation” on page 66

“Fixing an Unsuccessful SiteProtector Recommended Installation” on page 68

“Removing SiteProtector Completely” on page 69
Issues Related to SiteProtector Installation

This topic provides solutions to issues that you might encounter when you install or uninstall SiteProtector components.

Not Found messages displayed

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

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

issApp login already exists

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

Explanation: This usually occurs when you attempt to install the Application Server over an unsuccessful uninstallation. If the RealSecure 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: Do the following:
1. Make sure both services (or applications, if running as such) are stopped.
2. Use SQL Server 2000 Enterprise Manager or SQL Server 2005 Management Studio to manually delete the existing issApp login, which is located in the /Security/Logins folder for the Site Database.

Event collector login cannot be deleted

Description: 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.

Solution: Do one of the following:
- 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 2000 Enterprise Manager or SQL Server 2005 Management Studio to manually delete the existing EventCollector_<computer> login, located in the /Security/Logins folder for the Site Database.

**Additional Event Collector encryption**

**Description:** When you install an additional Event Collector, the encryption is not initially set.

**Solution:** After installing an additional Event Collector, you must stop, and then restart it, to set encryption.

To stop, and then restart an Event Collector:

1. Select the Asset node in the Site Manager group tree.
2. Select the **Agent** view.
3. Right-click the Event Collector you want to restart from the pop-menu.
4. Select **Event Collector → Stop**.

   **Note:** When the Event Collector is stopped, the value in the Status column is “Stopped.”

5. Right-click the **Event Collector** in the pop-up menu.
6. Select **Event Collector → Start**.

   **Note:** When the event collector starts, the value in the Status column reads “Active.”

**Can’t stop the Event Collector**

**Description:** You have removed the Application Server and the Console, but can’t stop the Event Collector.

**Solution:** The two ways to handle this are as follows:

- 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.

**Database in use error**

**Description:** While uninstalling the Site Database, an error states that the database is in use.
Solution: Use the SQL Server 2000 Enterprise Manager or SQL Server 2005 Management Studio to manually stop all processes associated with the Site Database, and then uninstall the database.

Fixing an Unsuccessful SiteProtector Recommended Installation

SiteProtector is not completely installed until you install every component. This topic explains what to do if the installation of any component is unsuccessful during a Recommended installation. In most cases, you can fix the problem by running the installation program again. This topic explains when you can and cannot do that.

About the installation

The following information about how the SiteProtector Recommended installation works may help you to better understand the process of fixing an unsuccessful installation:

- The installation program only installs components that are not already installed on the computer.
- 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.

Fixing an unsuccessful installation

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

- For each component except the Site Database, you can run the installation program for that component again to see if the installation succeeds the second time.
- For the Site Database, you must first remove every SiteProtector component (except for the Deployment Manager), if any are installed, and then reinstall them.

CAUTION:
If you reinstall only the Site Database; SiteProtector does not return to its pre-installation state.

- If the installation of more than one component did not succeed, follow the original installation instructions so that you install the components in the correct order.
Removing SiteProtector Completely

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. Site Database
7. 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, do one of the following:
   • 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 Communication

The encryption and authentication protocols that are enabled between SiteProtector components are not automatically enabled on database components. If you want to encrypt and authenticate database communications, you must do it manually. This chapter tells how to encrypt and authenticate database communications using Microsoft SQL encryption protocols.

**Important**: The Site Database contains sensitive information about the security of your network. IBM ISS recommends that you secure all database communications.

**Topics**

- [“Configuring Encryption Protocols” on page 72](#)
- [“Important Requirements and Considerations for Configuring Encryption” on page 73](#)
- [“Configuring SSL Encryption” on page 74](#)
- [“Configuring multiprotocol encryption” on page 76](#)
- [“Restarting SiteProtector Components” on page 79](#)
Configuring Encryption Protocols

This topic discusses the different types of encryption protocols, which type you should use, and how to configure the encryption protocol for your computer.

Two types of encryption protocols

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

<table>
<thead>
<tr>
<th>Encryption Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiprotocol</td>
<td>Multiprotocol encryption uses the Multiprotocol Server Network Library to encrypt and authenticate communication. Multiprotocol does not require certificates and can establish encrypted and authenticated communication over most network application interfaces, such as TCP/IP sockets and Named Pipes. <strong>Important:</strong> You cannot configure Microsoft SQL 2005 using the Multiprotocol encryption. For more information on Microsoft SQL 2000 encryption, go to the following Web site: <a href="http://support.microsoft.com/default.aspx?scid=kb;en-us;238984">http://support.microsoft.com/default.aspx?scid=kb;en-us;238984</a></td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer (SSL) encryption is more secure but much more difficult to configure and requires that you purchase certificates. Both Microsoft SQL 2000 and 2005 can use SSL encryption. For information about how to secure database communication with SSL, search the IBM ISS Knowledgebase for the article “How do I set up SiteProtector to use encryption for database communication?” (Answer ID 1824) at the following link: <a href="http://www.iss.net/support/knowledgebase/">http://www.iss.net/support/knowledgebase/</a></td>
</tr>
</tbody>
</table>
Which encryption protocol should I use?

Use the following table to determine which encryption protocol to configure:

<table>
<thead>
<tr>
<th>If you are running this version of SQL server...</th>
<th>Then configure encryption using the following protocol...</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000 and earlier</td>
<td>Multiprotocol or SSL</td>
</tr>
<tr>
<td>2005</td>
<td>SSL</td>
</tr>
</tbody>
</table>

**Important:** If you are using multiprotocol and are planning to upgrade to SQL 2005, you must delete the multiprotocol setup, and then set up the SSL encryption protocol.

**Important Requirements and Considerations for Configuring Encryption**

Before you secure database communication, review the following requirements and considerations.

**Prerequisites**

You must have the following privileges to perform the procedures in the chapter:

- SiteProtector Administrator privileges
- SA privileges on the Site Database

**Communication that is not encrypted automatically**

Securing database communications is a two-way process. You must manually configure encryption and authentication on the following components if they are not installed on the Site Database computer:

- Event Collector
- Agent Manager
- SecurityFusion Module (always a standalone component)
- Active Directory

**Restarting components**

You must restart SiteProtector components after you configure encryption and authentication.
Configuring SSL Encryption

About this task


You can configure SSL encryption when you use both Microsoft SQL 2000 and 2005 versions.

**Important:** Though the above article does not mention this, you must install private certificate material along with the public certificate material when you install the certificate on the SQL Server computer.

**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 with an Event Collector**

**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, refer to the Microsoft article to determine what is wrong.

7. From a Site Protector Console, stop, and then restart the Event Collector.

**Enabling SSL with Active Directory**

**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, refer to 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 with an Agent Manager
Procedure
1. Locate the installation directory for the Agent Manager, and then open the RSPDC.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. Refer to the Microsoft article to determine what is wrong.

Enabling SSL with the SecurityFusion module
Procedure
1. In the Site Protector 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, check 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. Refer to the Microsoft article to determine what is wrong.
Configuring multiprotocol encryption

This topic gives the procedures for securing database communication when configuring multiprotocol encryption and authentication on the Site Database.

About this task

Important: You can only configure multiprotocol encryption when you use Microsoft SQL 2000 and previous versions.

Configuring Microsoft SQL encryption

Procedure

1. On the Start menu, select Programs → Microsoft SQL Server, and then click Server Network Utility. The Server Network Utility window appears.
2. If Multiprotocol does not appear under the Enabled protocols column, select Multiprotocol, and then click Enable.
3. Click Multiprotocol, and then click Properties.
4. Do you want to force all clients connecting through the Site Database to be encrypted?
   - If yes, select Enable Encryption.
   - If no, click OK.

Note: This is the default. A window appears, stating that these changes will not take effect until SQL Server is restarted.
5. Restart SQL Server.

Adding a registry key

About this task

Note: After you secure communication on the Site Database, you must add registry keys for each component that communicates with the Site Database. Perform this procedure only on components that are not installed on the Site Database computer.

The registry key enables encryption between the component computer and the Site Database. You must add the registry key to any computer on which the following components are installed:

- Event Collector
- Agent Manager
- SecurityFusion Module
- Active Directory
Procedure
1. On the computer where the component is installed, select Start → Run. The Run window appears.
2. Type regedit. The Registry Editor appears.
3. Navigate to the following folder:
   HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/MSSQLServer/
   Client/RPCNetlib
   
   Note: If the RPCNetlib registry key folder does not appear on your system, you must manually create it. The system creates the registry key the first time you successfully connect to a server using multiprotocol. If you have not successfully connected to a server using multiprotocol, then the system does not create a registry key.

   Tip: To create a RPCNetlib registry key folder, right-click the Client folder, and then select New to create the folder.
4. Right-click the RPCNetlib folder. A pop-up menu appears.
5. Select New → String Value. A new value is created and added to the right pane.
6. Name the value Security.
8. Type Encrypt, and then click OK.
9. Close the Registry Editor.
10. Repeat Step 1 through Step 9 for each component you are configuring.

Securing SiteProtector component communication
About this task
After you add registry keys, you must configure encryption and authentication on the components that communicate with the Site Database. This topic provides procedures for securing the following components:
• Event Collector
• Agent Manager
• SecurityFusion Module

Important: The client computer where the remote components are installed and the Site Database server must reside on the same domain.

Enabling encryption on the Event Collector computer
Procedure
1. On the Start menu, select Settings → Control Panel → Administrative Tools → Data Sources (ODBC). The ODBC Data Source Administrator Wizard window appears.
2. Select the **System DSN** tab.
3. Select **RSNTEventCollector**.
4. Click **Configure**.
5. Click **Next**. The Microsoft SQL Server DSN Configuration window appears.
6. Click **Client Configuration**. The Edit Network Library Configuration window appears.
7. Select **Multiprotocol**, and then click **OK**. The Microsoft SQL Server DSN Configuration window appears.
8. Complete the configuration information, and then click **OK**.
9. Click **Finish**, and then click **OK**.

### Configuring encryption on the Agent Manager or the SecurityFusion Module computer

**Procedure**

1. Start the client configuration program file (CLICONFG.EXE) in the \Winnt\System32 directory. The SQL Server Client Network Utility window appears.
2. Select **Multiprotocol**, and then click **Enable**. The Multiprotocol option moves to the Enable area of the window.
3. Click **OK**.

### Enabling encryption between Active Directory and the Site Database

**About this task**

If you are using Active Directory to populate and manage hosts in the Enterprise Groups pane, you must secure the communication between Active Directory and the Site Database.

This procedure configures encryption and authentication between the Active Directory reconciler process and the Site Database.

**Important:** This procedure does not encrypt the actual Active Directory query run on the Active Directory servers. This communication is transmitted in clear text (without encryption).

**Procedure**

1. On the **Start** menu, select **Settings** → **Control Panel** → **Administrative Tools** → **Data Sources (ODBC)**. The ODBC Data Source Administrator Wizard window appears.
2. Select the **System DSN** tab.
3. Select **IssADReconciler**.
4. Click **Configure**.
5. Click **Next**. The Microsoft SQL Server DSN Configuration window appears.
6. Click **Client Configuration**. The Edit Network Library Configuration window appears.
7. Select **Multiprotocol**, and then click **OK**. The Microsoft SQL Server DSN Configuration window appears.
8. Complete the configuration information, and then click **OK**.
9. Click **Finish**, and then click **OK**.

### Restarting SiteProtector Components

**About this task**

After you secure database communications, you must restart the SiteProtector components that you have reconfigured so that the changes take effect.

**Note:** This procedure does not apply to the Active Directory communications.

**Procedure**

1. Select the **Agent** view.
2. Right-click the name of the component in the right pane, and then select **Stop** from the menu.
3. Verify that the component has stopped.
4. Right-click the name of the component, and then select **Start**.
5. Repeat Steps 1 through 4 for each component you are configuring.
Appendix. Database Parameters

Database parameters control the size and specify the location of Site Database files. This appendix lists default parameters for the following Site Database files:

- Primary data
- Log

Editing database parameters

You can edit database parameters, as follows:

- If you are using the Recommended option, you can change most of the parameters when you install SiteProtector.
- If you are using the Express option, you must accept the defaults when you install SiteProtector, but you can edit them after SiteProtector is installed using a SQL Server application.

Primary data file parameters

The primary data file stores your data. The following table shows the default information for the primary data file:

<table>
<thead>
<tr>
<th>Primary Data File Information</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filename</td>
<td>RealSecureDB.mdf</td>
</tr>
<tr>
<td>Path</td>
<td>\Program Files\ISS\RealSecure\SiteProtector\Enterprise Database\Data</td>
</tr>
<tr>
<td>Initial Size</td>
<td>512 MB</td>
</tr>
<tr>
<td>Size of Increment</td>
<td>256 MB</td>
</tr>
<tr>
<td>Note: If available disk space is less than approximately 1 gigabyte (GB), this parameter will be adjusted.</td>
<td></td>
</tr>
<tr>
<td>Increment Automatically</td>
<td>Yes</td>
</tr>
<tr>
<td>Maximum File Size</td>
<td>50% of available disk space</td>
</tr>
</tbody>
</table>

Note: If available disk space is less than approximately 1 gigabyte (GB), the Initial Size parameter will be adjusted accordingly.
Default information for log files

The log file stores any changes you make to your data, in case of database failure. The following table shows the default information for the log file:

<table>
<thead>
<tr>
<th>Log File Information</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filename</td>
<td>RealSecureDBLog.mdf</td>
</tr>
<tr>
<td>Path</td>
<td>\Program Files\ISS\RealSecure\SiteProtector\Enterprise Database\Data</td>
</tr>
<tr>
<td>Initial Size</td>
<td>32 MB</td>
</tr>
<tr>
<td>Size of Increment</td>
<td>128 MB</td>
</tr>
<tr>
<td>Note: If available disk space is less than approximately 1 gigabyte (GB), this parameter will be adjusted.</td>
<td></td>
</tr>
<tr>
<td>Increment Automatically</td>
<td>Yes</td>
</tr>
<tr>
<td>Maximum File Size</td>
<td>20% of primary data file's maximum size</td>
</tr>
<tr>
<td></td>
<td>20% of available disk space</td>
</tr>
</tbody>
</table>
Index

A
Agent Managers
  installing  58
  role in securing database communication  78
agent, description  1
appliance, description  1
attack pattern recognition  6

C
can't stop error, Event Collector  67
components illustration  3
cryptographic providers, guidelines for selecting  31

data file parameters, primary  81
database
  editing data and log file parameters  81
  installing non-English databases  36, 41
  list of fully qualified names  15
database in use error  67
Deployment Manager
  downloading  35
  entering the correct address  36
  Express installation option  36
  starting  35

E
encryption not initially set error  67
evaluating SiteProtector Express option  36, 41
Event Archiver  60
Event Archiver Installation
  Information Needed  61
Event Collectors
  can't stop error  67
  changing passwords  25
  installing additional  57
  redirecting agents to  58
Event Viewer, installing an additional  60
Express Option from Deployment Manager, installing  36
Express Option, installing  41

H
hard drives, computers with multiple  10
Hfnetcheck  27
hotfixes, installing the latest  26

I
IBM Internet Security Systems
  technical support ix
  Web site ix
impact analysis  6
installation
  identification number assigned during  11
  options  56
  phases  29, 53
  third-party software security issues  24
installing
  additional components, illustration  54
  additional Event Collector  57
  additional Event Viewer  59
  Event Viewer, installing an additional  59
Installing the Event Archiver  60
IP addresses, computers with multiple  10
issApp already exists error  66

L
log files  11, 82
login cannot be deleted error  66

M
Microsoft SQL Server
  deleting the existing issApp
    login  66
  encryption  72
  non-English version  37, 42
  security issues with  24
Microsoft Windows Server 2003
  download settings  10
  hardening security  25
MSDE
  installed with Express option  36, 41
  non-English version  37, 42
Multiprotocol Server Network Library  72

P
parameters, data file  81
passwords, Event Collector  25
patches, applying Microsoft  24
Primary Datafile, installation defaults  81
private keys
  guidelines for selecting archives  31
  installation programs that archive  31
  preliminary considerations  10

R
RealSecureDB.mdf  81
RealSecureDBLog.mdf  82
Recommended Option, installing  39
registry keys, role in securing database communication  76
removing components, order of  69
reporting  6

S
Scalability Guidelines, implementing  32
scanner, description  1
SecurityFusion Module  6
  attack pattern recognition  6
  impact analysis  6
  role in securing database communication  78
sensor, description  1
service packs, installing the latest  26
SiteProtectorExpress-Setup.exe  42
SSL  72

T
technical support, IBM Internet Security Systems ix
Third Party Module
description  6
third-party software
  fixing security issues  25
third-party software (continued)
hardening security
  on Microsoft Windows 2003 Server 24
preliminary security
  measures 24
security issues with 24
troubleshooting
  identification number generated
    by installation programs 11
tasks 65
  uninstalling SiteProtector 69
trusted sites 10

U
  uninstalling SiteProtector 69

W
Web site, IBM Internet Security
  Systems ix