

IBM Proventia<sup>®</sup> Management SiteProtector<sup>™</sup>

# Configuration Guide

Version 2.0, Service Pack 7.0

© Copyright IBM Corporation 1994, 2008.  
IBM Global Services  
Route 100  
Somers, NY 10589  
U.S.A.

Produced in the United States of America.

All Rights Reserved.

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](mailto:support@iss.net).

May 30, 2008

# Contents

## Preface

Overview . . . . .	9
How to Use SiteProtector System Documentation . . . . .	10
Getting Technical Support. . . . .	11
. . . . .	12

## Chapter 1: Introduction to the SiteProtector System

Overview . . . . .	13
What is the SiteProtector System? . . . . .	14
SiteProtector System Components. . . . .	15
Additional Modules for a SiteProtector System. . . . .	18

## Chapter 2: The SiteProtector System Setup Process

Overview . . . . .	19
Stages of the Setup Process. . . . .	20

## Part I: Configuring and Updating a SiteProtector System

### Chapter 3: The Configuration and Update Stage

Overview . . . . .	25
Overview of this Stage . . . . .	26
Checklist for this Stage. . . . .	27

### Chapter 4: Configuring the Console

Overview . . . . .	29
Setting General Options . . . . .	30
Setting Logging Options . . . . .	32
Setting Documentation Options . . . . .	33
Setting Browser Options. . . . .	35
Setting Global Summary Options . . . . .	36
Setting Notifications Options . . . . .	37
Setting Report Options . . . . .	38
Setting Authentication Options. . . . .	39
Setting Summary Options . . . . .	40
Setting Asset View Options . . . . .	44
Setting Ticket Options. . . . .	45
Setting Agent View Options . . . . .	46
Setting Analysis View Options . . . . .	47

### Chapter 5: Setting Up Licenses

Overview . . . . .	49
What are Licenses?. . . . .	50
What are OneTrust Tokens and OneTrust Licenses? . . . . .	52
Proventia OneTrust Licensing . . . . .	53
Processes for Using OneTrust Licenses . . . . .	55
Downloading OneTrust Licenses. . . . .	56
Working with OneTrust Tokens . . . . .	59
Obtaining Agent and Desktop Licenses . . . . .	61

Adding and Removing Agent or Desktop Licenses . . . . .	62
<b>Chapter 6: Configuring Agent Managers</b>	
Overview . . . . .	65
What is the Agent Manager? . . . . .	66
Configuring Agent Manager Properties . . . . .	67
Viewing Agent Manager Properties . . . . .	68
Creating Agent Manager Accounts . . . . .	69
Assigning Agent Managers to Agents . . . . .	70
<b>Chapter 7: Configuring X-Press Update Servers</b>	
Overview . . . . .	71
What is the X-Press Update Server? . . . . .	72
Configuring the Server Settings Policy . . . . .	73
Configuring the XPU Settings Policy . . . . .	75
Setting Up Additional Stand-Alone XPU Servers . . . . .	76
Configuring XPU Servers to Download from Other XPU Servers . . . . .	79
Securing XPU Servers . . . . .	81
Clustering XPU Servers . . . . .	82
Configuring XPU Servers for Manual Updates . . . . .	84
<b>Chapter 8: Updating Your SiteProtector System</b>	
Overview . . . . .	87
<b>Section A: Updates Overview</b> . . . . .	89
Overview . . . . .	89
Update Process . . . . .	90
X-Press Updates . . . . .	92
Service Packs . . . . .	94
<b>Section B: Updating SiteProtector System Components</b> . . . . .	95
Overview . . . . .	95
Determining Update Status . . . . .	96
Applying Updates to SiteProtector System Components . . . . .	97
Applying Updates to the SiteProtector Core Component . . . . .	99
<b>Section C: Applying Security Content to Agents</b> . . . . .	101
Overview . . . . .	101
Determining Whether Security Content Updates Are Available . . . . .	102
Updating Agent Security Content . . . . .	103
Verifying an Agent's Update History . . . . .	105
Removing Agent Security Content . . . . .	106
<b>Section D: Applying Updates without XPU Server Internet Access</b> . . . . .	109
Overview . . . . .	109
Update Process without XPU Server Internet Access . . . . .	110
Downloading Update Files with the Manual Upgrader . . . . .	111
Downloading Update Files from the IBM ISS Download Center . . . . .	112
Copying Update Files to the XPU Server . . . . .	114
Manually Refreshing Component or Agent Status . . . . .	117
Updating the Update Server and the Event Archiver . . . . .	118
<b>Chapter 9: Configuring Event Collectors</b>	
Overview . . . . .	121
What is the Event Collector? . . . . .	122
Assigning Event Collectors Manually . . . . .	123
Event Collector Failover Process . . . . .	124

Configuring Event Collectors for Failover . . . . .	125
<b>Chapter 10: Enabling the Event Viewer</b>	
Overview . . . . .	127
What is the Event Viewer? . . . . .	128
Enabling the Event Viewer . . . . .	129
Starting the Event Viewer . . . . .	130
<b>Chapter 11: Configuring the Site Database</b>	
Overview . . . . .	131
Viewing Site Database Properties. . . . .	132
Setting Database Maintenance Options. . . . .	134
Database Defragmenting . . . . .	137
Log File Purge. . . . .	138
Database Table Purge . . . . .	139
Emergency Database Purge . . . . .	143
Configuring Database Notifications . . . . .	145
Automatic Database Backup . . . . .	147
<b>Chapter 12: Configuring User Permissions</b>	
Overview . . . . .	151
<b>Section A: SiteProtector System Permission Management.</b> . . . . .	153
Overview . . . . .	153
Methods for Managing Permissions . . . . .	154
Searching for Users and Groups . . . . .	156
Permissions Affected by Upgrades . . . . .	157
Working with Policy Permissions . . . . .	159
<b>Section B: SiteProtector System User Groups</b> . . . . .	161
Overview . . . . .	161
What is a SiteProtector System User Group? . . . . .	162
Creating SiteProtector System User Groups . . . . .	163
Adding Members to SiteProtector System User Groups . . . . .	164
<b>Section C: Global Permissions</b> . . . . .	167
Overview . . . . .	167
What are Global Permissions? . . . . .	168
Assigning and Removing Global Permissions . . . . .	170
<b>Chapter 13: Configuring the Event Archiver</b>	
Overview . . . . .	173
Important Requirements and Considerations . . . . .	174
Event Rules. . . . .	175
Creating Event Rules that Filter by IP Address . . . . .	176
Creating Event Rules That Filter by Event Type . . . . .	179
Setting the Order of Event Rules . . . . .	180
Viewing Archived Events . . . . .	181
Modifying the Event Archiver Directory Structure . . . . .	182
<b>Chapter 14: Configuring Ticketing</b>	
Overview . . . . .	185
Working with the Remedy Action Request System (Remedy) . . . . .	187
Working with Tickets . . . . .	190
Working with Vulnerability Auto Tickets . . . . .	192
Working with Ticketing Logs . . . . .	196
Defining Notification Settings. . . . .	197

Defining Ticket Priorities . . . . .	198
Defining Ticket Status. . . . .	200
Defining Custom Categories . . . . .	202
Managing Ticketing Plug-ins. . . . .	203
Defining Response Settings. . . . .	205
Defining Auto Ticketing Settings. . . . .	207

## Part II: Setting Up Groups

### Chapter 15: The Group Setup Stage

Overview . . . . .	211
Overview of this Stage . . . . .	212
Checklist for this Stage. . . . .	213

### Chapter 16: Setting Up Groups

Overview . . . . .	215
What are Groups?. . . . .	216
Default Group Names. . . . .	219
Organizing Groups and Subgroups . . . . .	223
Creating Groups . . . . .	225
Creating System Scanner Vulnerability Assessment Application Groups . . . . .	228

### Chapter 17: Setting Group-Level Permissions

Overview . . . . .	229
What are Group-Level Permissions?. . . . .	230
Working with the Permissions Property Window . . . . .	233
Setting up Group-Level Permissions . . . . .	235
Working with Permission Inheritance . . . . .	238
Setting Permissions with <i>Show Subgroups</i> Enabled . . . . .	241

### Chapter 18: Working with Components

Overview . . . . .	243
Stopping, Starting, and Refreshing Components. . . . .	244
Resetting Component Passwords. . . . .	246
Distributing Keys to SiteProtector System Components . . . . .	250

## Part III: Setting Up Agents

### Chapter 19: The Agent Setup Stage

Overview . . . . .	257
Overview of this Stage . . . . .	258
Appliance Setup Checklists . . . . .	261
Scanner Setup Checklists . . . . .	262
Network Sensor and Server Sensor Setup Checklists . . . . .	264

### Chapter 20: Setting Up Agents

Overview . . . . .	265
<b>Section A: Installing Agents</b> . . . . .	267
Overview . . . . .	267
Installation Methods. . . . .	268
Installing Agents with the Deployment Manager . . . . .	269
Adding Installation Packages to the Deployment Manager . . . . .	271
Installing Agents with Separate Installation Packages . . . . .	272

<b>Section B: Registering Agents</b> . . . . .	273
Overview . . . . .	273
New Agent Wizard . . . . .	274
Automatically Registering Agents . . . . .	276
Manually Registering Agents with the Site . . . . .	278
<b>Section C: Distributing Keys and Certificates</b> . . . . .	281
Overview . . . . .	281
Manually Distributing Keys . . . . .	282
Using the Public Key Configuration Tool . . . . .	285
<b>Section D: Updating Agents</b> . . . . .	287
Overview . . . . .	287
Determining Agent Update Status . . . . .	288
Updating Agents . . . . .	289
Removing Updates . . . . .	291

## Part IV: Adding Assets

### Chapter 21: The Asset Setup Stage

Overview . . . . .	295
Overview of this Stage . . . . .	296
What are Assets? . . . . .	297

### Chapter 22: Adding Assets

Overview . . . . .	299
Adding Assets Manually . . . . .	301
Adding Assets from a Host File . . . . .	303
Adding Assets from an Asset Definition File . . . . .	305
Adding Assets from Active Directory . . . . .	308
Adding Assets with Network Internet Scanner . . . . .	311
Editing Asset Properties . . . . .	313
Grouping Ungrouped Assets . . . . .	316

## Part V: Setting Up the Reporting Module

### Chapter 23: Reporting Module

Overview . . . . .	321
Working with Reports . . . . .	322
Working with Event Data Reports . . . . .	323
Compliance and Summary Reports . . . . .	325
Working with Compliance and Summary Reports . . . . .	329

### Chapter 24: Configuring Audit Options

Overview . . . . .	331
Audit Options . . . . .	332
Configuring the SiteProtector System to Log Actions . . . . .	339

## Part VI: Troubleshooting

### Chapter 25: Troubleshooting

Overview . . . . .	343
Issues Related to Agents and Components . . . . .	344

---

**Contents**

---

Issues Related to Operating a SiteProtector System . . . . .	351
Issues Related to Reporting Module . . . . .	353
Issues Related to Low Memory . . . . .	354
Issues Related to Configuring and Updating the SiteProtector System . . . . .	355
<b>Index</b> . . . . .	<b>357</b>



# Preface

## Overview

- Introduction**      The *SiteProtector System Configuration Guide* contains the information a Security Manager needs to configure, update, and maintain a SiteProtector system.
- Scope**              This guide explains what you need to do to configure your SiteProtector system and make it fully operational. This guide also contains configuration information you need to maintain your site as it grows and as new software becomes available. Before you begin, you must have installed your SiteProtector system and any components that support agents and appliances.
- Audience**          This guide is written for the person who configures, updates, and maintains your SiteProtector system. For many sites, that person is the Security Manager who is responsible only for maintaining the security of the network. For other sites, the Security Manager may also be responsible for aspects of network and security administration, such as network administration and security analysis.

# How to Use SiteProtector System Documentation

**Using this guide** Use this guide to configure and maintain your SiteProtector system after you have installed your SiteProtector system and any components that support agents and appliances. To configure your SiteProtector system the first time, use the “Checklist for this Stage” on page 27. Then use the guide as a reference guide for installing agents and appliances, changing configuration settings, and maintaining your SiteProtector system.

**Assumptions** When a procedure references an installation folder, it refers to the default installation folder. If you used a different folder, you must adjust the procedure accordingly.

**User role** You must be a SiteProtector system Administrator to perform most of the tasks in this guide.

**Related publications** Use the following documents if you have not yet installed your SiteProtector system and need information about SiteProtector system configuration options:

- *SiteProtector System Requirements*
- *SiteProtector System Supported Agents and Appliances*

**Other SiteProtector system user documents** Table 1 describes other SiteProtector system user documents.

Document	Contents
<i>SiteProtector System Installation Guide</i>	Provides the tasks for installing SiteProtector system components and optional modules. It includes information about advanced configuration tasks such as hardening third-party software security, securing database communication, configuring firewalls for SiteProtector system traffic, and configuring failover Event Collectors
<i>SiteProtector System Policies and Responses Configuration Guide</i>	Contains information for a Security Manager to configure, update, and maintain policies and responses for a SiteProtector system
<i>SiteProtector System User Guide for Security Analysts</i>	Contains information for a Security Analyst to manage policy and responses for a SiteProtector system
<i>SiteProtector System Help</i>	Contains all the procedures that you need to use a SiteProtector system, including advanced procedures that may not be available in a printed user document

**Table 1:** *Description of SiteProtector system user documents*

**License agreement** For licensing information about IBM Internet Security Systems products, download the IBM Licensing Agreement from [http://www-935.ibm.com/services/us/iss/html/contracts\\_landing.html](http://www-935.ibm.com/services/us/iss/html/contracts_landing.html).

## Getting Technical Support

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

**The IBM ISS Web site** The IBM Internet Security Customer Support Web page (<http://www-935.ibm.com/services/us/index.wss/offerfamily/iss/a1029129>) provides direct access to online user documentation, current versions listings, detailed product literature, white papers, and the Technical Support Knowledgebase.

**Hours of support** The following table provides hours for Technical Support at the Americas and other locations:

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

**Table 2:** *Hours for technical support*

**Contact information** For contact information, go to the IBM Internet Security Systems Contact Technical Support Web page at <http://www-935.ibm.com/services/us/index.wss/offering/iss/a1029178>.



## Chapter 1

# Introduction to the SiteProtector System

## Overview

### Introduction

This chapter provides an overview of the SiteProtector system and includes information about SiteProtector system components and additional modules.

### In this chapter

This chapter contains the following topics:

<b>Topic</b>	<b>Page</b>
What is the SiteProtector System?	14
SiteProtector System Components	15
Additional Modules for a SiteProtector System	18

# What is the SiteProtector System?

## Introduction

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

## SiteProtector system architecture

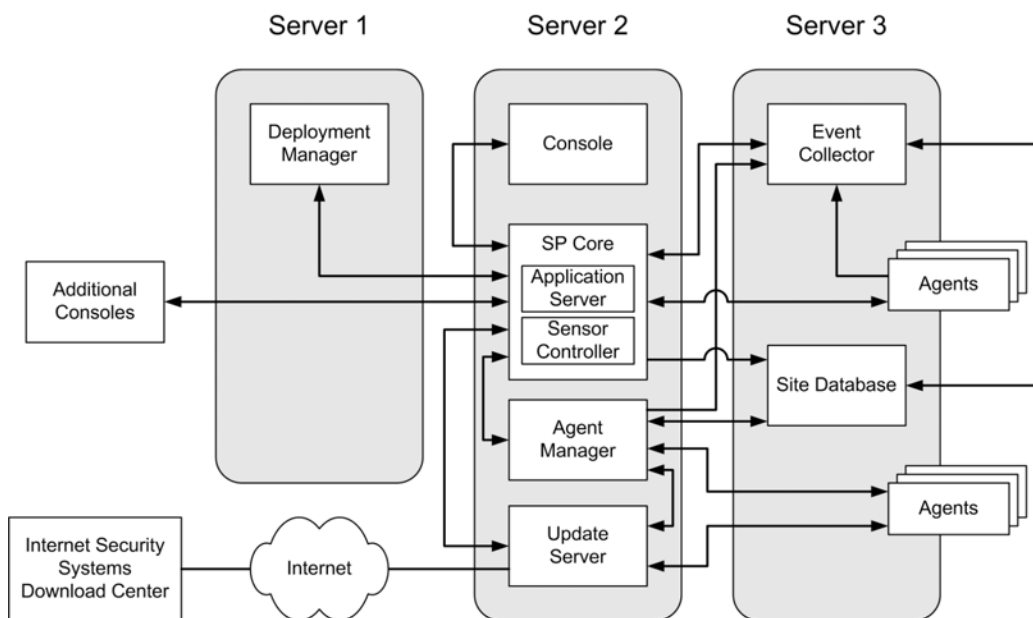
Table 3 describes the SiteProtector system architecture.

Components	Reference
core SiteProtector system functionality	See “SiteProtector System Components” on page 15.
additional modules that provide added SiteProtector system functionality	See “Additional Modules for a SiteProtector System” on page 18.

**Table 3:** *SiteProtector system architecture*

## Illustration

Figure 1 illustrates the architecture of a SiteProtector system, including SiteProtector system components and the agents that work with the SiteProtector system:



**Figure 1:** *Components and agents in a typical Site*

## Communication channels

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

# SiteProtector System Components

## Introduction

The SiteProtector system consists of different components, each with a very specific function in the SiteProtector system. The SiteProtector system interface refers to SiteProtector system components as agents.

## Component descriptions

Table 4 describes the SiteProtector system components.

Component	Description
Agent Manager (previously known as Desktop Controller)	<p>Provides you with the ability to configure, update, and manage the following SiteProtector components and other IBM ISS products:</p> <ul style="list-style-type: none"> <li>• X-Press Update Server</li> <li>• Desktop Protection agents</li> <li>• Proventia G appliances</li> <li>• Proventia Network IPS</li> <li>• Proventia Network MFS</li> </ul> <p>As these agents generate security data, the Agent Manager also facilitates the data processing required for you to view the data in the Console.</p>
Console	<p>The interface where you perform all SiteProtector system tasks, including the following:</p> <ul style="list-style-type: none"> <li>• configure, update, and manage a SiteProtector system</li> <li>• configure, update, and manage other IBM ISS products such as Desktop Protector agents, scanners, appliances, and sensors</li> <li>• create and manage security policies and responses</li> <li>• set up, organize, and manage groups for the IT assets that a SiteProtector system monitors</li> <li>• set up users and user permissions</li> <li>• monitor security events and vulnerabilities on your network</li> <li>• run and schedule command jobs such as scan jobs, product updates, and database maintenance jobs</li> <li>• generate reports</li> <li>• generate tickets</li> </ul>
Databridge	<p>Enables the SiteProtector system to collect and display security data from older IBM ISS products such as System Scanner vulnerability assessment application or from third-party systems.</p>
Deployment Manager	<p>A Web-based application that can be used to install a SiteProtector system and other IBM ISS products from a central location on your network.</p>
Event Archiver	<p>Archives security events to a remote location.</p>
Event Collector	<p>Gathers security data generated by the IBM ISS products and sends it to the Site Database for processing. After processing, the data can be viewed in the SiteProtector Console. The Event Collector also sends unprocessed security data to the Event Viewer.</p>

**Table 4:** *SiteProtector system component descriptions*

Component	Description
Event Viewer	Provides an alternate interface for viewing security events. The Event Viewer receives the unprocessed events directly from the Event Collector. This interface is used primarily for troubleshooting. IBM ISS recommends that you use the Console for most security management tasks.
Site Database	Stores the following information: <ul style="list-style-type: none"> <li>• security data generated by your IBM ISS products</li> <li>• statistics for security events</li> <li>• group information</li> <li>• command and control data</li> <li>• the XPU status of all agents</li> <li>• SiteProtector system user accounts and permissions</li> <li>• tickets</li> <li>• customized views, reports, and other settings</li> </ul>
SiteProtector Application Server	Facilitates communication between the SiteProtector Console and all other agents. The Application Server makes it possible for multiple Consoles to perform the following functions: <ul style="list-style-type: none"> <li>• communicate with the SiteProtector Database</li> <li>• monitor and manage the same set of Event Collectors and agents</li> </ul> <p><b>Note:</b> The Application Server includes the Sensor Controller and the integrated X-Press Update Server. These three components are installed together automatically on the same computer. These three components are totally integrated and cannot be separated. You can deploy additional stand-alone X-Press Update Servers.</p>
Sensor Controller	Facilitates command and control between the Console and all other agents. For example, it relays commands from the Console to the Network Internet Scanner such as start and stop scan. <p><b>Note:</b> The Sensor Controller is integrated with the Application Server. The Sensor Controller is installed automatically with the Application Server on the same computer automatically. These components are totally integrated and cannot be separated.</p>
X-Press Update Server	The primary tool for updating the SiteProtector system and the other IBM ISS products that work with it. The X-Press Update Server does the following: <ul style="list-style-type: none"> <li>• connects to the IBM ISS download center</li> <li>• downloads software updates</li> <li>• provides the updates to a SiteProtector system where they can be distributed and applied to a SiteProtector system and other integrated IBM ISS products</li> </ul> <p><b>Note:</b> The X-Press Update Server is integrated with the Application Server. The integrated X-Press Update Server is installed together with the Application Server on the same computer automatically. These components are totally integrated and cannot be separated. You can deploy additional stand-alone X-Press Update Servers.</p>

Table 4: SiteProtector system component descriptions (Continued)



---

---

Component	Description
Web Console	A read-only, Web-based interface that provides access to limited SiteProtector system functionality. The Web Console is used primarily for monitoring SiteProtector system assets and security events.

---

---

**Table 4:** *SiteProtector system component descriptions (Continued)*

## Additional Modules for a SiteProtector System

**Introduction** This topic describes the additional modules you can purchase to extend the functionality of a SiteProtector system.

**Note:** The SiteProtector system interface refers to additional modules as agents.

**Module descriptions** Table 5 describes the additional SiteProtector system modules.

Module	Description
SecurityFusion module	<p>This add-on module provides you with the ability to do the following:</p> <ul style="list-style-type: none"> <li>conduct impact analysis on security events</li> <li>conduct attack pattern recognition</li> </ul> <p><b>Reference:</b> See the <i>SiteProtector SecurityFusion Module Guide</i>.</p>
Third Party Module	<p>This add-on module provides you with the ability to do the following:</p> <ul style="list-style-type: none"> <li>retrieve security events and other data from third-party firewalls</li> <li>view the security events and other data in the Console</li> <li>associate security events with specific firewalls</li> </ul> <p><b>Reference:</b> See the <i>SiteProtector Third Party Module Guide</i>.</p>
Reporting Module	<p>This add-on module provides you with the ability to generate a very wide range of reports in a variety of formats, including the following:</p> <ul style="list-style-type: none"> <li>Vulnerability Assessment reports</li> <li>Attack Activity reports</li> <li>User Audit reports</li> <li>Content Filtering reports</li> <li>User Permission reports</li> </ul> <p>Reference: See “Setting Up the Reporting Module” on page 319.</p>
SecureSync Module	<p>This add-on module provides you with the ability to do the following:</p> <ul style="list-style-type: none"> <li>transfer Site data between primary and back-up Sites</li> <li>transfer agent management from one Site to another.</li> </ul> <p>This feature is used to implement a failover system.</p> <p><b>Reference:</b> See the <i>SiteProtector SecureSync Guide</i>.</p>

**Table 5:** *Descriptions of additional SiteProtector system modules*

## Chapter 2

# The SiteProtector System Setup Process

## Overview

**Introduction** After you have installed your SiteProtector system, you must complete the setup process. This chapter provides an overview of the SiteProtector system setup process.

- Goals** The goals of the SiteProtector system setup process are as follows:
- configure and update the SiteProtector system product
  - create groups for your network assets and the agents that monitor them in the SiteProtector Console
  - install, update, and configure IBM ISS agents to monitor your network assets and work with the SiteProtector system
  - configure and apply security policies and responses for the integrated IBM ISS agents to meet your security requirements
  - set up the network assets in the SiteProtector system that you want the agents to monitor and protect

- Assumptions** This process assumes the following:
- you have installed your SiteProtector system
  - you have not installed the other IBM ISS products that you want to use with your SiteProtector system

**In this chapter** This chapter contains the following topics:

Topic	Page
Stages of the Setup Process	20

## Stages of the Setup Process

### Introduction

The initial setup process provides a structured method for implementing, configuring, and integrating your SiteProtector system and your other IBM ISS products. This process is complex and incremental, meaning that some setup tasks cannot be performed until others have been completed. The setup process is divided into stages, and each stage has a specific purpose and goal. This topic provides an overview of the SiteProtector system setup process.

**Note:** This guide only describes the *best* approach for setting up the SiteProtector system. The guide does not address alternate setup methods.

### Related information

This guide provides an overview and checklist for each stage of the setup process. If you are an experienced SiteProtector system user or are using this guide only as a reference, then you can skip this information. Each chapter is designed to assist both users who are setting up a SiteProtector system for the first time and users who are using the guide as a product reference.

### Stages

Table 6 describes the stages of the SiteProtector system setup process.

Stage	Description
1	SiteProtector System Configuration and Updates: <ul style="list-style-type: none"> <li>• Configure the SiteProtector system components.</li> <li>• Update the SiteProtector system components.</li> <li>• Set up SiteProtector system users and permissions for the users.</li> </ul> <b>Reference:</b> See Part I, "Configuring and Updating a SiteProtector System" on page 23.
2	Group Setup: <ul style="list-style-type: none"> <li>• Develop a plan for organizing network assets and agents into groups.</li> <li>• Create the groups and subgroups to support the organizational plan.</li> <li>• Configure properties for the groups, such as membership rules and group-level permissions.</li> </ul> <b>Reference:</b> See Part II, "Setting Up Groups" on page 209.
3	Agent Setup: <ul style="list-style-type: none"> <li>• Install, update, and configure the other IBM ISS products (agents) that you want to use with SiteProtector system, such as Desktop Protection products, appliances, sensors, and scanners.</li> <li>• Verify that the products are registered and configured to work with your SiteProtector system.</li> </ul> <b>Reference:</b> See Part III, "Setting Up Agents" on page 255.
4	Policy Configuration: <ul style="list-style-type: none"> <li>• Configure security policies and responses for your agents.</li> <li>• Configure Central Responses.</li> <li>• Configure ticketing.</li> </ul> <b>Reference:</b> See the <i>SiteProtector System Policies and Responses Configuration Guide</i> .

**Table 6:** *Stages of SiteProtector system setup process*

Stage	Description
5	Asset Setup: <ul style="list-style-type: none"> <li>• Add critical network assets to your SiteProtector system that will be monitored by the agents.</li> <li>• Adjust asset grouping.</li> </ul> <b>Reference:</b> See Part V, "Adding Assets" on page 293.

**Table 6:** *Stages of SiteProtector system setup process (Continued)*

## Next steps

After you have set up your SiteProtector system, you should install and configure any additional modules that you purchased.

- For information about using the Reporting Module, see the *SiteProtector System User Guide for Security Analysts*.
- For information about using SecurityFusion Module for extended security event analysis, see the *SiteProtector SecurityFusion Module Guide*.
- For information about using SecureSync for failover, see the *SiteProtector - SecureSync Guide*.
- For information about using Third Party Module to display firewall events from third party firewalls in your SiteProtector system, see the *SiteProtector Third Party Module Guide*.



# Configuring and Updating a SiteProtector System





## Chapter 3

# The Configuration and Update Stage

## Overview

### Introduction

The first stage in setting up your SiteProtector system is the Configuration and Update stage. In this stage, you configure the SiteProtector system components, update the components to the latest versions, and set up SiteProtector system users. This chapter provides an overview of the SiteProtector system configuration and update stage.

The procedures in this stage are intended to configure and update the components that comprise a SiteProtector system, such as the Agent Manager, X-Press Update Server, and the Site Database.

**Reference:** For information about configuring and updating other products that work with a SiteProtector system, such as Network Sensor and Network Internet Scanner, see Part III, “Setting Up Agents” on page 255.

### In this chapter

This chapter contains the following topics:

Topic	Page
Overview of this Stage	26
Checklist for this Stage	27

## Overview of this Stage

### Introduction

This topic provides an overview of the Configuration and Update stage.

### Configuration

The SiteProtector system is designed with complex configuration options to meet your individual security requirements. When you configure your SiteProtector system for the first time, you must perform the configuration tasks in a specific sequence. If you do not follow this sequence during the initial setup, then some components might not be able to communicate properly with each other. The chapters in this part of the manual are organized according to the sequence you must follow when you configure and update a SiteProtector system.

**Note:** After you configure the SiteProtector system components the first time, you can change these configuration settings to meet your security needs.

### Updates

IBM ISS regularly releases updates for the SiteProtector system. Some updates might have been released since you installed the product. IBM ISS recommends that you update your SiteProtector system as soon as possible in the initial setup process to ensure that you have the most current and secure versions of the software. These updates do not affect your configuration settings.

The X-Press Update Server must be configured and updated before you update the other SiteProtector system components because the XPU Server retrieves and delivers the updates.

**Note:** After you update the SiteProtector system components the first time, you should always apply the latest software updates as soon as they are released.

### SiteProtector system users

The SiteProtector system automatically grants full access to the user who has installed it. You should have this user perform all the initial setup tasks. If you have to delegate any of these tasks to other users, you must first set up the users in your SiteProtector system, and then give them the permissions required to perform those tasks.

**Important:** Managing permissions in your SiteProtector system is complicated. You should review the entire setup process before you delegate any setup tasks to additional users.

## Checklist for this Stage

### Introduction

This topic provides a checklist for configuring and updating your SiteProtector system.

### Checklist

Table 7 provides a task checklist to ensure that you perform all the tasks required to configure and update your SiteProtector system.

✓	Task
<input type="checkbox"/>	Start and configure the Console. See “Configuring the Console” on page 29.
<input type="checkbox"/>	Set up licenses and tokens for the following: <ul style="list-style-type: none"> <li>• your SiteProtector system</li> <li>• all the other IBM ISS products you plan to manage with your SiteProtector system</li> </ul> See “Setting Up Licenses” on page 49.
<input type="checkbox"/>	Configure Agent Managers. See “Configuring Agent Managers” on page 65.
<input type="checkbox"/>	Configure the X-Press Update Server(s). See “Configuring X-Press Update Servers” on page 71.
<input type="checkbox"/>	Update SiteProtector system components. See “Determining Update Status” on page 96.
<input type="checkbox"/>	Configure Event Collectors. See “Configuring Event Collectors” on page 121.
<input type="checkbox"/>	Enable the Event Viewer. See “Enabling the Event Viewer” on page 127.
<input type="checkbox"/>	Configure Site Database maintenance. See “Configuring the Site Database” on page 131.
<input type="checkbox"/>	Add users and groups to SiteProtector system User Groups. See “Configuring User Permissions” on page 151.
<input type="checkbox"/>	Configure Event Archiver. See See “Configuring the Event Archiver” on page 173.

**Table 7:** Checklist for configuring and updating your SiteProtector system



## Chapter 4

# Configuring the Console

## Overview

### Introduction

The chapter provides information about configuring Console options. The options you set in this chapter apply to any Site you access with the Console. You cannot set different Console options for different Sites.

**Note:** The Console is designed to operate without any custom configuration, so configuring the Console is optional. If the default Console settings accommodate your requirements, then you can skip the tasks in this chapter.

### In this chapter

This chapter contains the following sections:

Topic	Page
Setting General Options	30
Setting Logging Options	32
Setting Documentation Options	33
Setting Browser Options	35
Setting Global Summary Options	36
Setting Notifications Options	37
Setting Report Options	38
Setting Authentication Options	39
Setting Summary Options	40
Setting Asset View Options	44
Setting Ticket Options	45
Setting Agent View Options	46
Setting Analysis View Options	47

## Setting General Options

### Introduction

You can set general options in your SiteProtector system to control Console behavior, such as the default view that appears when you start the Console, the default time zone, and the default time format.

### Procedure

To set general options:

1. Start the Console, and then select **Tools** → **Options**.

The Options window appears.

2. Select **General** in the left pane.
3. Set the following General options:

Option	Description
Restore tabs from previous session OR Open default view	Opens the tabs that were open at the end of the previous session  Specifies the tab to open by default when you start the Console
Time Zone	Specifies the time zone
Time Format	Specifies the date/time format in selection fields throughout the Console <b>Note:</b> Time format does not affect date/time format in portlets in the Summary view.
Prompt before console exit	Select whether you want your SiteProtector system to prompt you each time you try to exit the Console.
Include subgroups	Select this option if you want your SiteProtector system to display data for the group and any subgroups in the group.
Show Alert Con / refresh every	Select this option if you want your SiteProtector system to display the AlertCon condition. The drop-down menu allows you to set the refresh interval. Your changes take effect the next time you access your SiteProtector system.
Show message regarding View permission on Site Group	Select this option if you want your SiteProtector system to display "permission denied" information regarding the current site group.
Set cell select mode in edit menu default to on	Allows you to select a single cell at a time, instead of selecting the entire row in a table

4. Select **Tables** in the left pane, and then select the following Table options:

Option	Description
Maximum number of rows to display	Specifies the number of data rows displayed in the main pane of the Console
Font size	Specifies the font size of data displayed in the main pane of the Console

Option	Description
Show grid lines	Displays grid lines in the main pane of the Console <b>Tip:</b> Click the sample grid box to select a grid color.

5. Select **Auto Refresh** in the left pane.

**Note:** The options for automatically refreshing data apply to every tab except the **Policy** tab.

6. Select the following Auto Refresh options:

Option	Description
Refresh Interval	How often to refresh the data in the Console automatically
Enable automatic refresh by default when opening a new tab	Enables automatic refresh globally
When auto refresh is enabled	Specifies one of the following: <ul style="list-style-type: none"> <li>• <b>Only refresh active consoles:</b> Refreshes data in active Consoles only</li> <li>• <b>Always refresh active, inactive, and minimized consoles:</b> Refreshes data for the console in any state of activity</li> </ul>

7. Click **Apply**, and then click **OK**.

## Setting Logging Options

**Introduction** You can set logging options to control how your SiteProtector system handles logging.

**Procedure** To set logging options:

1. Start the Console, and then select **Tools** → **Options**.

The Options window appears.

2. Select **Logging** in the left pane.
3. If you want to use a different log file for the text version of the log file, type or browse to the **Log Filename**.

**Note:** You must also select the **Text File** check box to use the log file.

4. Select a log level:

Log Level	Description
Fatal	Log only fatal messages.
Error (default)	Log error and fatal messages.
Warn	Log warn, error, and fatal messages.
Info	Log info, warn, error, and fatal messages.
Debug	Log debug and all other levels of tracing. <b>Important:</b> This level produces a high volume of messages.
All	Log all messages.

**Caution:** Change the log level only when you are troubleshooting an issue with the help of IBM ISS Technical Support.

5. Select the output format(s) to use for the log:

Option	Description
Standard Output	Sends log information to the standard output device of the operating system.
Text File	Sends log information to the specified text file.

6. (Optional) To set the Root Logger level or output type for a specific area of the Console, click **Advanced**.
7. Click **Apply**, and then click **OK**.



# Setting Documentation Options

## Introduction

By default, detailed security information and user documents are stored on the IBM ISS Web site. If you prefer to provide access to those documents locally, you must perform the tasks and configure your preferences as described in this topic.

## Task overview

This topic covers the following tasks:

Task	Description
1	Store security information locally
2	Store user documents locally
3	Set documentation preferences

## Storing security information locally

To store security information locally:

1. Download the security information zip file (XForceHelpFiles.zip) from [http://www.iss.net/security\\_center/reference/vuln/](http://www.iss.net/security_center/reference/vuln/) to your local drive.
2. Unzip the file.
3. Specify the path of the folder as described in the procedure below.

## Storing user documents locally

To access security information locally:

1. Download the SiteProtector Service Pack Documentation Bundle zip file from <http://www.iss.net/support/documentation> to your local drive.
2. Unzip the file into the SiteProtector Application Server root directory, which is typically  
`\Program Files\ISS\RealSecure SiteProtector\Application Server`
3. Specify the path of the folder as described in the procedure below.

## Setting documentation preferences

To set documentation preferences:

1. Start the Console, and then select **Tools** → **Options**.  
The Options window appears.
2. Select **Documentation** in the left pane.
3. In the **Location of Security Information** section, select one of the following the locations:

Location	Description
Local directory	Select this location if you want to store and access security information locally, and then specify the path.
Remote URL	Select this location if you want to access security information from a remote location, and then specify the URL. <b>Note:</b> The default URL is as follows: <a href="http://www.iss.net/security_center/reference/vuln">http://www.iss.net/security_center/reference/vuln</a> .

4. In the **Location of Documentation** section, select one of the following locations:

<b>Location</b>	<b>Description</b>
On SiteProtector Server	Select this location if you want to store and access SiteProtector documentation from the SiteProtector Server, and then type the address of the application server in the following format:  <b>https://</b> <i>application_server_IP_address_or_DNS_name:3994/</i>
On www.iss.net	Select this location if you want to access SiteProtector documentation from the IBM ISS Product Documentation Web site.

5. Click **Apply**, and then click **OK**.

# Setting Browser Options

## Introduction

If a proxy server is between your console and the application server, you must configure that proxy server in the Proxy tab in your SiteProtector system.

**Note:** If a network connection is attempted within a browser window, the browser uses the proxy settings defined in the browser's properties to establish the connection.

## Procedure

To set proxy options:

1. Start the Console, and then select **Tools** → **Options**.

The Options window appears.

2. Select **Browser** in the left pane.
3. Select the **Use Proxy** option, and then specify the following options:

Option	Description
Proxy Host	Name of the host used by the proxy sever.
Proxy Port	Port used by the proxy server.

4. (Optional) Choose an option for displaying Proventia Network ADS content:

Option	Description
View browser links in a new window	Enables the Console to open ADS content in a separate browser window
Open links in existing browser tabs	Enables the Console to open ADS content in an existing browser tab <b>Note:</b> If you have selected to open links in existing browser tabs, when you open new ADS content, it replaces ADS content previously opened in the same tab.

5. Click **Apply**, and then click **OK**.

## Setting Global Summary Options

### Introduction

Use global summary options to specify what you want to see in the Summary tab when you open the Console.

### Procedure

To set global summary options:

1. Start the Console, and then select **Tools** → **Options**.

The Options window appears.

2. Select **Global Summary** in the left pane.
3. Select what you want to see in the Summary tab when you start the Console:

Option	Description
What's New in SiteProtector	Displays information about new functionality in the SiteProtector system
IBM Internet Security Systems homepage	Displays the IBM ISS Web site
Custom location	Displays a Web site that you specify

4. Click **Apply**, and then click **OK**.

# Setting Notifications Options

**Introduction** Use Notifications options to specify the type and severity of notifications to display in the Console and to configure e-mail alerts for Critical or High severity notifications.

**Procedure** To set notifications options:

1. Start the Console, and then select **Tools** → **Options**.  
The Options window appears.
2. Select **Notifications** in the left pane.
3. Select the **Console** tab, and then select at least one Severity.
4. Select the **Email** tab, and then select the Site for which you want to configure email notifications.
5. If you want to send an email for every Critical or High severity notification, select the **Send an email for every Critical or High severity notification** check box, and then complete the following fields:

Options	Description
SMTP Server	The name of your local mail server name
System Email	The full email address used by the system

6. If the email addresses you want to send the notifications to are already configured in the User Email Addresses window, select them from the **Select SiteProtector User email addresses** list.
7. If you want to send notifications to email addresses that are not configured in the User Email Address window, type them in the **Type additional email addresses here** box.
8. Click **Apply**, and then click **OK**.

## Setting Report Options

**Introduction** Use Report options to include your company logo on reports.

**File requirements** Observe the following requirements for your logo image file:

- You can have only one image per Site.
- The image can be in jpg, png, or bmp format.
- The image should be 240 pixels in width by 96 pixels in height.
- If the image exceeds the pixel dimensions, the SiteProtector system can resize the image.

**Procedure** To set report options:

1. Start the Console, and then select **Tools** → **Options**.  
The Options window appears.
2. Select **Report** in the left pane.
3. Select the Site for which you want to configure a report logo from the list.
4. Browse to the file with your company logo.
5. Click **Apply**, and then click **OK**.

---

# Setting Authentication Options

## Introduction

Use Authentication options if your Site requires a user certificate to log on to your SiteProtector system. The certificate may be from a Windows store or from a smart card.

**Note:** Authentication options affect the fields that appear in the Logon to SiteProtector window. Your SiteProtector system administrator should know how to configure the options for your Site.

## Configuring two-factor authentication

If you need information about setting up two-factor authentication for SiteProtector system Console users, see the *SiteProtector System Two-Factor Authentication Guide* available at <http://www.iss.net/support/documentation>.

## Procedure

To set authentication options:

1. Start the Console, and then select **Tools** → **Options**.  
The Options window appears.
2. Select **Authentication** in the left pane.
3. Do one of the following:
  - If you use the standard Windows certificate store, select **Local windows certificate store**, and then skip to the last step.
  - Select **Smart card**.
4. Specify the location of your card reader's PKCS#11 library that the console needs to communicate with the smart card.  
**Note:** Check the documentation for your card reader to find the location of the library.
5. If you need to enter the personal identification number (PIN) for the smart card in the Logon to SiteProtector window, select the **Use login dialog field to enter pin** check box.  
**Note:** Do not select this check box if the smart card provides a keypad or its own window for the PIN.
6. Click **Apply**, and then click **OK**.

## Setting Summary Options

### Introduction

This topic provides information about settings summary view options.

### Summary information

Table 8 describes the information that you can display on the Summary view.

Information	Displays the following information:
Agent Event History by Day	<p>Displays a bar graph that illustrates the following information:</p> <ul style="list-style-type: none"> <li>total number of high priority security events by day</li> <li>total number of medium priority security events by day</li> <li>total number of low priority security events by day</li> <li>total number of all security events by day</li> </ul> <p>Provides navigation to the Analysis View (Event Analysis - Details) by clicking on the graph (High/Med/Low) or the days (Sun, Wed, Thurs, etc.) and prepopulates the Severity and Date filters</p>
Agent Event History by Month	<p>Displays a bar graph that illustrates the following information:</p> <ul style="list-style-type: none"> <li>total number of high priority security events by month</li> <li>total number of medium priority security events by month</li> <li>total number of low priority security events by month</li> <li>total number of all security events by month</li> </ul> <p>Provides navigation to the Analysis View (Event Analysis - Details) by clicking on the graph (High/Med/Low) or the days (Sun, Wed, Thurs, etc.) and prepopulates the Severity and Date filters</p>
Agent Event History by Week	<p>Displays a bar graph that illustrates the following information:</p> <ul style="list-style-type: none"> <li>total number of high priority security events by week</li> <li>total number of medium priority security events by week</li> <li>total number of low priority security events by week</li> <li>total number of all security events by week</li> </ul> <p>Provides navigation to the Analysis View (Event Analysis - Details) by clicking on the graph (High/Med/Low) or the days (Sun, Wed, Thurs, etc.) and prepopulates the Severity and Date filters</p>
Available Updates	<p>The number of updates in the following categories:</p> <ul style="list-style-type: none"> <li>Security content updates for SiteProtector system agents and for other agents</li> <li>Product maintenance updates for SiteProtector system agents and for other agents</li> <li>Product feature updates for SiteProtector system agents and for other agents</li> </ul>
Offline/Stopped Agents	<p>Shows the number of offline or stopped agents, by group, with navigation to the Agent tab. Data is shown for the selected group and up to two levels of subgroups</p>
Scan Progress	<p>Shows the number of scan jobs currently in progress and provides a link to the Properties tab for the Site where you can view all command jobs for the Site.</p>

**Table 8:** Information in the Summary view



Information	Displays the following information:
Site/[Group] Summary	<ul style="list-style-type: none"> <li>• Name of the Site (may be the IP address of the Site Host)</li> <li>• Site port</li> <li>• Asset Count</li> <li>• Number of agents in the Site and how many are active</li> </ul> <p><b>Note:</b> The SiteProtector system displays Site Summary information if you have selected a Site in the left pane and Group Summary information if you have selected a Group in the left pane.</p>
[Site]/Group Summary	<ul style="list-style-type: none"> <li>• Group Name</li> <li>• Group Description</li> <li>• Asset Count</li> <li>• Number of agents in the Group and how many are active</li> </ul> <p><b>Note:</b> The SiteProtector system displays Group Summary information if you have selected a Group in the left pane and Site Summary information if you have selected a Site in the left pane.</p>
System Health	<ul style="list-style-type: none"> <li>• The number of components that are unhealthy, healthy, and have a warning</li> <li>• Provides a link to the Health Summary tab of each agent that has a warning</li> <li>• Provides a link to the Agent tab for the Site where you can view detailed information for each agent, but only if all components are healthy</li> </ul>
Ticket Status	<ul style="list-style-type: none"> <li>• Displays the total number of critical, high, medium, and low priority tickets by status</li> </ul> <p>Provides navigation to Ticket view with Severity and Status filters set</p>
Today's Event Summary by Event Name	<p>Lists all security events for the current day by Event Name and Severity and provides navigation to the Analysis View, Event Analysis - Details</p>
Today's Event Summary by Source	<p>Lists all security events for the current day by source IP address and provides the following information for each event:</p> <ul style="list-style-type: none"> <li>• source IP address of the security event</li> <li>• number of high priority security events on the source IP address</li> <li>• number of medium priority security events on the source IP address</li> <li>• number of low priority security events on the source IP address</li> <li>• total number of security events in all priority categories for the source IP address</li> </ul> <p>Provides navigation to Analysis tab with Severity, Source, and Date filters set</p>

**Table 8:** Information in the Summary view (Continued)

Information	Displays the following information:
Today's Event Summary by Target	<p>Lists all security events for the current day by target IP address and provides the following information for each event:</p> <ul style="list-style-type: none"> <li>target IP address of the security event</li> <li>number of high priority security events on the target IP address</li> <li>number of medium priority security events on the target IP address</li> <li>number of low priority security events on the target IP address</li> <li>total number of security events in all priority categories for the target IP address</li> </ul> <p>Provides navigation to Analysis tab with Severity, Target, and Date filters set</p>
Vulnerability History by Day	<p>Displays a bar graph that illustrates the following information:</p> <ul style="list-style-type: none"> <li>total number of high priority vulnerabilities by day</li> <li>total number of medium priority vulnerabilities by day</li> <li>total number of low priority vulnerabilities by day</li> <li>total number of all vulnerabilities by day</li> </ul> <p>Provides navigation to Analysis view (Vuln Analysis - Details) with Severity and Date filters set</p>
Vulnerability History by Month	<p>Displays a bar graph that illustrates the following information:</p> <ul style="list-style-type: none"> <li>total number of high priority vulnerabilities for the month</li> <li>total number of medium priority vulnerabilities for the month</li> <li>total number of low priority vulnerabilities for the month</li> <li>total number of all vulnerabilities for the month</li> </ul> <p>Provides navigation to Analysis view (Vuln Analysis - Details) with Severity and Date filters set</p>
Vulnerability History by Week	<p>Displays a bar graph that illustrates the following information:</p> <ul style="list-style-type: none"> <li>total number of high priority vulnerabilities by week</li> <li>total number of medium priority vulnerabilities by week</li> <li>total number of low priority vulnerabilities by week</li> <li>total number of all vulnerabilities by week</li> </ul> <p>Provides navigation to Analysis view with Severity and Date filters set</p>
Vulnerability Summary by OS	<p>Lists vulnerabilities for each operating system and provides the following information for each operating system:</p> <ul style="list-style-type: none"> <li>total number of high priority vulnerabilities on the operating system</li> <li>total number of medium priority vulnerabilities on the operating system</li> <li>total number of low priority vulnerabilities on the operating system</li> <li>total number of vulnerabilities in all categories on the operating system</li> </ul> <p>Provides navigation to Analysis view (Vuln Analysis - Target OS) with Severity and OS filters set</p>

**Table 8:** Information in the Summary view (Continued)

## Procedure

To set summary options:

1. Start the Console, and then select **Tools** → **Options**.

The Options window appears.

2. Select **Summary** in the left pane.
3. Do one of the following if you want your SiteProtector system to automatically update the content displayed when you change a group:
  - If you do want your SiteProtector system to automatically update the content displayed when you change a group, then select the **Update Content on Group Change** option.
  - If you do not want your SiteProtector system to automatically update the content displayed when you change a group, then clear the **Update Content on Group Change** option.
4. In the **Available** section, select the items you want to display on the Summary page, and then click **Add**.

The **Displayed** section shows the items that will appear on the Summary tab. The items will appear in the order listed.
5. Repeat Steps 1 through 4 until the **Display** section includes all the items you want to display on the Summary view.
6. Click **Apply**, and then click **OK**.

## Setting Asset View Options

**Introduction** The Asset view displays information about the assets in a group. You can customize the Asset view and save your custom settings in an *assetview.xml* file.

**Procedure** To set Asset view options:

1. Start the Console, and then select **Tools** → **Options**.  
The Options window appears.
2. Select **Asset** in the left pane.  
The Asset view options appear.
3. Do one of the following if you want your SiteProtector system to automatically update the content displayed when you change a group:
  - If you do want your SiteProtector system to automatically update the content displayed when you change a group, then select the **Update Content on Group Change** option.
  - If you do not want your SiteProtector system to automatically update the content displayed when you change a group, then clear the **Update Content on Group Change** option.
4. In the **Asset Default View** section, select the Asset view that you want to use.  
**Note:** The default view is *factory-default.xml*. Custom views that you create are included in this list.
5. In the **Risk Index** section, set the **Show Vulnerabilities for the Past** option.
6. Click **OK**.

# Setting Ticket Options

**Introduction** Use the ticket options to change the default view for the **Ticket** tab.

**Procedure** To set Ticket default view:

1. Start the Console, and then select **Tools** → **Options**.

The Options window appears.

2. Select **Ticket** in the left pane.
3. In the **Ticket Default View** list, select the Ticket view that you want to use.

**Note:** The default view is `factory-default.xml`. Custom views that you create are included in this list.

4. Click **OK**.

## Setting Agent View Options

**Introduction** The Agent view displays information about the agents in a group. You can customize the Agent view and save your custom settings in an *agentview.xml* file.

**Procedure** To set Agent view options:

1. Start the Console, and then select **Tools** → **Options**.  
The Options window appears.
2. Select **Agent** in the left pane.  
The Agent view options appear.
3. Do one of the following if you want your SiteProtector system to automatically update the content displayed when you change a group:
  - If you do want your SiteProtector system to automatically update the content displayed when you change a group, then select the **Update Content on Group Change** option.
  - If you do not want your SiteProtector system to automatically update the content displayed when you change a group, then clear the **Update Content on Group Change** option.
4. In the **Agent Default View** section, select the Agent view that you want to use.  
**Note:** The default view is *factory-default.xml*. Custom views that you create are included in this list.
5. Click **OK**.

---

# Setting Analysis View Options

**Introduction**      The Analysis view displays information such as security events related to the assets in a group.

**Procedure**      To set Analysis view options:

1. Start the Console, and then select **Tools** → **Options**.

The Options window appears.

2. Select **Analysis** in the left pane.

The Analysis view options appear.

3. Do one of the following:

- If you want your SiteProtector system to automatically update the content displayed when you change a group, then select the **Update Content on Group Change** option.
- If you do not want your SiteProtector system to automatically update the content displayed when you change a group, then clear the **Update Content on Group Change** option.

4. Click **Apply**, and then click **OK**.





## Chapter 5

# Setting Up Licenses

## Overview

- Introduction** This chapter provides information about setting up licenses for your SiteProtector system and the other IBM ISS products that you want to use with the SiteProtector system.
- Requirement** You *must* set up licenses and tokens for your SiteProtector system and other IBM ISS products as soon as possible in the initial setup process. Otherwise, you will not be able to use the full capabilities of your SiteProtector system or perform all the tasks described in this guide.
- Archiving licenses** In the event that you have to reinstall and reconfigure your SiteProtector system, IBM ISS strongly recommends that you archive your licenses in a safe, remote location as soon as you receive them from IBM ISS.
- In this chapter** This chapter contains the following topics:

Topic	Page
What are Licenses?	50
What are OneTrust Tokens and OneTrust Licenses?	52
Proventia OneTrust Licensing	53
Processes for Using OneTrust Licenses	55
Downloading OneTrust Licenses	56
Working with OneTrust Tokens	59
Obtaining Agent and Desktop Licenses	61
Adding and Removing Agent or Desktop Licenses	62

## What are Licenses?

### Introduction

A license is issued to you for each IBM ISS purchase. The license verifies your right to use the product. The license contains the following information:

- the period of time that you can use the product
- the number of agents by type that you can use
- the number of IP addresses that you can scan with Network Internet Scanner
- the maintenance expiration date for the product (maintenance allows you to get updates for the product)

**Note:** You must renew all maintenance dates yearly. If you do not renew your maintenance date, then you cannot get updates for the product after the expiration date.

### Types

IBM ISS issues different types of licenses depending on the product you purchase.

Table 9 describes the types of licenses that a SiteProtector system supports.

Type	Description	Components and Products
OneTrust License	An alphanumeric ID, called a token, is associated with your IBM ISS customer ID, and that identifies your OneTrust licenses. <b>Note:</b> If you have an earlier type of license for a product and you also have a OneTrust license for that product, your SiteProtector system uses the OneTrust license.	Issued for SiteProtector system components and for Proventia Network Enterprise Scanner
	A serial number on an appliance that enables the appliance to download licenses	SiteProtector system SP1001 appliance
Agent License	A file that contains the license key and other license information. The file has one of the following extensions: <ul style="list-style-type: none"> <li>• <code>.key</code> (a text file that contains the license key and other license information) <b>Example:</b> <code>IS500.key</code></li> <li>• <code>.isslicense</code> (a text file that contains the license key and other license information) <b>Example:</b> <code>ISSInternetScanner.isslicense</code></li> </ul>	Issued for all IBM ISS products <i>except</i> the following: <ul style="list-style-type: none"> <li>• RealSecure Desktop 7.0</li> <li>• Proventia Network Enterprise Scanner</li> </ul>
Desktop License	An alphanumeric license key <b>Example:</b> <code>ABCabc123A1B2C3aBcCb1</code>	Issued for RealSecure Desktop 7.0

**Table 9:** *Types of licenses and the component and products for which they are issued*

**Separate licenses** IBM ISS accepts separate license files for the following:

**IBM ISS Products:**

- RealSecure Network Gigabit
- RealSecure Server Sensor
- Internet Scanner software
- RealSecure Desktop
- Proventia Desktop
- Proventia Network IDS
- Proventia Network IPS
- Proventia Network MFS

**License requirement for updates**

Before you can update any SiteProtector system components, you must set up at least one license in your SiteProtector system.

## What are OneTrust Tokens and OneTrust Licenses?

### Introduction

The topic provides information about OneTrust tokens and OneTrust licenses and how these items are used with Proventia OneTrust licensing.

### Tokens

The OneTrust token is an alphanumeric ID that IBM ISS distributes to you if you buy one of the following products:

- SiteProtector system (used for the X-Press Update Server and Event Archiver components)
- Network Enterprise Scanner

The token is associated with your OneTrust license at IBM ISS.

### Licenses

The OneTrust license contains the following information:

- the list of products that you have purchased
- the quantity of each product
- the maintenance plan expiration dates for the products
- the usage expiration for the products

The information in the license is encrypted. A SiteProtector system extracts and decrypts this information and displays it for you in the Console. As you purchase new products, your SiteProtector system automatically updates the information displayed in the Console.

### Multiple tokens

Typically, you can expect to have one customer ID and one token. In some cases, your company might purchase products separately for different divisions within your organization. In this case, IBM ISS issues different customer IDs and tokens for the different divisions. The result is that you might have multiple tokens in your SiteProtector system for the different divisions. However, there can be only one license file that contains all licenses for this Site.

# Proventia OneTrust Licensing

## Introduction

Proventia OneTrust licensing is the latest licensing system for IBM ISS products. The following SiteProtector system components and IBM ISS agents use OneTrust licensing:

### SiteProtector components

- X-Press Update Server
- Event Archiver
- Reporting

### IBM ISS agent

- SiteProtector SP1001 appliance
- Proventia Network Enterprise Scanner

## Benefits

OneTrust licensing offers the following benefits:

- provides a single, simplified licensing process to acquire IBM ISS products
- decreases the time required to deploy IBM ISS products
- decreases the amount of license key management
- moves product usage and maintenance management to IBM ISS

## Previous licensing

Previous licensing required a separate license key for each IBM ISS product order. OneTrust licensing requires a single token.

## Access levels

Table 10 describes the four access levels.

Access Level	Description
Full Access	<p>This level provides the following:</p> <ul style="list-style-type: none"> <li>• licensed use of purchased products</li> <li>• access to all products and features<sup>a</sup></li> <li>• use of an unlimited quantity of purchased products</li> <li>• access to updates for purchased products</li> </ul> <p>This level has the following requirement:</p> <ul style="list-style-type: none"> <li>• the maintenance agreement on at least one product must be current</li> </ul>
Limited Access	<p>This level provides the following:</p> <ul style="list-style-type: none"> <li>• licensed use of purchased products</li> <li>• use of an unlimited quantity of purchased products</li> <li>• access to updates for purchased products</li> </ul> <p>This level has the following requirements:</p> <ul style="list-style-type: none"> <li>• the maintenance agreement on at least one product must be current</li> <li>• one of each purchased product type must be current</li> </ul>
No Access	This level provides no access to any products or product updates.

**Table 10:** Access level descriptions

Access Level	Description
Evaluation Access	<p>This level provides the following:</p> <ul style="list-style-type: none"><li>• access to all products and features</li><li>• use of an unlimited quantity of purchased products</li><li>• access to updates for purchased products</li></ul> <p>This access level has the following requirements:</p> <ul style="list-style-type: none"><li>• the maintenance agreement on at least one product must be current</li><li>• one of each purchased product type must be current</li><li>• you have 45 days of access only</li></ul>

**Table 10:** *Access level descriptions (Continued)*

- a. Some products might not be included because of third-party agreements, export compliance issues, or other factors.

## Processes for Using OneTrust Licenses

**Introduction** This topic describes the automatic and the manual processes for using OneTrust licenses.

**Process: automatic** Table 11 describes the automatic process for using OneTrust licensing.

Stage	Description
1	You purchase the OneTrust-enabled product.
2	IBM ISS generates the following information: <ul style="list-style-type: none"> <li>• a unique customer ID associated with the customer account</li> <li>• a unique token associated with the customer ID</li> <li>• a license associated with the customer ID</li> </ul>
3	You configure your SiteProtector system with your MyISS account or product order number, and then your SiteProtector system downloads from IBM ISS and enters the token for you automatically.
4	Your SiteProtector system displays the license information in the Console.
5	You deploy the OneTrust-enabled product and register it with your SiteProtector system.
6	When you attempt to update the product, IBM ISS determines whether you can download updates for the product based on the license. This stage is performed at the IBM ISS Web server.

**Table 11:** *Automatic process for using OneTrust licensing*

**Process: manual** Table 12 describes the manual process for using OneTrust licensing.

Stage	Description
1	You purchase the OneTrust-enabled product.
2	IBM ISS generates the following information: <ul style="list-style-type: none"> <li>• a unique customer ID associated with the customer account</li> <li>• a unique token associated with the customer ID</li> <li>• a license associated with the customer ID</li> </ul>
3	You use one of the following manual methods to obtain the token: <ul style="list-style-type: none"> <li>• Obtain the token from IBM ISS through email.</li> <li>• Use your “MyISS” account to download the token.</li> <li>• Use the Manual Upgrader to download the token.</li> </ul>
4	You manually enter the token.
5	You obtain the license manually from the IBM ISS Download Center and use the Import License feature to import the license to the correct location in your SiteProtector system.
6	Your SiteProtector system displays the license information in the Console.
7	You deploy the OneTrust-enabled product and register it with your SiteProtector system.

**Table 12:** *Manual process for using OneTrust licensing*

## Downloading OneTrust Licenses

### Introduction

This topic explains how to download OneTrust licenses.

### Methods

Table 13 describes the two methods for downloading OneTrust licenses.

Method	Description
Automatic	You can configure your SiteProtector system to contact IBM ISS and download your licenses automatically. This method requires Internet access for your SiteProtector system and one of the following: <ul style="list-style-type: none"> <li>• a token</li> <li>• a valid MyISS user name and password</li> <li>• a valid Onyx user name and password</li> </ul>
Manual	You can download a license with the Manual Upgrader, and then import the file into your SiteProtector system manually. This method requires the Manual Upgrader software and Internet access on the computer where the Manual Upgrader is installed.

**Table 13:** *Methods for downloading licenses*

### Automatically downloading licenses

To configure your SiteProtector system to download license updates automatically from the IBM ISS Download Center:

1. In the left pane, select *Site Node*.
2. Select **Tools** → **Licenses** → **OneTrust**.  
The OneTrust License Information window appears.
3. Select the **Licenses** tab, and then click **Download Options**.  
The Download Options window appears.
4. Select **Auto Download Licenses**, and then set the interval in hours that you want your SiteProtector system to check for license updates.
5. Click **OK**.
6. Select the **Licenses** tab, and then provide one of the following:
  - a token
  - a valid MyISS username and password
  - a valid Onyx username and password
 Your SiteProtector system uses this information to access the IBM ISS Download Center.
7. Click **OK**.



**Task overview: manually downloading licenses**

If your installation of your SiteProtector system does not have Internet access, then you can download your license with Manual Upgrader. Table 14 describes the tasks for manually downloading a license.

Task	Description
1	Download the license from IBM ISS with the Manual Upgrader. For more information about Manual Upgrader, including instructions for installing the software, See "Downloading Update Files with the Manual Upgrader" on page 111.
2	Import the license into your SiteProtector system.

**Table 14:** Tasks for manually downloading an license file

**Downloading licenses with Manual Upgrader**

To download a license with Manual Upgrader:

**Note:** To complete this procedure, you must have an agent license file.

1. Double-click `ManualUpgrader.exe`.
2. Did the Please select a valid IBM Internet Security Systems sensor or agent license file window appear?
  - If *yes*, go to Step 3.
  - If *no*, go to Step 6.
3. Locate and select a valid license file.  
The name of the file you select appears in the File name box.
4. Click **Open**.  
The EULA window appears.
5. Read and accept all licensing and export agreements.  
A Manual Upgrader alert window appears.
6. Do you want to receive a new catalog of available updates to the Web?
  - If *yes*, click **Yes**.
  - If *no*, click **Yes**.
7. In the Manual Upgrader menu bar, select **Licensing** → **Request a One Trust License**.  
The Token Requests window appears.
8. Do you want to manually enter your token?
  - If *yes*, type your token into the Manually enter a token box, and then click **Use Token**.
  - If *no*, type your user name and password in the section called Download a Token from IBM Internet Security Systems, and then click **Download Token**.
9. Repeat Step 8 for as many tokens as you want to enter.  
As you add tokens, the tokens are displayed in the **Current Token List** box.

10. To select the directory where you want to place your OneTrust license, click the ellipses (...) located to the right of the OneTrust License directory field, select a directory, and then click **OK**.

**Note:** You can skip this step to accept the current directory. The current directory is listed in the box called Onetrust License directory.

**Note:** You can store only one token file in a directory, but your token file can contain several tokens.

11. Click **Download OneTrust** License.

If the operation is successful, a message appears stating that the OneTrust License is received.

12. Import the license into your SiteProtector system.

For information about importing licenses into your SiteProtector system, see Importing licenses in this topic.

### **Importing licenses**

To import a license manually:

1. Copy the license directory that you want to import to your SiteProtector system Console.

**Note:** The “license directory” refers to the directory you specified in Step 10 of the procedure, “Downloading licenses with Manual Upgrader”, earlier in this topic.

2. Select **Tools** → **Licenses** → **OneTrust**.

The OneTrust License Information window appears.

3. Select the **License** tab, and then click **Remove**.

Your SiteProtector system removes any old license information.

**Note:** If no old license information exists in your SiteProtector system, the **Remove** button is not available. Go to the next step.

4. Click **Import**.

The Choose Import Directory window appears.

5. Navigate to the directory that contains your licenses, and then select **Open**.

Your license information appears in the Licenses tab.

6. Click **OK**.

---

# Working with OneTrust Tokens

## Introduction

This topic explains how to perform the following tasks:

- obtain tokens from IBM ISS
- add tokens to your SiteProtector system manually
- add tokens to your SiteProtector system automatically
- edit tokens
- delete tokens

**Note:** When you add, edit, or delete a token, the OneTrust license summary will reflect the changes.

## Requirement

You must add the required tokens to your SiteProtector system before you can download or view the contents of your OneTrust license in the Console.

## Obtaining tokens

To obtain your token, you can use one of the following methods:

- Send an email to [license@iss.net](mailto:license@iss.net).
- Log on to MyISS or Onyx with a valid user name and password, and then copy the token.
- Configure your SiteProtector system to contact the IBM ISS Download Center, and then download the token for you automatically.  
See “Adding tokens automatically” on page 60.
- Use the Manual Upgrader to download the tokens and licenses.

## Adding tokens manually

To add a token to your SiteProtector system manually:

**Note:** If your installation of your SiteProtector system does not have Internet access, then you must add tokens to your SiteProtector system manually. You must obtain your token before you perform this task.

1. In the left pane, select the *Site Node*.
2. Select **Tools** → **Licenses** → **OneTrust**.  
The OneTrust License Information window appears.
3. Select the **Licenses** tab, and then click **Add**.  
The Add Token(s) window appears.
4. Select the **Token** option.
5. Type the 32-digit **token number**, and then click **OK**.

**Important:** Make sure that you enter the token number correctly. Your SiteProtector system does not check the validity of the number you enter. If you enter the token number incorrectly, then the Summary tab does not show any licenses. Use the Edit button to reenter the token number correctly. You can use the copy and paste functionality to ensure that you enter the number correctly.

### Adding tokens automatically

To configure your SiteProtector system to download tokens automatically from the IBM ISS Download Center:

**Note:** If your installation of your SiteProtector system has Internet access, then you can configure your SiteProtector system to download tokens from the IBM ISS Download Center automatically. To use this feature, you must provide your SiteProtector system with a valid MyISS or Onyx user name and password.

1. In the left pane, select the *Site Node*.
2. Select **Tools**→**Licenses**→**OneTrust**.  
The OneTrust License Information window appears.
3. Select the **Licenses** tab, and then click **Add**.  
The Add Token(s) window appears.
4. Select the **IBM ISS User Name/ OCN Password** option.
5. Type a valid MyISS or Onyx user name and password, and then click **OK**.  
Your SiteProtector system contacts the IBM ISS Download Center, and then downloads your token to your SiteProtector system. After your SiteProtector system downloads your token, it uses the token (not your user name and password) for all future communications with the IBM ISS Download Center regarding licenses.

### Editing tokens

To edit a token:

1. In the left pane, select the *Site Node*.
2. Select **Tools**→**Licenses**→**OneTrust**.  
The OneTrust License Information window appears.
3. Select the **Licenses** tab
4. Select the token you want to edit, and then click **Edit**.  
The Edit Token(s) window appears.
5. Type the correct token number, and then click **OK**.

### Deleting tokens

To delete a token:

1. In the left pane, select the *Site Node*.
2. Select **Tools**→**Licenses**→**OneTrust**.  
The OneTrust License Information window appears.
3. Select the **Licenses** tab.
4. Select the token you want to edit, and then click **Remove**.  
Your SiteProtector system displays a confirmation message.
5. Click **Yes**.

# Obtaining Agent and Desktop Licenses

**Introduction** There are several ways to obtain agent and Desktop licenses with varying levels of security. You should use the most secure method available.

**Methods** Table 15 describes the methods for obtaining an agent or Desktop license.

Method	Description
Browser download	Download the license with your browser. This method takes advantage of the built-in Secure Sockets Layer (SSL) security in your browser.
Email	Request that IBM ISS send the license to you in an email with PGP encryption or without PGP encryption. If you want to use PGP encryption, then you must provide IBM ISS with your public PGP key to use this method. To make license request and provide keys, contact IBM ISS at licenses@iss.net.
Browser	Copy and paste the license from the text displays in the browser to your license repository.

**Table 15:** *Methods for obtaining licenses*

**Storing licenses** IBM ISS strongly recommends that you archive licenses in a secure, remote location separate from your SiteProtector system as soon as you receive them from IBM ISS. This practice ensures quick access to these items in the event that you must reinstall and reconfigure your SiteProtector system for any reason. If you misplace or lose your agent or Desktop licenses, then you must request and wait for new ones to be issued.

**Upgrade licenses** If you want to update from RealSecure Desktop 3.6 or 7.0 to Proventia Desktop, then you must contact IBM ISS to obtain an upgrade license. The upgrade license is issued as a license file. After you add the upgrade license to your SiteProtector system, you can download the full upgrade for the product.

**Note:** Licenses for RealSecure Desktop 3.6 or 7.0 were issued as alphanumeric license keys. The process to upgrade from one of these products to Proventia Desktop requires that the license key for Desktop 3.6 or 7.0 be converted from an alphanumeric license key to a license file. To facilitate the upgrade process, your SiteProtector system automatically converts the alphanumeric license key to a license file and saves it for you in the appropriate location.

**Obtaining tokens** For information about how to obtain tokens for Proventia Network Enterprise Scanner, X-Press Update Server, or Event Archiver, see “Working with OneTrust Tokens” on page 59.

## Adding and Removing Agent or Desktop Licenses

### Introduction

This topic explains how to add and remove the following types of licenses to your SiteProtector system:

- Agent and module licenses
- Desktop licenses

### Adding agent or module licenses

To add a license to your SiteProtector system for an agent or module:

1. In the left pane, select the *Site Node*.
2. Select **Tools**→**Licenses**→**Agent/Module**.  
The File-Based License Information window appears.
3. Select the **Licenses** tab, and then click **Add**.  
The Add License to SiteProtector window appears.
4. Navigate to the folder that contains the license you want to add, select the license file, and then click **OK**.  
**Note:** License key files have either a `.key` or `.isslicense` file extension.  
The End User License Agreement appears.
5. Click **Accept**.  
The license appears in the License tab.

### Removing agent and module licenses

To remove a license from your SiteProtector system for an agent or module:

1. In the left pane, select the *Site Node*.
2. Select **Tools**→**Licenses**→**Agent/Module**.  
The File-Based License Information window appears.
3. Select the **Licenses** tab.
4. Select the license you want to remove, and then click **Remove**.  
A confirmation message asks if you are sure you want to removes the license.
5. Click **Yes**.  
The license is removed.

### Adding desktop licenses

To add a desktop license to your SiteProtector system:

**Note:** Desktop licenses are used for RealSecure Desktop 7.0 products only.

1. In the left pane, select the *Site Node*.
2. Select **Tools**→**Licenses**→**RealSecure Desktop**.  
The RealSecure Desktop License Information window appears.
3. Click **Add**.  
The Add RealSecure Desktop License window appears.

4. Type the license key and description, and then click **OK**.

The Software License Agreement window appears.

5. Click **Accept**.

The license appears in the License tab.

### Removing desktop licenses

To remove a desktop license from your SiteProtector system:

1. In the left pane, select the Site Node.

2. Select **Tools** → **Licenses** → **RealSecure Desktop**.

The RealSecure Desktop License Information window appears.

3. In the License Key list, select the desktop license you want to remove, and then click **Remove**.

A confirmation message asks if you are sure you want to remove the license.

4. Click **Yes**.

The license is removed.





## Chapter 6

# Configuring Agent Managers

## Overview

### Introduction

Components and agents communicate with the SiteProtector system either through the Agent Manager or the Sensor Controller. This chapter explains procedures related to using the Agent Manager.

### Agents and components

The SiteProtector system regularly adds support for new agents. The following is a partial list of SiteProtector system components and agents that communicate with the Agent Manager:

- X-Press Update Server
- Event Archiver
- RealSecure Desktop 7.0 and Proventia Desktop
- Proventia Network IPS and Proventia Network MFS
- Proventia Server IPS and Proventia Server IPS for Windows
- Enterprise Scanner
- Proventia Network ADS

### Secure communication

To ensure secure communication between the components and the Agent Manager, set up Agent Manager accounts before you configure the other SiteProtector system components that communicate with the Agent Manager.

### In this chapter

This chapter contains the following topics:

Topic	Page
What is the Agent Manager?	66
Configuring Agent Manager Properties	67
Viewing Agent Manager Properties	68
Creating Agent Manager Accounts	69
Assigning Agent Managers to Agents	70

## What is the Agent Manager?

### Description

The Agent Manager provides the following functions for SiteProtector system components and agents:

- manages the various command and control activities
- facilitates data transfer to the Event Collector
- accepts heartbeats
- provides updates for Proventia Desktop and Proventia Server IPS for Windows

### Process

Table 16 describes the process for how SiteProtector system components and agents get policies and other important information from a SiteProtector system through the Agent Manager.

Stage	Description
1	The agent initiates a heartbeat to its Agent Manager.
2	The Agent Manager receives the heartbeat.
3	The Agent Manager compares the agent settings to its group settings to determine what data to send the agent.
4	The Agent Manager sends the agent the required data. The data sent can include any of the following: <ul style="list-style-type: none"> <li>• no data</li> <li>• policy changes</li> <li>• files the agent requested when the agent sees that it is out-of-date</li> <li>• policy changes and updates</li> </ul>

**Table 16:** *Process for communication between agents and Agent Managers*

### Heartbeat

A heartbeat is a scheduled request that includes the agent status and a request for the latest applicable policies. Poster-acceptor agents periodically send heartbeats to the Agent Manager, and the Agent Manager responds with any policies that have changed.

Heartbeats are encrypted HTTP or HTTPS requests. RealSecure Desktop 7.0 sends HTTP requests. All other poster-acceptor agents send HTTPS requests by default.

**Note:** Scheduled heartbeats do not affect security events.

---

# Configuring Agent Manager Properties

## Introduction

This topic explains how to configure Agent Manager properties. These settings control the following Agent Manager behaviors:

- how the Agent Manager installs Desktop Protection agents
  - how the Agent Manager reports events from Desktop Protection agents
  - how the Agent Manager responds when the connection with the Site Database is lost
  - how agents authenticate communication with the Agent Manager
- See “Creating Agent Manager Accounts” on page 69.

## Procedure

To configure Agent Manager properties:

1. In the left pane, select the *Site Node*.
2. In the view drop-down menu, select **Agent**.
3. In the right-pane, right-click **Agent Manager**, and then select **Properties** from the pop-up menu.  
The Agent Manager properties tab appears.
4. In the left pane, select **Agent Properties**, and then click **Edit Agent Properties** in the right pane.  
The Policy Editor appears.
5. Edit the following properties as needed:
  - Communication Settings
  - Diagnostic Settings
  - Database Connection Loss Actions
  - Accounts
  - Proventia Desktop Access Control**Note:** For instructions on how to edit these settings, see the Policy Editor help.
6. Click **Save**, and then from the **File** menu, select **Exit**.

## Viewing Agent Manager Properties

**Introduction** This topic provides information about viewing Agent Manager properties.

**Procedure** To view the properties for the Agent Manager:

1. In the left pane, select the *Site Node*.
2. In the **Go to** list, select **Agent**.
3. In the right pane, right-click the **Agent Manager**, and then select **Properties** from the pop-up menu.

The Properties tab displays the properties.

### Agent Manager property descriptions

Table 17 describes the Agent Manager properties.

Property	Description
License State	Indicates whether the license for the Agent Manager is valid, such as Key Good.
Sensor Status	Status of the Agent Manager, such as Active.
Event Collector Connection Status	Status of the Agent Manager connection to its Event Collector, such as Online.
Version	Version of the Agent Manager, such as 6.9 (SP 7.1).
XPU Status	Status of the software version, such as Current.
Last Installed XPU	Version of the last software update installed, such as SP 7.1.
Event Collector Assigned	Name of the Event Collector assigned to the Agent Manager, such as <i>ComputerName_EventCollector</i> .
Event Collector Keys Installed	Indicates whether the required encryption keys from the Event Collector are installed on the Agent Manager, such as Yes.
XPU Date	Date and time the last software update was installed, such as October 1, 2005 1:00PM.
Option Flag	Option flag set for the Agent Manager, such as Default.
Logging Level	Indicates the type of information created in the log files for the Agent Manager, such as Informational.
Event Port	The event port that the Agent Manager uses for communication, such as 914.
Control Port	The control port that the Agent Manager uses, such as Default.
Master Console	The name of the Console assigned Master Status.
Control Channel	The status of the control channel, such as Closed.
Engine UUID	The identification for the engine.
Last Modified by	The name of the component that last modified the Agent Manager and the date and time of the modification.

**Table 17:** *Agent Manager property descriptions*

---

# Creating Agent Manager Accounts

- Introduction** You can create Agent Manager accounts for the components and products that communicate with the Agent Manager. Agent Manager accounts provide a way to authenticate the components and products that are trying to communicate with the Agent Manager. This topic explains how to create Agent Manager accounts.
- Recommendation** IBM ISS strongly recommends that you require all agents to use Agent Manager accounts to securely communicate with the Agent Manager.
- Procedure** To create an Agent Manager account:
1. In the left pane, select the *Site Node*.
  2. In the view drop-down menu, select **Agent**.
  3. In the right pane, right-click the **Agent Manager**, and then select **Properties** from the pop-up menu.  
The Properties tab appears.
  4. In the left pane, select **Agent Properties**, and then click **Edit Agent Properties** in the right pane.  
The Policy Editor appears.
  5. In the left pane of the Policy Editor, select **Accounts**.  
The Accounts pane displays a list of the current account names and descriptions.
  6. Click **Add**.
  7. Type a unique **Account Name**, and then click **Enter Password**.
  8. Type and confirm the **Password**, and then click **OK**.
  9. Type a **Description** for the account, and then click **OK**.
  10. From the **File** menu, select **Save**, and then select **Exit**.

## Assigning Agent Managers to Agents

### Introduction

This topic explains how to assign Agent Managers to agents. If you can assign a more than one Agent Manager, them in order in which you want them to be used.

### Procedure

To assign an Agent Manager to agents:

1. In the left pane, right-click the group that contains the agent, and then select **Manage Policy**.
2. Right-click the **Default Repository**, and then click **New** → **Policy**.
3. In the Create New Policy window, select **Group Settings** for **Policy Type**, and then type a **Policy Name**.  
The Group Settings policy opens in a tab.
4. Select the **Agent Manager List** tab.
5. If the Agent Manager you want to select appears in the Agent Manager Information list, go to Step 8.
6. Click **Add**.
7. To select an Agent Manager that is on another Site, type the information in the fields, and then go to Step 11.
8. Click **Choose an Agent Manager**.
9. Select the Agent Manager to use, and then click **OK**.
10. On the Add Agent Manager Information window, click **OK**.
11. If the list contains more than one Agent Manager, select the primary Agent Manager, and click the up arrow to move the primary Agent Manager to the top row.
12. Click **OK**.
13. Close policy window, and click **Yes** to confirm saving the changes.
14. Check the **Deploy This New Version** check box, and then click **OK**.
15. In the Deploy Policy window, select **Targets** and check each group that you want to deploy the policy to.
16. Click **OK**.

## Chapter 7

# Configuring X-Press Update Servers

## Overview

### Introduction

You must configure the XPU Server before you can update your SiteProtector system. This chapter provides information about the following X-Press update Server (XPU Server) tasks:

- configuring the integrated XPU Server that is installed with the Application Server
- installing and configuring XPU Servers on remote computers

### In this chapter

This chapter contains the following topics:

Topic	Page
What is the X-Press Update Server?	72
Configuring the Server Settings Policy	73
Configuring the XPU Settings Policy	75
Setting Up Additional Stand-Alone XPU Servers	76
Configuring XPU Servers to Download from Other XPU Servers	79
Securing XPU Servers	81
Clustering XPU Servers	82
Configuring XPU Servers for Manual Updates	84

## What is the X-Press Update Server?

### Introduction

The X-Press Update Server (XPU Server) provides a secure, streamlined method for updating your SiteProtector system and other the IBM ISS products that you manage with your SiteProtector system.

The SiteProtector system installation includes one integrated XPU Server as part of the Application Server, but you can install additional stand-alone XPU Servers on other computers.

### Integrated XPU Server

The integrated XPU Server is installed on the Application server and is completely integrated with the Application Server. The XPU Server cannot be separated or removed from the Application Server without uninstalling the entire Application Server. In addition, you cannot install an additional XPU Server on the Application Server.

The XPU Server integrated on one instance of your SiteProtector system can be used as the remote XPU Server for another instance of your SiteProtector system. For example, the integrated XPU Server on Site A contacts the integrated XPU Server on Site B for updates.

### Stand-alone XPU Servers

A stand-alone XPU Server can be installed separately on non-Application Server computers using the Deployment Manager. Stand-alone XPU servers can be added and removed without affecting the Application Server.

A stand-alone XPU Server can be used by an integrated XPU Server or by another stand-alone XPU Server for updates.

For example, the integrated XPU Server on Site A contacts a stand-alone XPU Server. The stand-alone XPU Server then contacts another stand-alone XPU Server for updates.

### Downloading updates

Integrated and stand-alone XPU Servers can download updates directly from [xpu.iss.net](http://xpu.iss.net). By default, an XPU server is configured to download updates directly from this location. This default setting requires that the XPU Server have Internet access.

In some cases, an XPU server does not have Internet access or is specifically configured not to contact the Internet. In these cases, you can set up XPU cascading. XPU cascading allows you to point the XPU Server to another XPU server, and then point that XPU Server to another, and so on. Eventually, one XPU Server must connect to the Internet to download the updates. If you do not have any XPU Servers in your SiteProtector system installation that can contact the Internet, then you must manually download the updates using one of the following methods:

- Manual Upgrader
- an Internet browser that connects to the IBM ISS download center



# Configuring the Server Settings Policy

**Introduction** This topic provides instructions for configuring the Server Settings policy.

**Description** The Server Settings policy controls the following XPU Server behaviors:

- whether an XPU Server can download updates from other XPU servers including [www.iss.net](http://www.iss.net)
- how much bandwidth an XPU Server can use when sending updates to SiteProtector system components and agents
- what types of information the XPU Server sends to the log files

**Procedure** To configure the Server Settings policy:

1. In the left pane, select the group that contains the X-Press Update Server.
2. In the **Go to** list, select **Agent**.
3. In the right pane, right-click the **X-Press Update Server**, and then select **Manage Policy**.

The Policy tab appears.

4. In the right-pane, expand **Policy Types Not Deployed**.
5. Right-click **Server Settings**, and then select **Open Policy**.

**Note:** For a new installation, the X-Press Update Server is in the **Locally Configured Agents** group.

6. Configure the following options:

Option	Description
Download from other X-Press Update Servers	Select this option if you want the XPU Server to be able to download updates from another XPU Server or from <a href="http://xpu.iss.net">xpu.iss.net</a> . <b>Default Setting</b> = Enabled
Throttle downloads to clients	Select this option to limit the bandwidth that your SiteProtector system can use for downloading XPUs from the XPU Server. If you select this option, then you must set the following: <ul style="list-style-type: none"> <li>• Maximum number of connections allowed to the XPU Server</li> <li>• Maximum bandwidth in kilobytes per second that the XPU Server can use</li> </ul>
Logging	Select the type of information you want your SiteProtector system to record in the XPU Server log files: <ul style="list-style-type: none"> <li>• Debug</li> <li>• Info</li> <li>• Warn</li> <li>• Error</li> </ul>
Maximum number of log files	The number of log files to maintain <b>Note:</b> A new log file is created for every restart.

Option	Description
Rotate Log Files	When to close a log and start a new one <ul style="list-style-type: none"><li>• Every Restart</li><li>• Every Day</li></ul>
Status Page: Enable detailed status page	Allows more information to be displayed on your status page ( <a href="http://your_IP_address:3994/updateserver/status">http://your_IP_address:3994/updateserver/status</a> )
Heartbeating Interval	How frequently the X-Press Update Server heartbeats in <b>Note:</b> Under normal circumstances it should not be necessary to increase the frequency.

7. Click **Save All**.

# Configuring the XPU Settings Policy

**Introduction** The XPU settings policy controls how the XPU Server downloads, installs, and manages updates for itself only.

**Advanced Parameters** Advanced Parameters are used for debugging problems with updates and certain communication settings. Advanced parameters are unnecessary for most users.

**Procedure** To configure the XPU Settings policy:

1. In the left pane, select the group that contains the X-Press Update Server.
2. In the **Go to** list, select **Agent**.
3. In the right pane, right-click the **X-Press Update Server**, and then select **Manage Policy**.

The Policy tab appears.

4. In the right-pane, right-click **XPU Settings**, and then select **Open Policy**.
5. Select the **XPU** tab, and then configure the following options:

Option	Description
Automatically download updates	Select this option to automatically download updates for the XPU Server when they are available.
Automatically install updates	Select this option to automatically install updates for the XPU Server after they are downloaded. Do not select this option if you want to manually install updates for the XPU Server.
Check for updates every X hours	Select how often you want the XPU Server to check for available updates. The default value is once every 24 hours.

**Note:** These settings do not control how the XPU Server downloads, installs, and manages updates for other SiteProtector system components or agents. This topic provides instructions for configuring XPU settings.

6. Select the **Servers** tab, and then add, remove, and edit the servers from which the XPU Server can download updates.

**Reference:** For instructions on how to configure an XPU Server to download updates from another XPU Server, See “Configuring XPU Servers to Download from Other XPU Servers” on page 79.

7. Click **Save All**.

## Setting Up Additional Stand-Alone XPU Servers

### Introduction

This topic provides information about setting up and configuring additional stand-alone XPU Servers. These servers cannot be installed on the Application Server.

After you set up the stand-alone XPU servers, you can configure the stand-alone XPU servers to connect to IBM ISS for updates, and then configure the integrated XPU Server to download updates from the stand-alone XPU Server. This approach allows you to download updates from IBM ISS without allowing your Application Server Internet access.

**Important:** Do not install additional stand-alone XPU Servers until after you have installed your SiteProtector system. If you try to install additional stand-alone XPU Servers before you install your SiteProtector system, then it will be difficult for you to provide required information during the XPU Server installation.

### Before you begin

When you install an additional XPU Server, the installation program asks for certain information that is used to automatically configure some XPU Server settings for you. To ensure that you have this information during the installation process, IBM ISS recommends that you perform the tasks in Table 18 *before* you install the additional XPU Servers.

Task	Description
1	Set up a license for the XPU Server. See "Proventia OneTrust Licensing" on page 53.
2	Create an Agent Manager account for the XPU Server (optional). You will need the following information during the installation: <ul style="list-style-type: none"> <li>Account name</li> <li>Password</li> </ul> See "Creating Agent Manager Accounts" on page 69.
3	Create and configure the group where you want to put the XPU Server, including the Agent Manager settings, or obtain the name of an existing group (optional). You will need the name of the group during the installation. See "Creating Groups" on page 225.
4	Obtain information about the Agent Manager that the XPU Server will connect to. You will need this information during the installation: <ul style="list-style-type: none"> <li>name (optional)</li> <li>IP address or DNS name where the Agent Manager is installed</li> <li>Port</li> <li>Account name and password for the Agent Manager account (optional)</li> </ul>
5	If the XPU Server will need access through a firewall or proxy server, then obtain the information about the firewall or proxy server. You will need the following information during the installation: <ul style="list-style-type: none"> <li>IP address</li> <li>port</li> </ul>

**Table 18:** *Before you install additional XPU Servers*

**Procedure**

To install an additional XPU Server:

1. Connect to the Deployment Manager on the computer where you want to install the XPU Server.  
**Note:** Do not install the XPU Server on the same computer where the Agent Manager is installed. If you do, then the Agent Manager might experience performance issues.
2. Select **Install SiteProtector**.  
 The SiteProtector Installation page appears.
3. Select **Additional X-Press Update Server Installation**.  
 The Prerequisites page appears.
4. Review the prerequisites, and then click **Next**.  
 The Prepare to Install window appears.
5. Click **Install**.  
 The File Download window appears.
6. Click **Open**.  
 The InstallShield Wizard Welcome window appears.
7. Click **Next**.  
 The License Agreement window appears.
8. Review the terms of the license agreement, click **I Accept**, and then click **Next**.  
 The Choose Destination Location window appears.
9. Select a destination folder, and then click **Next**.  
 The X-Press Update Server Configuration (Specify Agent Manager location) window appears.
10. Complete the following fields, and then click **Next**:

<b>Field</b>	<b>Description</b>
Name	The name of the Agent Manager that the XPU Server will connect to. <b>Example:</b> AgentManager_100
Address (IP or DNS)	Either the IP address or DNS where the Agent Manager is located.
Port	The port the XPU Server should use to communicate with the Agent Manager. (3995 is the default port.)
Account Name	The user name the XPU Server should use to initiate communication with the Agent Manager.
Password	The password the XPU Server must use to initiate communication with the Agent Manager.

The X-Press Update Server Configuration (Specify SiteProtector Group Name) window appears.

11. Complete the following fields, and then click **Next**:

Field	Description
SiteProtector Group Name	The name of the group where you to put the XPU Server. If you leave this field blank, then your SiteProtector system puts the XPU Server in Ungrouped Assets.
X-Press Update Server security mode	One of the following: <ul style="list-style-type: none"> <li>Trust all, which allows other servers to connect to the XPU Server every time it attempts a connection; no certificates are used for authentication.</li> <li>First time trust, which allows other servers to connect to this XPU Server one time only. After the first connection, the XPU Server uses the connecting server's certificate to authenticate all future connections.</li> <li>Explicit trust, which requires this XPU Server to use a local certificate to authenticate the server it is connecting to.</li> </ul>
Primary IP	If the local computer has more than one network interface, select the IP address that will be used for XPU Server communication.
Address (IP or DNS)	If the XPU Server will require access through a firewall or proxy server, then enter the IP address or DNS of the firewall or proxy server.
Port	The port through which the XPU Server will access the firewall or proxy server.

The Archival: Private Key Archival window appears.

12. In the **Folder** box, type the location where you want to archive private keys, and then click **Next**.

**Tip:** IBM ISS recommends that you archive keys on a removable medium.

The Ready to Install the Program window appears.

13. Click **Install**.

The InstallShield Wizard Complete Window appears.

14. Click **Finish**.

15. Configure the XPU Server settings as described in this chapter.

# Configuring XPU Servers to Download from Other XPU Servers

**Introduction** This topic provides instructions for setting up an XPU Server to download updates from another XPU Server.

**Important:** Do not use the procedures in this topic to configure XPU Servers for Proventia Network MFS or Proventia Network IPS.

**Purpose** After you set up stand-alone XPU Servers, you can configure the integrated XPU Server to download updates from the stand-alone XPU Server, rather than the IBM ISS download center. This approach is useful for customers who want to prevent the Application Server from accessing the Internet but still want to download updates from IBM ISS.

**Cascading** You can use the XPU Server cascading feature where the local XPU server is installed on the Application Server and the remote XPU server is not installed on the Application Server.

**Note:** The remote XPU server for a given SiteProtector system instance can be an XPU server installed on the Application Server of a different SiteProtector system instance.

**Task overview** Table 19 describes the tasks for configuring an XPU Server to download updates from another XPU Server.

Task	Description
1	Verify that the Download from other X-Press Update Servers option is enabled for the XPU Server. This option is enabled by default.
2	Add an XPU Server to the list of possible servers that the XPU Server can download from, and move it to the top of the server list.

**Table 19:** *Configuring an XPU Server to download from other XPU Servers*

**Required information** Before you configure an XPU Server to download updates from another XPU Server, you must obtain the following information about the XPU Servers that you are configuring:

- IP address or DNS name
- Port (default port is 3994)

**XPU Server list** In XPU Server settings, you can set up a list of XPU Servers and direct the XPU Server to download updates from the servers in the list. An XPU Server can only download updates from one server at a time. The XPU Server contacts the servers in the order listed. For example, the XPU Server attempts to contact the first server in the list. If this server is unavailable, then the XPU Server attempts to contact the next server in the list. The process continues until the XPU Server successfully establishes communication with one of the servers in the list.

In XPU Server settings, you can manage this list as follows:

- add servers to the list
- remove servers from this list
- change the order in which the servers are listed

**Verify XPU Server can download from other servers**

To verify that the XPU Server is configured to download from other XPU Servers:

1. In the left pane, select the group that contains the X-Press Update Server.
2. In the **Go to** list, select **Agent**.
3. In the right pane, right-click the **X-Press Update Server**, and then select **Manage Policy**.  
The Policy tab appears.
4. In the right-pane, right-click **Server Settings**, and then select **Open Policy**.  
The Policy tab appears.
5. Verify that the **Download from other XPU Servers** option is enabled.

**Adding XPU Servers to the XPU Server list**

To add an XPU Server to the list of available servers that the XPU Server can download from:

1. In the left pane, select the group that contains the X-Press Update Server.
2. In the **Go to** list, select **Agent**.
3. In the right pane, right-click the **X-Press Update Server**, and then select **Manage Policy**.  
The Policy tab appears.
4. In the right-pane, right-click **XPU Settings**, and then select **Open Policy**.  
The Policy tab appears.
1. Select the **Servers** tab  
The pane displays the Download from these X-Press Update Servers list.
2. Click **Add**.  
The Add XPU Server window appears.
3. Complete the following fields:
  - **Name**
  - **Host or IP**
  - **Port**
  - **Proxy Host**
  - **Proxy Port**
  - **Proxy User**
  - **Proxy Password**
  - **Trust level**
4. Click **OK**.  
The XPU Server is added to the list. The XPU Server that you are configuring can now download updates from this XPU Server.
5. Select the XPU Server you added, and then click **Up** to move it to the top of the list.  
The XPU Server attempts to contact this server first for updates.



# Securing XPU Servers

## Introduction

Unprotected X-Press Update Servers are vulnerable to malicious attacks and software piracy. Unauthorized distribution of IBM ISS software can violate your license agreement. IBM ISS recommends that you protect XPU Servers from unauthorized remote access. To secure this communication, consider implementing the following:

- firewalls or proxies between X-Press Update Servers and the Internet
- RealSecure Server Sensors on computers where X-Press Update Servers are installed
- secure trust levels
- SSL certificates

## Proxy servers

A proxy server can allow or deny the XPU Server access to the Internet based on the XPU Server's User-Agent string.

If the XPU Server accesses the Internet using a proxy server, then you must make sure that the proxy server is configured to allow the User-Agent string called "UpdateMirrorWorker." The XPU Server sends this User-Agent string when it tries to access the Internet through a proxy server.

## Trust levels

Table 20 describes the trust levels you can establish between XPU Servers and other XPU Servers.

Level	Description
Trust all	The client trusts the server and does not try to validate the certificate.
First time trust	The client trusts the first certificate it receives from the server and stores this certificate locally. The client uses this certificate to validate all future communication with this server.
Explicit trust	The server's certificate must reside on the client's local directory before the agent or component can initiate communication with the server. Typically, the server's certificate is transferred to the client outside the standard communication channels.

**Table 20:** *Trust levels between XPU Servers*

## Server SSL certificates

SSL certificates are used to validate a server's identity when an XPU Server attempts to communicate with the server. Typically, an XPU Server stores certificates locally and then tries to match it to the certificate that the server sends during the communication startup. If these certificates do not match, the XPU Server shuts down the connection.

The certificate is created when you install the XPU Server.

# Clustering XPU Servers

## Introduction

Clustering XPU Servers can improve performance and provide failover. You can cluster with or without load balancing.

## Load balancing

Load balancing tries to distribute the workload to the available servers evenly so that the work is done more efficiently and so that failover can occur smoothly. IBM ISS does not support the clustering of X-Press Update Servers with load balancing; however, IBM ISS recommends that you use the `mod_rewrite` program that is free with Apache software.

**Note:** If you want robust load balancing, consider using a commercial solution such as Cisco's Local Director or Microsoft Network Load Balancing.

## Option 1: Clustering without load balancing

When you configure a list of X-Press Update Servers, agents connect to a list of X-Press Update Servers in a round-robin fashion. Agents try to connect with the first server on the list. If the first connection fails, the agent attempts to connect to the second server on the list, and so on, as shown in Figure 2:

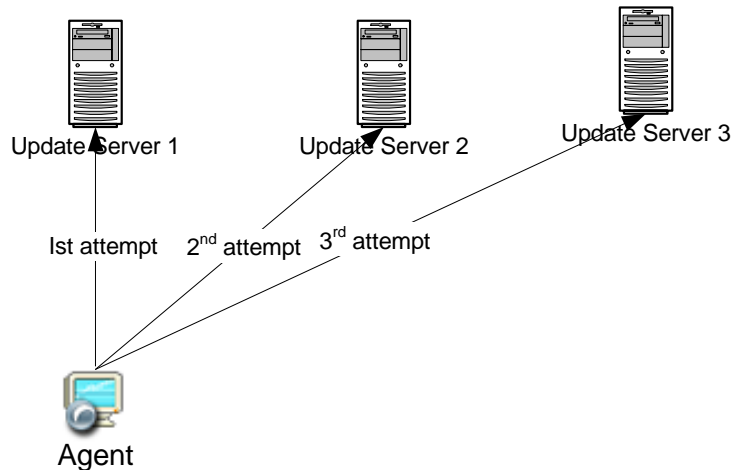
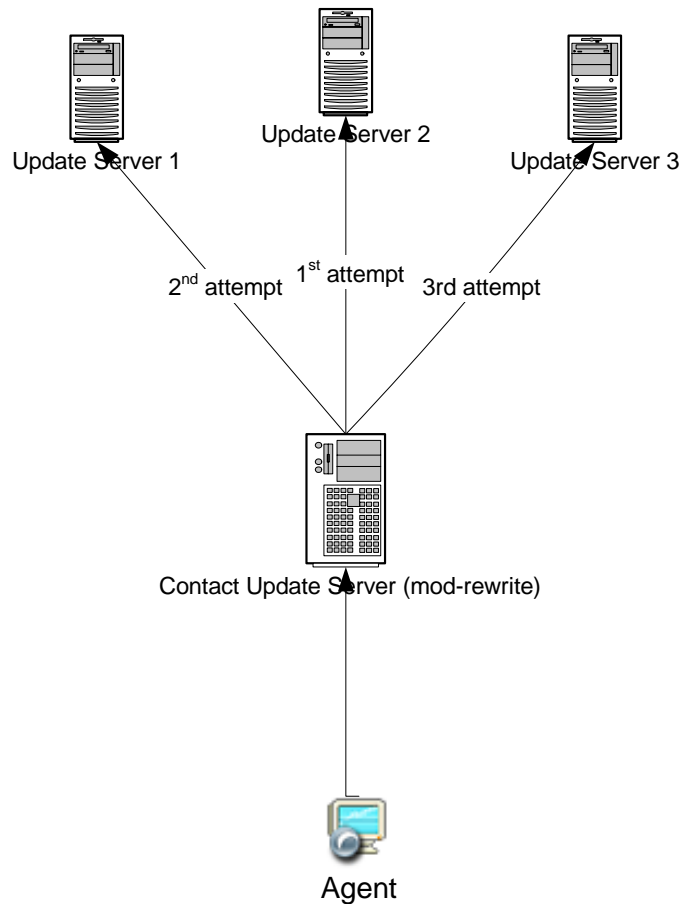


Figure 2: The Agent tries to connect to X-Press Update Servers in a round-robin fashion

**Option 2: Clustering with load balancing**

Apache software provides a free `mod_rewrite` program that can redirect agents to X-Press Update Servers in a way that distributes the workload. The contact server randomly redirects agents to each X-Press Update Server in the group:



**Figure 3:** X-Press Update Server randomly redirecting agents using `mod_rewrite`

**Reference:** For information about configuring the `mod_rewrite` module to perform load balancing, refer to your Apache Web server documentation.

## Configuring XPU Servers for Manual Updates

### Introduction

The X-Press Update Server is designed to keep itself updated with the latest features and fixes from the IBM ISS Web site. However, for security reasons, some users do not have access to the Internet from their SiteProtector systems.

This topic explains how to download update files for the XPU Server manually get updates directly from the IBM ISS Download Center.

### Task overview

Table 21 describes the tasks for configuring an XPU Server to update itself manually.

Task	Description
1	Download the required update files from the IBM ISS Download Center.
2	Add a required license file to the XPU Server, and configure the Update Server.conf file.
3	Modify the XPU Server's file structure.

**Table 21:** Tasks for configuring XPU Servers for manual self-updates

### Downloading an update file

Download the following files from the IBM ISS Download Center:

- the XPU files
- the XPU\_5\_0.xml file, which can be retrieved at [https://www.iss.net/update/SiteProtector/XPU\\_5\\_0.xml](https://www.iss.net/update/SiteProtector/XPU_5_0.xml)
- XPU\_2\_7.xml
- RiskIndex.xml

### Adding a license

To add the required IBM ISS license:

**Note:** You do not have to perform this procedure if you have a OneTrust license at the Site that manages the update server.

1. Place a valid license on the X-Press Update Server's file system.
2. Copy and paste the path to this license file.
3. Use the following table to determine your next steps:

If you are updating...	Then...
the integrated XPU Server on the Application Server	Open the UpdateServer.conf file using a text editor such as Notepad. The default path to the file on the Application Server computer is as follows: <code>\Program Files\ISS\SiteProtector\Application Server\webserver\Apache2\conf\Update Server.conf</code>
a stand-alone XPU Server on a non-Application Server computer	Open the UpdateServer.conf file using a text editor such as Notepad. The default path to this file on the computer where the stand-alone XPU Server is as follows: <code>\Program Files\ISS\SiteProtector\X-Press Update Server\webserver\Apache2\conf\UpdateServer.conf</code>

4. In the text editor, locate the text 'LicenseFile "None."'
5. Replace "None" with the full path to the local license file.
6. Save the Update Server.conf file.
7. Restart the SiteProtector Web Server service.

## Modifying the XPU structure

The XPU Server also requires a specific file structure for self-updating. The integrated XPU Server uses a different file structure than a stand-alone XPU Server.

To modify the XPU Server's file structure:

1. Navigate to the XPU Server's Apache2 directory.

Server	Default Path
Integrated XPU Server	\Program Files\ISS\SiteProtector\Application Server\webserver\Apache2
Stand-alone XPU Server	\Program Files\ISS\SiteProtector\X-Press Update Server\webserver\Apache2

2. Create a folder within the Apache2 directory called XpuSelf as follows:

```
\Program Files\ISS\SiteProtector\X-Press Update
Server\webserver\Apache2\XpuSelf
```

3. In the XpuSelf directory, create a SiteProtector folder as follows:

```
\Program Files\ISS\SiteProtector\X-Press Update
Server\webserver\Apache2\XpuSelf\SiteProtector
```

4. Put the XPU\_4\_0.xml catalog file in the SiteProtector directory.

- for versions XPU 1.1 and earlier, use the \XPU\_4\_1.xml catalog file
- for versions XPU 1.2 and later, use the \XPU\_5\_0.xml catalog file

5. In the SiteProtector directory, create an UpdateServer directory as follows:

```
\Program Files\ISS\SiteProtector\X-Press Update
Server\webserver\Apache2\XpuSelf\SiteProtector\UpdateServer
```

6. Move the XPU files to the Update Server directory.

The XPU Server is configured to update itself manually. The self-update could take several hours or more, depending on the policy settings for the XPU Server.



## Chapter 8

# Updating Your SiteProtector System

## Overview

### Introduction

This chapter provides information about the following:

- updating your SiteProtector system
- updating agent security content
- updating your SiteProtector system manually

### Requirement

You must update your SiteProtector system with the latest software updates before you configure the other components. This approach ensures that you have the latest, most secure and reliable IBM ISS software available.

### In this chapter

This chapter contains the following sections:

<b>Section</b>	<b>Page</b>
Section A, "Updates Overview"	89
Section B, "Updating SiteProtector System Components"	95
Section C, "Applying Security Content to Agents"	101
Section D, "Applying Updates without XPU Server Internet Access"	109





# SECTION A: Updates Overview

## Overview

**Introduction** This section provides information about the update process and the types of updates that IBM ISS provides for its products.

**Note:** The information in this section applies to all other IBM ISS products such as Network Sensor and Server Sensor.

**In this section** This section contains the following topics:

Topic	Page
Update Process	90
X-Press Updates	92
Service Packs	94

# Update Process

## Introduction

This topic explains the following:

- the stages of a typical update process
- the types of update files required during the update process
- the statuses that components and agents might show during the update process.

**Note:** The information in this topic assumes that the XPU Server is configured with Internet access. For information about updating agents and components without Internet access, see *Manually Updating Agents and Components*.

## Updating components and agents

The update process relates to:

- Legacy sensors (Network Sensor, Server Sensor)
- Database Service Packs
- SiteProtector Core XPU
- Event Collector XPU
- Agent Manager XPU

The update process does not relate to the Update Server, Event Archiver, Proventia Network MFS or Proventia Network IPS as these systems update automatically.

## Typical process

Table 22 describes a typical update process.

Stage	Description
1	The SiteProtector system checks the IBM ISS Web site for new catalog files once every 24 hours by default.
2	If a new catalog file is available, then the SiteProtector system retrieves the new catalog file.
3	The SiteProtector system reviews the information in the catalog file to determine that available product or component updates, and then passes this information to the Site Database.
4	The Console updates the status of components to reflect whether updates are available. If an update is available for a component, then the component's status is Out of Date.
5	The SiteProtector system downloads the update files to a repository on the Application Server when you make an XPU request.
6	The Sensor Controller applies the update files to the Out of Date components (according to your scheduling settings) or applies the update files when you initiate the process. If you configure the XPU settings to wait for you to initiate the Apply Update process, the Sensor Controller applies the update files from the repository location. The XPU Server does not have to download the files again from the IBM ISS Download Center.

**Table 22:** *Update process*

**Required files**

Table 23 describes the files required during an update:

Required File	Description
License file	<ul style="list-style-type: none"> <li>• a file that allows you to use and update the IBM ISS products</li> <li>• required for the SiteProtector system Export Compliance check that ensure all updates and downloads meet Export Compliance laws</li> </ul>
Catalog file	<ul style="list-style-type: none"> <li>• contains information about the updates available for the product or component</li> <li>• the SiteProtector system uses the information in this file to determine the status of components</li> <li>• available from the IBM ISS Download Center</li> <li>• downloaded automatically if your Site has Internet connectivity</li> </ul>
Update file	<ul style="list-style-type: none"> <li>• contains information about the updates available for the product or component</li> <li>• the SiteProtector system uses the information in this file to determine the status of components</li> <li>• available from the IBM ISS Download Center</li> <li>• downloaded automatically if your Site has Internet connectivity</li> </ul>

**Table 23:** *Files required for updates*

## X-Press Updates

**Introduction** An X-Press Update (XPU) is a software release that contains new security content, including the following:

- new signatures
- new checks
- revised signatures
- revised checks
- revised policies that address security issues

**Agents** IBM ISS provides XPUs for all agents, including the following:

- Desktop Protection agents such as Proventia Desktop
- appliances such as Proventia Network MFS and Proventia Network IPS
- agents such as Network Sensor, Server Sensor, and Proventia Server IPS
- scanners such as Network Internet Scanner, Network Enterprise Scanner, and System Scanner vulnerability assessment application

**SiteProtector system components** IBM ISS provides XPUs for the following SiteProtector system components:

- the Site Database
- the XPU Server
- Event Archiver

**Cumulative and incremental XPUs** Table 24 describes the differences between cumulative and incremental XPUs.

Type of XPU	Description
Cumulative XPU	<ul style="list-style-type: none"> <li>• used for agents such as Network Sensor and Server Sensor</li> <li>• contains all the changes released in previous XPUs</li> <li>• when you install a cumulative XPU, the SiteProtector system updates the agent with all current signature and code changes</li> <li>• when you remove a cumulative XPU, the SiteProtector system returns the agent to its previous state before the XPU was applied</li> </ul>
Incremental XPU	<ul style="list-style-type: none"> <li>• used for agents such as Network Internet Scanner</li> <li>• contains only the changes since the previous XPU</li> <li>• does not include changes from prior XPUs</li> <li>• when you install an incremental XPU, the SiteProtector system automatically installs any prior XPUs not already installed</li> <li>• when you remove an incremental XPU, the SiteProtector system removes only the most recently applied XPU. To remove all changes, you must remove each previously applied XPU separately to return the agent to its previous state</li> </ul>

**Table 24:** Cumulative and incremental XPUs

---

**Naming conventions** XPUs are named and numbered based on the following format:

*product name a.b*

*product name* represents the product

*b* increments with each XPU

*a* increments with each major release of the software and resets *b*

#### Examples

- RealSecure Server Sensor Policy Update for XPU 22.36
- RealSecure Server Sensor Policy Update for XPU 22.37
- RealSecure Server Sensor Policy Update for XPU 23.2

#### Required XPUs for agents that use policies

When you update an agent that uses policies, the SiteProtector system applies two XPUs:

- the XPU that updates the agent
- the XPU that updates the policy

If you manually download XPUs, then you must make sure you download both required files for agents of this type.

#### Example

You are downloading update files for Network Internet Scanner manually. You must download the following XPUs:

- XPU called Internet Scanner 7.0 SP2 - XPU 7.2.10, which updates the agent
- XPU called Internet Scanner Policy XPU for Internet Scanner 7 (XPU 7.2.10), which updates the policies

## Service Packs

### Introduction

A service pack is a software release that includes any of the following:

- product fix
- product enhancement
- new security content

The release might include a new agent, new manager, daemon binary, or some combination of files. If you have a strict change control process, then you might be required to manage service packs in the same way that you manage full releases.

### Agents

IBM ISS provides service packs for all agents, including the following:

- Desktop Protection agents such as Proventia Desktop
- Sensors such as Network Sensor and Server Sensor
- Scanners such as Network Internet Scanner and System Scanner vulnerability assessment application

### SiteProtector system components

IBM ISS provides service packs for the following SiteProtector system components:

- SiteProtector Core component, which includes the Application Server, Sensor Controller, Console, and an integrated XPU Server
- Event Collector
- Agent Manager
- SecurityFusion module
- System Scanner Databridge
- Database

### Obtaining service packs

You can obtain a service pack from the following:

- product interface
- IBM ISS Download Center
- product CD

### Naming conventions

Service packs are named and numbered based on the following format:

*Product/Component Name Version* **Service Pack** *x.y.z*

#### Examples

- Agent Manager 6.9 Service Pack 6.23
- SiteProtector Database 2.0 Service Pack 5.13
- Event Collector 6.9 Service Pack 1.12

# SECTION B: Updating SiteProtector System Components

## Overview

**Introduction** This section provides information about updating your SiteProtector system.

**Before you begin** Before you update your SiteProtector system, you must complete the following tasks:

- Set up licenses for your SiteProtector system.  
See “Setting Up Licenses” on page 49.
- Configure the XPU Server.  
See “Configuring X-Press Update Servers” on page 71.

**In this section** This section contains the following topics:

Topic	Page
Determining Update Status	96
Applying Updates to SiteProtector System Components	97
Applying Updates to the SiteProtector Core Component	99

## Determining Update Status

### Introduction

This topic explains how to determine the update status of a SiteProtector system component or an agent.

### Update statuses

Table 25 describes the available update statuses for SiteProtector system components.

Component	Status	Description
<ul style="list-style-type: none"> <li>• SiteProtector Core</li> <li>• Agent Manager</li> <li>• Site Database</li> <li>• Event Collector</li> <li>• SecurityFusion module</li> <li>• Third Party Module</li> </ul>	Current	No updates are available for the component.
	Out of Date	Updates are available for the component, and you must update the component.
	Error	An error condition exists.
	In Progress	The SiteProtector system is updating the component.
	blank	The component is not reporting its update status to the SiteProtector system.

**Table 25:** *Update Statuses for the SiteProtector system components*

**Reference:** See “Determining Whether Security Content Updates Are Available” on page 102 for information about agent update statuses.

### Procedure

To determine the update status of a SiteProtector system component:

1. In the left pane, select the *Site Node*.
2. In the **Go to** list, select **Agent**.
3. Locate the component in the Update Status column.

This column shows the update status for the component.



# Applying Updates to SiteProtector System Components

## Introduction

This topic explains how to apply updates to SiteProtector system components.

**Note:** You cannot remove updates from SiteProtector system components.

## Task overview

After you install the SiteProtector system, some SiteProtector system components might be Out of Date, which indicates that updates have been released since you installed the product. In this case, you must update all of the SiteProtector system components and follow this sequence.

Task	Description
1	Update the following components if updates are available: <ul style="list-style-type: none"> <li>• Site Database</li> <li>• Event Collector</li> <li>• Agent Manager</li> </ul>
2	Update the SiteProtector Core component. This update includes an update for the Console. After you update the Core component, the status of other components might change to Out of Date, indicating that additional updates are available as a result of the Core update.
3	Update any components whose status changed to Out of Date. If you are updating more than one component, then update the components in this order: <ul style="list-style-type: none"> <li>• Event Collector(s)</li> <li>• Database XPU's</li> <li>• Database Service Packs</li> <li>• Agent Manager(s)</li> <li>• Deployment Manager</li> <li>• SecurityFusion module</li> </ul> <p><b>Note:</b> The recommended sequence might vary depending on the release. See the release notes for more information.</p>

**Table 26:** Task overview

## Procedure

To apply an update to a SiteProtector system component:

1. In the left pane, select the *Site Node*.
2. In **Go to** list, select **Agent**.  
The Agent view appears in the right pane.
3. In the right pane, right-click the component you want to update, and then select **Updates** → **Apply XPU**.  
The Schedule Update window appears.
4. Do you want to update the agent immediately?
  - If *yes*, select **Run Once** in the **Recurrence Pattern** section, click **OK**, and then go to Step 5.

- If *no*, schedule a command job to update agents on a recurring basis, and then click **OK**.

**Note:** If you selected Run Once to install the update immediately, then the installation process begins. If you scheduled the update to install at later time, then the installation process will begin at the time you set.

For immediate installations, the SiteProtector system displays progress as follows:

Indicator	Description
Overall progress	Indicates progress of the entire update process
Current step progress	Indicates progress of each individual step in the update process; the text box displays a summary of the current step

The End User License Agreement window appears.

5. Review the agreement, and then select **I Accept**.

The Select XPU window appears.

6. Select the type of update you want to install:

- Full Upgrade
- Service Pack
- X-Press Update

7. When you are ready to install the updates, click **Finish**.

**Important:** If you are updating the SiteProtector Core component, then the process can take up to 45 minutes. Do not reboot during this time.

8. Click **Finish** when the installation process is finished.

# Applying Updates to the SiteProtector Core Component

## Introduction

The process for updating the SiteProtector Core component is different from the process for updating other SiteProtector system components. The XPU downloads an installation file that you must run from the Application Server computer to install the update.

## Before you begin

Check the following before you begin to update the SiteProtector Core component:

- You must have administrative rights to log on to the Application Server computer.
- You must supply the credentials for an account with administrative access to the SQL Server database.
- You must close all local consoles.

## During the installation

Table 27 describes the major steps of the installation program.

Installation Step	Result
System check	<p>Before the core update begins, the program checks for the following:</p> <ul style="list-style-type: none"> <li>• Disk space The installation stops if insufficient disk space is available.</li> <li>• Database space The installation stops if insufficient database space is available.</li> <li>• System memory A warning is issued if system memory is too low.</li> <li>• Processor speed A warning is issued if the processor speed is too low.</li> </ul>
Antivirus handling	<ul style="list-style-type: none"> <li>• On an Application Server computer, the update presents a list of known antivirus programs found on the computer that you should shut down.</li> <li>• On the SP1001 appliance, the Proventia Server services are shut down and restarted after the update.</li> </ul>
Installation	As the installation runs, the current step is shown in the installation program window.
If the update fails	The installation program identifies the step on which the installation failed to use for troubleshooting.

**Table 27:** Major installation steps

**Process**

Table 28 describes the process to follow to update the SiteProtector Core component.

Stage	Description
1	Download the SiteProtector Core XPU through the standard Apply Update process for the SP Core component. Watch for important messages that provide information about pre- and post-installation requirements. <b>Note:</b> When the download completes, the SP Core version will not change.
2	Run the Core Update from the Application Server. Click <b>Start</b> → <b>Programs</b> → <b>ISS</b> → <b>SiteProtector</b> → <b>Install SiteProtector 2.0 SP7</b> . The installation program guides you through the process.

**Table 28:** *Stages of the update process for the SiteProtector Core component*

## SECTION C: Applying Security Content to Agents

### Overview

**Introduction** The speed with which you update your agents with the latest signatures and checks can make or break the security of your network. To save time, the SiteProtector system provides a streamlined process for applying the security content of X-Press Updates (XPU) to multiple agents.

**Scope** This section applies only to appliances that are new to the IBM ISS product line, such as the latest versions of the Proventia Network IPS and Proventia Network IDS. The procedures for updating or removing other XPU content are as follows:

- To update or remove software updates from agents, you must use the agent's local management interface. These updates are referred to in SiteProtector system as major or minor features. See the documentation for the agent that you want to configure.
- To update or remove security content from earlier Proventia Network IPS and Proventia Network IDS, you must use the agent's local management interface.

**Agent security content** Agent security content consists of updates that prevent threats, vulnerabilities, or other security issues from occurring. Security content updates for the Proventia Network IPS and Proventia Network IDS are referred to as Protocol Anomaly Module (PAM) updates.

**In this section** This section contains the following topics:

Topic	Page
Determining Whether Security Content Updates Are Available	102
Updating Agent Security Content	103
Verifying an Agent's Update History	105
Removing Agent Security Content	106

## Determining Whether Security Content Updates Are Available

### Introduction

The SiteProtector system provides an easy way to determine whether agent updates are available and to verify the status of those updates. The statuses covered in this topic apply to following agent updates:

- security content
- software or firmware

### Update Status column

The Update Status column lets you sort agents so that agents that require updating (Out of Date status) appear first in the list. You can right-click a selection of these agents and apply multiple updates at the same time.

### Update status messages

Table 29 lists status messages in the Update Status column of the Agent view. These messages appear in the status column as details of the “Out of Date” messages.

Update Status	Description
Not licensed	Agent is not licensed. You must provide a valid license before you can update this agent.
Critical Content	Time-sensitive security content is available for this agent. Consider updating this agent as soon as possible. You can update this content in the SiteProtector system and in the agent's Proventia Manager.
Content	Security content is available for this agent. Consider updating this agent. You can apply these updates in the SiteProtector system and in the agent's Proventia Manager.
Maintenance	Time sensitive software updates that may contain important bug fixes are available. You must apply these updates in the agent's Proventia Manager.
Minor Features	Software updates that contain enhancements to existing features or user interfaces are available. You must apply these updates in the agent's Proventia Manager.
Major Features	Software updates that contain new features or user interfaces are available. You must apply these updates in the agent's Proventia Manager.

**Table 29:** *Update status messages*

**Note:** Depending on the agent, some of the statuses listed in this table may not appear.

---

# Updating Agent Security Content

## Introduction

When you update the security content of certain agents, the SiteProtector system lets you apply updates to multiple agents and skip several steps in the update process so that agents can begin to use this content without delay. This topic provides a procedure for updating agent security content with the Apply XPU option.

## How it works?

The Apply XPU option discovers, downloads, and applies the latest security content of an X-Press Update to a selected agent, folder, or group of agents. The Apply XPU option appears when you right-click an agent in the Agent view.

**Important:** The procedure in this topic applies only to certain agents. To determine whether this option is available for an agent, right-click the agent in the Agent view, and then verify that the Apply XPU option is available (not dimmed) on the pop-menu.

## How long does it take to update agents?

The update process begins shortly after you select the Apply XPU option. Depending on the number of agents you are updating, this process may take several minutes. You can monitor the progress of these updates, including the overall XPU status, in the Command Jobs window.

**Note:** The SiteProtector system first tries to contact the agent that you are trying to update. If the first attempt is unsuccessful, the agent will continue to contact the SiteProtector system as part of its normal communication process until the update can be applied successfully.

## Requirements for applying security content updates to multiple agents

The following requirements apply if you select multiple agents in the Agent view or select a folder from the grouping tree:

- If the group you select contains different versions that belong to the same agent type, the SiteProtector system applies the updates that are required to update each agent to the latest version.
- If the group you select contains agents or components that belong to different agent types, the SiteProtector system prompts you to choose the agent type that you want to update.

**Note:** You can update only one agent type at a time.

**Updating agent security content**

To update the security content of an agent or agents:

1. Select the **Agent** view.
2. Do one of the following:

<b>If you want to apply the update to...</b>	<b>Then do this...</b>
a single agent in the Agent view	Right-click the agent that you want to update, and then select <b>Updates</b> → <b>Apply XPU</b> from the pop-up menu.
multiple agents in the Agent view	Use the Windows shift-click (or cntrl-click) command to select agents you want to update, right-click the agents, and then select <b>Updates</b> → <b>Apply XPU</b> from the pop-up menu.
a folder in the grouping tree	Right-click the group that you want to update, and then select <b>Updates</b> → <b>Apply XPU</b> from the pop-up menu.

**Note:** If you are updating groups of agents, make sure that you apply updates to agents that are of the same type.

3. To verify the progress, right-click the active group, and then select **Properties** from the pop-up menu.

The Properties window for the current group appears.

**Note:** You must view the progress of updates, including individual policy updates, at the group level.

4. Select the **Command Jobs** icon from the left column, and then do the following:

<b>To view the...</b>	<b>Then do this....</b>
cumulative progress of the updates	View the top pane of the Command Jobs window. The progress of the entire group is displayed in a single status bar.
progress for each agent update	View the bottom pane of the Command Jobs window. The progress for an individual agent is provided in a separate status bar under the <b>Activity</b> tab. When an update finishes, the job that corresponds to this update is removed from the list.

5. If you want to review the progress of a command job after it has completed, right-click the command job, and then select **Open** from the pop-up menu.
6. If you want to stop or rerun an update, right-click the command job that corresponds to the update that you want to run, and then select one of the following options from the pop-up menu:
  - **Cancel**
  - **Rerun**



---

## Verifying an Agent's Update History

**Introduction** After you apply an update or group of updates, you may need to verify details of the command job or determine whether it was run successfully. The SiteProtector system provides a detailed history of updates that have been applied to an agent or group of agents in the Command Jobs window.

**Procedure** To verify an agent's update history:

1. Right-click the agent, component, or active group folder and then select **Properties** from the pop-up menu.  
The Properties window appears.
2. Select the **Command Jobs** icon from the left column.  
A list of command jobs appears in the Command Jobs window.
3. Sort the **Command** column so that the **Apply XPU** commands appear first in the list, and then locate the job that you want to view.
4. Right-click the job that you want to view, and then select **Open** from the pop-up menu.
5. Expand the Apply XPU window to navigate to the details of each individual update.

## Removing Agent Security Content

### Introduction

Security content updates can sometimes cause agents to perform in ways that you do not expect. To alleviate this, the SiteProtector system lets you remove security content that was last applied to an agent without affecting software updates.

**Important:** The procedure in this topic applies only to certain agents. To determine whether this option is available for an agent, right-click the agent in the Agent view, and then verify that the Remove Last XPU option is available from the pop-up menu.

### How it works

The Remove Last XPU option removes the update or group of updates that was last applied to this agent or, in other words, returns each agent to the XPU state that existed before the last update.

### Why the Remove Last XPU option does not always remove updates?

Because there is a limit to the number of updates you can remove from an agent, the Remove Last XPU option may not always remove updates, as illustrated in the example in Table 30.

Stage	Action	Result
1	Apply security update 1.2 to the following agents: <ul style="list-style-type: none"> <li>Agent A (1.0)</li> <li>Agent B (1.1)</li> </ul>	<ul style="list-style-type: none"> <li>Agent A (1.2)</li> <li>Agent B (1.2)</li> </ul>
2	Apply security update 1.3 to Agent A (1.2) only	<ul style="list-style-type: none"> <li>Agent A (1.3)</li> <li>Agent B (1.2)</li> </ul>
3	Remove Last XPU from the following agents: <ul style="list-style-type: none"> <li>Agent A (1.3)</li> <li>Agent B (1.2)</li> </ul>	<ul style="list-style-type: none"> <li>Agent A (1.2)</li> <li>Agent B (1.1)</li> </ul>
4	Remove Last XPU from the following agents: <ul style="list-style-type: none"> <li>Agent A (1.2)</li> <li>Agent B (1.1)</li> </ul>	<ul style="list-style-type: none"> <li>Agent A (1.0)</li> <li>Agent B (1.1)</li> </ul>

**Table 30:** Example that illustrates a series of updates that are applied to a group of agents

**Note:** When the Remove Last XPU option is applied to Agent B in Stage 4, no remaining updates can be removed from this agent. Therefore, Agent B’s version does not change.

**Procedure**

To remove a security content update from an agent:

1. Open the **Agent** view.
2. Do one of the following:

<b>If you want to remove updates from...</b>	<b>Then do this...</b>
a single agent in the <b>Agent</b> view	Right-click the agent that you want to update, and then select <b>Updates → Remove Last XPU</b> from the pop-up menu.
multiple agents in the <b>Agent</b> view	Use the Windows shift-click (or cntrl-click) command to select agents you want to update, right-click the agents, and then select <b>Updates → Remove Last XPU</b> from the pop-up menu.
a folder in the grouping tree	Right-click the group that you want to update, and then select <b>Updates → Remove Last XPU</b> from the pop-up menu.

**Note:** If you are updating groups of agents, make sure that you apply updates to agents that are of the same type.

3. To verify the progress of the removal job, right-click the active group, and then select **Properties** from the pop-up menu.

The Properties window appears.

**Note:** You must view the progress of update removal jobs, including individual jobs, at the group level.

4. Select the **Command Jobs** icon from the left column, and then view the status bar in the top pane to verify the progress of the removal job.
5. Select the **Command Jobs** icon from the left column, and then do the following:

<b>To view the...</b>	<b>Then do this....</b>
cumulative progress of the removal jobs	View the top pane of the Command Jobs window. The progress of the entire group is displayed in a single status bar.
progress for each removal job	View the bottom pane of the Command Jobs window. The progress for an individual agent is provided in a separate status bar under the <b>Activity</b> tab. When an update finishes, the job that corresponds to this update is removed from the list.

6. If you want to review the progress of a command job after it has completed, right-click the command job, and then select **Open** from the pop-up menu.
7. If you want to stop or rerun a removal job, right-click the command job that corresponds to the one that you want to configure, and select one of the following options from the pop-up menu:
  - **Cancel**
  - **Rerun**



# SECTION D: Applying Updates without XPU Server Internet Access

## Overview

### Introduction

This section provides information about a manual method for updating the SiteProtector system and other IBM ISS products. The method described in this section is intended for customers whose XPU Server is not configured with Internet access. This method requires that you manually download the required update files, store them in the correct folders, and apply the updates manually.

### In this section

This section contains the following topics:

Topic	Page
Update Process without XPU Server Internet Access	110
Downloading Update Files with the Manual Upgrader	111
Downloading Update Files from the IBM ISS Download Center	112
Copying Update Files to the XPU Server	114
Manually Refreshing Component or Agent Status	117
Updating the Update Server and the Event Archiver	118

## Update Process without XPU Server Internet Access

### Introduction

The manual process for updating the SiteProtector system components and agents is complex and can take a significant amount of time to finish. This topic provides an overview of the manual update process.

### Process

Table 31 describes the tasks required to update components and agents manually.

Stage	Description
1	<p>Configuring the XPU Server.</p> <p>Turn off automatic downloads in the XPU Server settings. This action prevents the SiteProtector system from deleting the catalog file you manually put on the Application Server.</p> <p>See “Configuring the XPU Settings Policy” on page 75.</p>
2	<p>Downloading the files to your computer.</p> <p>Use the Manual Upgrader utility to download the required update files to a computer that has access to the Internet. This computer does not have to be a computer where the SiteProtector system is installed.</p> <p>See “Downloading Update Files with the Manual Upgrader” on page 111.</p> <p><b>Note:</b> As an alternative, you can download the files individually from the IBM ISS Download Center, but you must identify each required file and copy it to the required subdirectories manually. See “Downloading Update Files from the IBM ISS Download Center” on page 112.</p>
3	<p>Setting up the file storage on your computer.</p> <p>Copy the required update files to the computer where the XPU Server resides. You can copy the files to either of the following:</p> <ul style="list-style-type: none"> <li>• The integrated XPU Server on the Application Server</li> <li>• A stand-alone XPU Server</li> </ul> <p>See “Copying Update Files to the XPU Server” on page 114.</p>
4	<p>Refreshing the SiteProtector system components and agents to refresh the status level.</p> <p>Restart the Sensor Controller service to refresh the status of your SiteProtector system components and agent.</p> <p>See “Manually Refreshing Component or Agent Status” on page 117.</p> <p><b>Note:</b> This stage happens automatically (without a restart) according to the schedule set in SP Core Properties.</p>
5	<p>Updating the components and agent updates.</p> <p>Update the SiteProtector system components and agents with the update files you downloaded.</p> <ul style="list-style-type: none"> <li>• See “Applying Updates to SiteProtector System Components” on page 97.</li> <li>• See “Updating Agents” on page 289.</li> </ul>

**Table 31:** *Tasks for manually updating agents and components*

# Downloading Update Files with the Manual Upgrader

## Introduction

The Manual Upgrader is a utility that you can use to retrieve update files from the IBM ISS Download Center, including the following:

- XPU's for agents
- XPU's for policies
- service packs
- OneTrust licenses

You might use the Manual Upgrader if the XPU Server cannot access the IBM ISS Download Center for any reason. The utility is available on the IBM ISS Download Center in the Other Section of the SiteProtector system area.

## Advantages of the Manual Upgrader

An update to the SiteProtector system often requires a large number of files. That number may increase substantially depending on the number of agents at the Site. The Manual Upgrader offers the following advantages over downloading the files individually:

- The Manual Upgrader identifies all the packages and downloads all the files you need, including those for any prerequisites.
- The Manual Upgrader saves each file in the subdirectory where it is needed to perform the update.
- The Manual Upgrader is scriptable so you can create a job to run it daily. See the Read Me file for the Manual Upgrader for detailed instructions.

## Installing the Manual Upgrader

To install the Manual Upgrader:

1. Obtain the Manual Upgrader installation file from one of the following locations:
  - Product CD  
The file is located in the following folder:  
`\accessories\ManualUpgrader`
  - IBM ISS Download Center  
The file is located in the SiteProtector system area under "Other Downloads."
2. Copy the file to a computer that has Internet access.
3. If you obtained the file from the IBM ISS Download Center, then you must extract the zip file to a directory.  
**Note:** If you enable the Use Folder Names option when you extract the zip file, then the program extracts the files to a directory called "ManualUpgrader."  
The Manual Upgrader is available to use.

## Running the Manual Upgrader

To run the Manual Upgrader:

1. On the computer where you installed the utility, navigate to the folder that contains the program.
2. To complete the process, refer to the Read Me file that comes with the Manual Upgrader.

## Downloading Update Files from the IBM ISS Download Center

**Introduction** This topic explains how to download update files from the IBM ISS Download Center.

**File name requirements** Some programs, such as Internet Explorer and WinZip, automatically add a .zip extension to file names when they download files. The XPU Server cannot locate files with a .zip extension. If you use a program such as Internet Explorer or WinZip to download the update files, then you must rename the files after you download them and remove the .zip extension.

**License requirements** You can only download update files that are released prior to the expiration date for the maintenance agreement for your agents and components. If you do not see an XPU listed on the IBM ISS Download Center or if you are unable to see the XPU after you download the file, then you should check the maintenance expiration date on the license to ensure that it has not expired.

**Locating files** Table 32 lists the locations of update files on the IBM ISS Download Center Web page.

Files	How files are listed
Agent XPUs	Agent XPUs are listed by their product name and version number.
Policy XPUs	Policy XPUs are listed under the SiteProtector system section by their product name and version number.
Service packs	Service packs are listed by their product name and version number.

**Table 32:** Location of update files

**Required files for SiteProtector system components** Table 33 lists the required files that you must download when you are updating SiteProtector system components.

Component	Cumulative Updates	Required Files
SiteProtector Core	No	Service Pack
Agent Manager	No	Service Pack
Site Database	No	Service Pack XPU
Event Collector	No	Service Pack
Deployment Manager	No	Service Pack
SecurityFusion	No	Agent XPU Policy XPU

**Table 33:** Required files for SiteProtector system component updates



**Required files for agents**

Table 34 lists the required files that you must download when you are updating agents that use policies.

Product	Cumulative Update	Required Files
Network Sensor	Yes	Agent XPU Policy XPU
Server Sensor	Yes	Agent XPU Policy XPU
Proventia appliances	Yes	Database Service Packs
Proventia Desktop	Yes	Database Service Packs
Network Internet Scanner	No	Agent XPU Policy XPU

**Table 34:** *Required files for IBM ISS agent updates*

## Copying Update Files to the XPU Server

### Introduction

After you download the required files to update the agent or the SiteProtector system component, you must copy the files to the appropriate directory on the computer where the XPU Server is installed. You can use either the integrated XPU Server that is installed on the same computer as the Application Server or an XPU Server that is installed on a separate computer.

If you did not download the required files to the computer where the XPU Server is installed, then you must transfer the files to that computer.

### Required directories

You must copy the required files to specific directories on the computer where the XPU Server is installed. If these directories do not exist, then you must create them before you can apply the updates.

**Important:** When you create the directories, you must spell and capitalize the directory names exactly as described in this topic. The directories described in this topic assume that you are creating the directories on the integrated XPU Server.

If you are creating the directories on a remote XPU Server, then you must create the directories in the following directory on the computer where the remote XPU Server is installed:

```
\Program Files\ISS\SiteProtector\X-Press Update  
Server\webserver\Apache2\htdocs\XPU\
```

**Note:** The Manual Upgrader creates all subdirectories in the correct relative paths. Copy them to the `\htdocs\XPU\` path as is.

**Required directories for SiteProtector system components**

Table 35 lists the required directories for update files and OneTrust license files for the SiteProtector system.

Update File	Required Directory
Site Database updates	\Program Files\ISS\SiteProtector\Application Server\webserver\Apache2\htdocs\XPU\SiteProtector Example filenames: DB_XPU_ DB_SP
SiteProtector system component updates and service packs	\Program Files\ISS\SiteProtector\Application Server\webserver\Apache2\htdocs\XPU\SiteProtector Example filenames: DepMan_ RSEvntCol69_ AgentManager69_ SP2_
Catalog Files	\Program Files\ISS\SiteProtector\Application Server\webserver\Apache2\htdocs\XPU\SiteProtector Example filenames: XPU_2_6.xml RiskIndex.xml

**Table 35:** *Required directories for update files*

**Required directories for agents**

Table 36 lists the required directories for agents.

<b>Update File</b>	<b>Required Directory</b>
Network Sensor non-policy updates	\Program Files\ISS\SiteProtector\Application Server\webserver\Apache2\htdocs\XPU\RealSecure Example filename: RSNetSnsr70_MU_
Server Sensor non-policy updates	\Program Files\ISS\SiteProtector\Application Server\webserver\Apache2\htdocs\XPU\RealSecure Example filename: RSSvrSnsr70_MU_
Proventia Network IPS and Proventia Network IDS updates	\Program Files\ISS\SiteProtector\Application Server\webserver\Apache2\htdocs\XPU\RealSecure
Proventia Network IPS non-policy updates	\Program Files\ISS\SiteProtector\Application Server\webserver\Apache2\htdocs\XPU\Proventia\G-Series
Proventia Network MFS non-policy updates	\Program Files\ISS\SiteProtector\Application Server\webserver\Apache2\htdocs\XPU\Proventia\M-Series
Network Internet Scanner non-policy updates	\Program Files\ISS\SiteProtector\Application Server\webserver\Apache2\htdocs\XPU\InternetScanner Example filename: XPressUpdate7_
Catalog Files	\Program Files\ISS\SiteProtector\Application Server\webserver\Apache2\htdocs\XPU\SiteProtector Example filenames: XPU_2_5.xml RiskIndex.xml
Policy updates	\Program Files\ISS\SiteProtector\Application Server\webserver\Apache2\htdocs\XPU\SiteProtector Example filenames: SPIS_POLICY_ SPNS_POLICY_ SPSS_POLICY_ SPIA_POLICY_

**Table 36:** Required directories for update files

---

# Manually Refreshing Component or Agent Status

**Introduction** Restarting the Sensor Controller ensures that the agents and components show the correct status, "Out of Date," in the Console.

**Note:** The SiteProtector system updates a status automatically according to the schedule that you set in SP Core Properties. You must restart the Sensor Controller only if you need to update a status immediately.

**Before you begin** Before you restart the Sensor Controller, verify that no scheduled command jobs are running. If you restart the Sensor Controller while the command jobs are running, then the jobs will fail.

**Procedure**

- On the Application Server, restart Sensor Controller Service using Windows service management.

**Note:** After you restart the Sensor Controller, the status of the agents and components should change to "Out of Date." If the status changes to "Unknown," then the Sensor Controller will re-read the catalog file to determine what updates are available and update the statuses.

## Updating the Update Server and the Event Archiver

**Introduction** Follow the instructions in this topic to update the Update Server and the Event Archiver.

**Prerequisite** Before you update the Update Server or the Event Archiver, do the following:

1. Download all available updates and catalog files and download your OneTrust tokens using the ISS Download Center (page 112) or the Manual Upgrader (page 111).
2. Import the OneTrust tokens and license documents into the OneTrust licensing dialog.

### Updating the Update Server

To update the Update Server:

1. Open an **Agent** tab in the Console, and then select the group containing the Update Server that you want to update.
2. Right-click the Update Server, then select **Manage Policy**.
3. In the right pane, right-click the **Server Settings** policy, and then click **Open**.
4. Clear the **Download from other X-Press Update Servers** check box.
5. In the navigation pane, select the Update Server again.
6. In the right pane, right-click the **XPU Settings** policy, and then click **Open**.
7. On the **XPU** tab, clear the **Download updates automatically** check box.
8. On the same tab, verify that the **Install updates automatically** check box is selected.
9. Save the policies, and then Deploy your policy changes to the Update Server.
10. Refresh the Update Server agent.
11. Copy `XPU_5_1.xml` to the Update Server's `\XpuSelf` directory.
  - For the Update Server on the Application Server:

```
\ISS\SiteProtector\Application
Server\webserver\Apache2\XpuSelf\SiteProtector
```
  - For a standalone Update Server:

```
\ISS\SiteProtector\X-Press Update
Server\webserver\Apache2\XpuSelf\SiteProtector
```
12. Create a directory named `UpdateServer` in the path from Step 11.
13. Copy the Update Server update files into the `UpdateServer` directory that you just created.
14. If you want to update your Update Server immediately, restart the **SiteProtector Web Server** service on the Update Server computer.

**Note:** If you do not restart the server, the Update Server is updated the next time its self-update process runs, which is every 24 hours by default.

### Updating the Event Archiver

To update the Event Archiver:

1. Open an **Agent** tab in the Console, and then select the group containing the Event Archiver that you want to update.
2. Right-click on the Event Archiver, then select **Manage Policy**.

3. In the right pane, right-click the **XPU Settings** policy, and then click **Open**.
4. On the **XPU** tab, clear the **Download updates automatically** check box.
5. On the same tab, verify that the **Install updates automatically** check box is selected.
6. Save the policy, and then Deploy your policy changes to the Event Archiver.
7. Refresh the Event Archiver agent.
8. Copy XPU\_5\_1.xml to the Event Archiver's XpuSelf directory:  
    \ISS\SiteProtector\Event Archiver\XpuSelf\SiteProtector
9. Create a directory named EventArchiver in the path from Step 8.
10. Copy the Event Archiver update files into the EventArchiver directory that you just created.
11. If you want to update your Event Archiver immediately, restart the "SiteProtector Event Archiver" service on the Event Archiver computer.  
**Note:** If you do not restart the server, the Event Archiver is updated the next time its self-update process runs, which is every 24 hours by default.





## Chapter 9

# Configuring Event Collectors

## Overview

### Introduction

The Event Collector is configured to function without any additional configuration. The tasks in this chapter are optional. These tasks are intended for customers who want to implement Event Collector failover and customize the Event Collector settings.

### In this chapter

This chapter contains the following topics:

Topic	Page
What is the Event Collector?	122
Assigning Event Collectors Manually	123
Event Collector Failover Process	124
Configuring Event Collectors for Failover	125

## What is the Event Collector?

### Introduction

The Event Collector gathers security data generated by an agent and directs the data to the SiteProtector Database for storage and processing. Agents pass security data to the Event Collector in real-time. There is no persistent storage on the agents. If the agent loses communication with the Event Collector, the agent caches the security data until it reestablishes communication with the Event Collector.

### Agents and components

An Event Collector is assigned to the following SiteProtector system components and agents:

#### Agents

- Databridge for System Scanner vulnerability assessment application
- Network Internet Scanner
- Network Sensor
- Proventia Network IPS
- Proventia Network IDS
- Server Sensor

#### SiteProtector system components

- Deployment Manager
- Other Event Collectors
- SecurityFusion module
- Third Party Module
- Agent Managers

### Assigning Event Collectors

Table 37 describes the methods for assigning Event Collectors to agents.

Method	Description
Manual	You can manually assign an Event Collector to an agent at any time. <b>Reference:</b> See “Assigning Event Collectors Manually” on page 123.
Auto-Assignment with Deployment Manager	When you install an agent with Deployment Manager, the agent is automatically assigned an Event Collector as follows: <ul style="list-style-type: none"> <li>• The Deployment Manager creates a registration file for the agent.</li> <li>• The Sensor Controller retrieves the registration file, processes it, and then assigns an Event Collector to the agent.</li> <li>• If you have more than one Event Collector, then the Site Database chooses the Event Collector with the fewest number of agents assigned to it.</li> </ul> <b>Reference:</b> See “Installing Agents with the Deployment Manager” on page 269.
New Agent Wizard	When you use the New Agent Wizard to register an agent with the Site, you select an Event Collector to assign to the agent. <b>Reference:</b> See “New Agent Wizard” on page 274.

**Table 37:** *Methods for assigning Event Collectors to agents*

---

# Assigning Event Collectors Manually

## Introduction

The topic explains how to assign an Event Collector manually to an agent or a SiteProtector system component:

If an agent loses its connection with an Event Collector for any reason, then you can perform this procedure to reassign an Event Collector. If your Event Collectors are configured for failover, then you can perform this procedure to fail back to the primary Event Collector after it is restored.

## Procedure

To assign an Event Collector to an agent manually:

1. In the left pane, select the group that contains the agent.
2. In the **Go to** list, select **Agent**.
3. Select the agent.
4. Click **Actions**→**Configure Agents**→**Assign Event Collector**.
5. Select the Event Collector, and then click **OK**.

## Event Collector Failover Process

- Introduction** Event Collector failover is the process of automatically directing events to a secondary Event Collector if the primary Event Collector becomes unavailable.
- Data preservation** Agents are capable of storing events on the computer where the agent is installed until an Event Collector becomes available. This approach ensures that you do not lose important security data while the Event Collector is unavailable.
- Process** Table 38 describes the stages of the Event Collector failover process.

Stage	Description
1	The Site Database performs an initial check on the primary Event Collector's status at the rate of one check every 10 minutes. You can change the frequency of the initial check using the Daily Frequency parameter.
2	If the Site Database detects that primary Event Collector status is any one of the following, then the Site Database fails over to the secondary Event Collector: <ul style="list-style-type: none"> <li>• not responding</li> <li>• unknown</li> <li>• stopped or stopping</li> <li>• paused or pausing</li> <li>• error</li> <li>• offline</li> </ul>
3	The Site Database continues to perform subsequent checks on the primary Event Collector's status at the rate of one check every 5 minutes until it is available again, and then it fails back to the primary Event Collector. You can change the frequency of the subsequent check using the WAITFORDELAY parameter.
4	When the primary Event Collector becomes available again, you manually redirect the agents back to the primary Event Collector.

**Table 38:** *Event Collector failover process*

# Configuring Event Collectors for Failover

**Introduction** This topic explains how to configure Event Collectors for failover.

**Prerequisites** Before you configure Event Collectors for failover, you must complete the following tasks:

- Use the Deployment Manager to install an additional Event Collector; this Event Collector serves as the secondary “backup” Event Collector.  
See the *SiteProtector System Installation Guide*.
- Verify that the Application Server is set up as a key administrator on the secondary Event Collector.
- Obtain the following database scripts from the IBM ISS product CD, and then put them in any directory on the Site Database:
  - Accessories\ECAutoFailover\AutoChangeECid.sql
  - Accessories\ECAutoFailover\CreateSP.bat
  - Accessories\ECAutoFailover\ECJob.sql

**Parameters** Table 39 describes the parameters that control the frequency with which the Site Database checks the primary Event Collector’s status.

Parameter	Description
Daily frequency	Controls how often the SiteProtector system performs the initial check of the primary Event Collector’s status. <b>Default:</b> One check every 10 minutes
WAITFORDELAY	Controls how often the SiteProtector system performs the subsequent checks of the primary Event Collector’s status after it becomes unavailable. <b>Default:</b> One check every 5 minutes

**Table 39:** *Parameters*

## Configuring a secondary Event Collector

To configure a secondary Event Collector:

1. On the Site Database, open a Windows command prompt, and then run the `CreateSP.bat` script.
2. Start the Microsoft SQL Enterprise Manager.
3. Select the **Tree** tab, and then expand the server group and server that contain the Site Database.
4. Expand the Management folder, expand **SQL Server Agent**, then select **Jobs**.
5. Double click the `AutoChangeECid.sql` job in the table on the right pane.  
The AutoChangeECid Properties window appears.
6. Click the **Steps** tab, and then double click the first row in the table (ID 1).  
The Edit Job Step window appears.

7. In the **Command** field, designate the primary and secondary Event Collector as follows, and then click **OK**.
  - replace `Event_Collector_A` with the name of the primary Event Collector
  - replace `Event_Collector_B` with the name of the secondary Event Collector

**Example:** `ATL100_EC01`
8. To change how often the database performs initial checks on the primary Event Collector's status:
  - Click the **Schedules** tab, and then double click the first row in the **Command** field.
  - Click **Change**.
  - Set the **Occurs every \_\_minute** field as appropriate, and then click **OK**.
9. To change how often the Site Database performs subsequent checks on the primary Event Collector's status:
  - Select the **Tree** tab, and then expand the server group and server that contains the Site Database.
  - Select **Databases** → **RealSecureDB** → **Stored Procedures**.
  - Right-click the `dbo.iss_AutoChangeECid` script, and then select **Edit** from the menu.
  - Locate the following line in the script:

```
'WAITFORDELAY '00:05:00'
```
  - Set how often you want the Site Database to perform the subsequent checks in the following parameter:

```
'00:05:00'
```

**Example:** For 1 check every 10 minutes, type the following:

```
'00:10:00'
```
  - Select **Query** → **Execute**.

## Chapter 10

# Enabling the Event Viewer

## Overview

### Introduction

This chapter provides information about enabling and using the Event Viewer. You can enable the Event Viewer if you want to view unprocessed security events outside of the SiteProtector Console. The Event Viewer is designed primarily for troubleshooting.

### In this chapter

This chapter includes the following topics:

Topic	Page
What is the Event Viewer?	128
Enabling the Event Viewer	129
Starting the Event Viewer	130

## What is the Event Viewer?

- Introduction** The Event Viewer is a program that runs independently from the Console and provides an alternative method for viewing events that are generated by the Event Collector.
- Secure communication** Communication between the Event Collector and the Event Viewer is always authenticated and encrypted.
- Overview process** Table 40 describes the process of transmitting events from the Event Collector to the Event Viewer.

Stage	Description
1	The Event Collector generates event log files.
2	The Event Viewer connects to the Event Collector.
3	The Event Viewer retrieves events from the event log files on the Event Collector.
4	The Event Viewer filters these events, based on user-defined settings, and then displays them.

**Table 40:** *Event Viewer process*



## Enabling the Event Viewer

**Introduction** This topic tells how to enable the Event Viewer.

**Procedure** To enable the Event Viewer:

1. In the left pane, select the group that contains the Event Collector.
2. In the **Go to** list, select **Agent**.
3. In the right pane, right-click the **Event Collector**, and then select **Properties** from the pop-up menu.  
The Event Collector properties tab appears.
4. Click **Agent Properties**.
5. Click **Edit Agent Properties**.  
The Event Collector Properties window appears.
6. Select the **General** tab, and then click **Advanced**.  
The Advanced Event Collector Configuration window appears.
7. In the Event Collector logging section, set the following options:

Option	Description
Enable event logging to log files	Select this option if you want to view events with the Event Viewer.
E.C. log file directory	Specify a location where you want to save event log files on the Event Collector.
Switch log files	Specify how often you want the Event Collector to create a new log file. You can specify the interval in MB or seconds. <b>Example</b> Create a new log file every 10 MB or 120 seconds.
Automatically clean up old log files	Select this option if you want the SiteProtector system to remove old log entries, and then specify how often you want the Event Collector to remove old log files. You can specify the interval in MB or seconds. <b>Example</b> Remove old log files when the log file directory reaches 500 MB. Remove old log files when log file is older than 10 days.

8. Click **OK**.  
The Event Collector Properties window appears.
9. Click **OK**.
10. Right-click the **Event Collector Properties** tab, and then select **Close**.

## Starting the Event Viewer

### Introduction

This topic explains how to start the Event Viewer from the Console or from the Windows Desktop.

### Starting the Event Viewer from the Console

To start the Event Viewer from the Console:

1. In the left pane, select the group that contains the Event Collector.
2. In the **Go to** list, select Agent.
3. In the right pane, right-click the Event Collector, and then select **Launch → Event Viewer** from the pop-up menu.

The SiteProtector Event Viewer appears.

### Starting the Event Viewer from the Desktop

To start the Event Viewer from the Windows Desktop:

1. Click **Start** on the task bar, and then select **Programs → ISS → SiteProtector → Event Viewer**.

The Login to SiteProtector Event Viewer window appears.

2. Complete the fields as follows:

Field	Description
Event Service	The IP address or URL of the Event Collector computer.
Event Service Port	The port number to use with the Event Collector computer. The default is 3993.
App Server	The IP address or URL of the application server computer.
App Server Port	The port number to use with the Event Collector computer. The default is 3998.
User name	Your SiteProtector user name.
Password	Your SiteProtector password.

3. Click **OK**.

The SiteProtector Event Viewer appears.

## Chapter 11

# Configuring the Site Database

## Overview

**Introduction** The Site Database is designed to perform minimal maintenance tasks automatically. For full maintenance, you must configure the Site Database maintenance options described in this chapter.

**Supported databases** The SiteProtector system supports SQL and MSDE databases.

**Related documentation** For more information about database maintenance, refer to your Microsoft SQL documentation or go to the Microsoft Web site.

**In this chapter** This chapter contains the following topics:

<b>Topic</b>	<b>Page</b>
Viewing Site Database Properties	132
Setting Database Maintenance Options	134
Database Defragmenting	137
Log File Purge	138
Database Table Purge	139
Emergency Database Purge	143
Configuring Database Notifications	145
Automatic Database Backup	147

## Viewing Site Database Properties

### Introduction

This topic provide information about viewing Site Database properties.

### Procedure

To view Site Database properties:

1. In the left pane, select the *Site Node*.
2. In the **Go to** list, select **Agent**.
3. In the right pane, right-click **SiteProtector Database** → **Properties**, and then select **Agent Details** from the pop-up menu.

The Properties tab displays the properties.

### Site Database property descriptions

Table 41 describes the Site Database properties.

Property	Description
License State	Indicates whether the license for this component is valid, such as Key Good.
Sensor Status	Status of the Site Database, such as Active.
Data File Status	Percentage full for the Site Database, such as 6% Full.
Transaction Log Status	Percentage full for the Site Database log file, such as 2% Full.
SQL Server Agent Status	Status of the SQL database that works with the Site Database, such as Running.
Data Load Status	Number of rows of data loaded to the Console, such as 5 rows were loaded on October 1, 2005 1:00PM.
Purge Status	Current status of a purge.
Purge Status Last Updated	Last time the purge ran.
Data Used (MB)	Amount of space used in the Site Database, such as 146 MB.
Auto Maintenance Job	Information about the automatic database maintenance jobs.
Auto Purge Setting	Schedule for the automatic database purge, such as Daily.
Defragment Index Setting	Schedule for the defragment index maintenance job, such as Daily.
Misc Maintenance Settings	Information about other database maintenance jobs, such as Auto Backups: Off; Emergency Purge: On; Recovery Model: simple.
Health Status Last Checked At	Date and time of last database health check.
Version	Version of the Site Database, such as 2.0 (SP 6.0:XPU 1.49).
XPU Status	Software update status, such as Out of Date.
Last Installed XPU	Version of the last software update that was installed, such as XPU 1.49.

**Table 41:** *Site Database property descriptions*

Property	Description
Site Group Name	Name of the top-level group in the Site, such as <i>ComputerName</i> .
Install Date	Date and time that the Site Database was installed, such as Aug 1 2005 1:00PM.
XPU Date	Date and time that the last XPU was applied, such as Aug 1 2005 1:00PM.
Option Flag	Option flag set for the Site Database, such as None.
Logging Level	Type of logging configured for the Site Database, such as Informational.
Last Modified by	Name of component that last modified the Site Database, such as Sensor Controller.

**Table 41:** *Site Database property descriptions (Continued)*

## Setting Database Maintenance Options

### Introduction

This topic explains how to set the database maintenance options.

**Note:** After you set up database maintenance the first time, you can adjust the settings later to accommodate your specific requirements.

### Before you begin

This procedure schedules database backups. Before you schedule or run the database backup job, you must set up a backup device. If you do not set up the backup device before you run the backup job, then the SiteProtector system cannot write the files to the correct location and the backup job will fail.

You must also add the backup device each time the backup part drive is changed.

For instructions on how to add a backup device, See “Automatic Database Backup” on page 147.

### Database maintenance time

Set the maintenance to occur during off-peak business hours.

**Default:** The default maintenance time is midnight Sunday EST.

**Time tab:** The Time tab allows you to set the database maintenance time.

### Procedure

To set general database maintenance options:

1. In the left pane, select the group that contains the Site Database.
2. In the **Go to** list, select **Agent**.
3. In the right-pane, right-click **SiteProtector Database** → **Properties**.
4. Click the **Database Maintenance** icon.  
The Database Maintenance options appear.
5. Select the **General** tab, and then set the following options:

Option	Description
Defragment: Frequency	Choose how often you want the SiteProtector system to run the defragmenting job: <ul style="list-style-type: none"> <li>• once daily</li> <li>• once weekly</li> <li>• never</li> </ul> <p><b>Note:</b> If your Site uses Microsoft SQL Server 2005 Enterprise Edition, this option rebuilds the index online instead of defragmenting the index.</p>
Maximum Log Entry Age (in days)	Set the maximum allowed age in days for log entries in the following logs: <ul style="list-style-type: none"> <li>• Analysis log</li> <li>• Message log</li> <li>• Maintenance log</li> </ul>

Option	Description
Maintain risk history data	The SiteProtector system prepares data to be used for the Risk Detail and Risk Summary reports. <b>Note:</b> If you find loading performance is slow and you don't use the risk reports, turn this setting off.

6. Select the **Time** tab, and then set the following options:

Option	Description
Database Maintenance Time	Choose a time zone: <ul style="list-style-type: none"> <li>Locally set time zone</li> <li>Greenwich Mean Time (GMT)</li> </ul>
Weekly maintenance day	For jobs that run once a week, choose the day of the week you want to run the jobs.
Maintenance time of day	For jobs that run once a day, choose the time of day you want to run the jobs.

7. Select the **Purge** tab, and then set the following options:

Option	Description
Emergency Purge	Select this option to enable automatic emergency database purges in the event that the database exceeds the size you specify in the Database Size Threshold.
Database Size Threshold	Set the maximum allowed percentage full for the database. <b>Note:</b> If the database size exceeds this percentage, then the SiteProtector system runs the emergency purge to bring the database size below this percentage.
Purge Margin	Specify the bulk percentage of data that the emergency purge job can remove if necessary to create more space in the database. During a second emergency purge, the job removes data in bulk regardless of the age of the data. See "Emergency Database Purge" on page 143. See "Database Table Purge" on page 139.
Purge Frequency	Choose how often you want to the SiteProtector system to run the database purge job: <ul style="list-style-type: none"> <li>Never</li> <li>Daily</li> <li>Weekly</li> </ul>

Option	Description
Maximum Item Age (in days)	Set the maximum allowed age for items in these tables: <ul style="list-style-type: none"> <li>• Audit</li> <li>• Incidents</li> <li>• Metrics</li> <li>• Cleared observances</li> <li>• Cleared agent data</li> <li>• Resolved tickets</li> <li>• Exceptions</li> <li>• Job history</li> <li>• Observances</li> <li>• Agent data</li> <li>• Unused assets</li> <li>• Mail data</li> </ul>
Purge assets even if grouped	See the description of “Unused Assets” on page 141.

8. Select the **Advanced Purge** tab.
9. To override the maximum age for a specific type of data, select the **Override** check box for the type of data in either the **Agent Data** or **Observances** area, and then type the number of days.
10. Select the **Daily Backup** tab, and then set the following options:

Option	Description
Perform automatic daily backup	Select this option to create daily database backups automatically.
Backup path	Specify the location for database backup files.
Recovery Model	Choose the recovery model you want to use: <ul style="list-style-type: none"> <li>• Simple</li> <li>• Full</li> <li>• Bulk Logged</li> </ul>
Log backup threshold	Specify the log backup threshold.

11. Click **Save All**.
12. Right-click the **SP Database Properties** tab, and then select **Close Tab**.



---

# Database Defragmenting

**Introduction** The database defragmenting job is designed to lower database index fragmentation and to maintain optimum database performance. This job runs automatically on a user-defined weekly or daily schedule. You cannot change the criteria for defragmenting. The defragmenting job runs while the system is in use and does not affect the SiteProtector system performance.

**Note:** If your Site uses Microsoft SQL Server 2005 Enterprise Edition, this option rebuilds the index online instead of defragmenting the index.

**Default settings** The default settings for defragmenting are the same regardless of the installation type. The following options are set by default:

- Enabled
- Runs once weekly
- Defragments indexes with a scan density less than 90%
- Defragments indexes with a logical fragmentation greater than 10%

**General tab** The General tab allows you to set defragmenting frequency.

**Rebuilding indexes** For information about how to rebuild indexes, see the IBM ISS Knowledgebase.

## Log File Purge

### Introduction

The log file purge job is designed to remove out-dated entries from the following log files and prevent the size of these log files from negatively affecting database performance:

- analysis log
- message log
- maintenance log

The purge job runs once every 10 minutes by default and cannot be disabled or rescheduled. The job removes any log entry that is older than the maximum allowed age. The maximum allowed age is user-defined.

### Default settings

Table 42 lists the default settings for the log file purge job by installation type.

Installation Type	Default Setting
Express	The following options are set by default: <ul style="list-style-type: none"> <li>• Enabled</li> <li>• Runs once every 10 minutes</li> <li>• Purges Analysis log entries older than 7 days</li> <li>• Purges Message log entries older than 30 days</li> <li>• Purges Maintenance log entries older than 7 days</li> </ul>
Recommended	The following options are set by default: <ul style="list-style-type: none"> <li>• Enabled</li> <li>• Runs once every 10 minutes</li> <li>• Purges Analysis log entries older than 7 days</li> <li>• Purges Message log entries older than 30 days</li> <li>• Purges Maintenance log entries older than 7 days</li> </ul>

**Table 42:** *Default settings for log file purge*

### General tab

The General tab is where you set the maximum allowed age for log entries.

### Log file descriptions

Table 43 describes the logs purged during a log file purge.

Log File	Description
Analysis log	Contains queries generated by the Analysis tab for diagnostic purposes.
Message log	Contains errors and information messages generated by SQL procedures in the Site database.
Maintenance log	Contains information about the activity of automated maintenance procedures.

**Table 43:** *Log files purged during log file purge*

# Database Table Purge

## Introduction

The database table purge job is designed to remove non-essential data from the following database tables and improve database performance:

- Audit
- Incidents
- Metrics
- Cleared Observances
- Cleared Agent Data
- Resolved Tickets
- Exceptions
- Job History
- Observances
- Agent Data
- Unused Assets

The job does not purge rules associated with incidents and exceptions.

## Default settings

Table 44 lists the default settings for the database table purge job by installation type.

Installation Type	Default Settings
Express	<p>The maximum item age (in days) is set by default as follows:</p> <ul style="list-style-type: none"> <li>• Audit 14 days</li> <li>• Incidents 90 days</li> <li>• Metrics 180 days</li> <li>• Cleared Observances 14 days</li> <li>• Cleared Agent Data 14 days</li> <li>• Resolved tickets 30 days</li> <li>• Exceptions 14 days</li> <li>• Job History 7 days</li> <li>• Observances 90 days</li> <li>• Agent Data 30 days</li> <li>• Unused Assets 30 days</li> </ul>
Recommended	The database table purge job is disabled by default.

**Table 44:** *Default settings for database table purge*

**Tabs**

Table 45 describes the tabs where you set database table purge options.

Tab	Description
Time	Use the Time tab to set the time of day that the job runs.
Purge	Use the Purge tab to set the following options: <ul style="list-style-type: none"> <li>purge frequency (never, daily, or weekly)</li> <li>maximum allowed age for items in the SiteProtector system database tables</li> </ul> <b>Note:</b> The job purges any item older than the user-defined age.
Advanced Purge	Use the Advanced Purge tab to set the maximum allowed age for items in different categories of data. <b>Note:</b> These values you set on the Advanced Purge tab override values you set on the Purge tab. The job purges any item older than the user-defined age.

**Table 45:** *Tabs for setting database table purge options*

**Database tables**

Table 46 describes the data purged and indicates where the data appears in the SiteProtector Console.

Item	Description	Displayed
Audit	Detailed information about user actions in the SiteProtector system.	Audit report
Incidents	Detailed information about events that you designate as incidents.	Analysis view
Metrics	Highly summarized, metric data that requires very little database space.	Summary view
Cleared Observances	Summary information about events that you designate as cleared.	Not displayed
Cleared Agent Data	Events generated by agents such as Network Sensor or Proventia Desktop that you designate as cleared.	Not displayed
Resolved tickets	Tickets that have been resolved.	Ticketing view
Exceptions	Information about events that you designate as exceptions.	Analysis view
Job History	Information about command jobs you run in SiteProtector system such as apply policy, apply update, or scan.	<i>Site Node</i> properties
Observances	Summary information about events.	Analysis view
Sensor Data	Events generated by agents such as Network Sensor or Proventia Desktop.	Analysis view
Mail data	Events generated by Proventia Mail Filter	Analysis view

**Table 46:** *Data types purged during scheduled data purge*

Item	Description	Displayed
Unused Assets	<p>Depends on whether the <b>Purge assets even if grouped</b> check box is selected</p> <p>If the check box is selected, the purge job removes the following:</p> <ul style="list-style-type: none"> <li>• The IP address of any asset that is ungrouped, unregistered, or not referenced in any event, including source IPs, target IPs, and agent IPs</li> <li>• all assets with an Added Date older than the user defined maximum item age</li> <li>• all assets that are not members of a group</li> <li>• all assets with no registered agents</li> <li>• all assets with no events associated with them</li> </ul> <p>If the check box is cleared, the purge job removes the following:</p> <ul style="list-style-type: none"> <li>• The IP address of any asset that is unregistered, or not referenced in any event, including source IPs, target IPs, and agent IPs</li> <li>• all assets with an Added Date older than the user defined maximum item age</li> <li>• all assets with no registered agents</li> <li>• all assets with no events associated with them</li> </ul>	Asset view

**Table 46:** Data types purged during scheduled data purge (Continued)

## Recommendations

The amount of data the Site Database stores and processes has a large impact on database performance. When the database receives a request for information, the database must determine the best way to retrieve the data, and then read the data from tables to provide the results. These operations involve using CPU, memory, and disk access.

The best way to improve database performance is to store only essential and necessary data in the database. IBM ISS recommends that you use the default settings for maximum item age. If you choose to change these settings, then follow these recommendations:

- Keep observances longer than you keep cleared observances.
  - Observances Maximum Item Age = 90 days
  - Cleared Observances Maximum Item Age = 14 days
- Keep sensor data longer than you keep cleared sensor data.
  - SensorData Maximum Item Age = 90 days
  - Cleared SensorData Maximum Item Age = 14 days

## Changing maximum item ages

To change the maximum item ages:

1. In the left pane, select the group that contains the Site Database.  
In the **Go to** list, select **Agent**.
2. In the right pane, right-click the **Site Database**, and then select **Properties**.  
The Site Database Properties tab appears.

3. Click the **Database Maintenance** icon.  
The Database Maintenance tabs appear.
4. Select the **Purge** tab, and then change the Maximum Item Age (in days) fields.
5. If you want to apply the purge settings to assets that belong to one or more groups, select the **Purge assets even if grouped** check box.
6. Click **Save All**.
7. Right-click the **Site Database Properties** tab, and then select **Close Tab** from the pop-up menu.

# Emergency Database Purge

## Introduction

The emergency database purge job is designed to prevent the database from becoming full and keeps the database size within a certain user-defined size limit. The job runs only if the database size exceeds the user-defined size limits and continues to run once every 10 minutes until the database size is within the user-defined size limitations.

## Default Settings

Table 47 lists the default settings for the emergency database purge job by installation type.

Installation Type	Default Setting
Express	The following options are set by default: <ul style="list-style-type: none"> <li>• Enabled</li> <li>• Database Size Threshold 85%</li> <li>• Purge Margin 5%</li> </ul>
Recommended	This job is disabled by default. <sup>a</sup>

**Table 47:** *Default settings for emergency database purge*

- a. If you do not enable this job, then the SiteProtector system automatically stops the Event Collectors and Agent Managers when the database reaches 85% full. These components remain inactive until you manually create more space in the database.

## Purge tab

Use the Purge tab to enable or disable the emergency database purge job and set the options described in Table 48.

Option	Description
Database Size Threshold	The percentage full the database size must exceed before the emergency database purge job begins.
Purge Margin	The emergency database purge job first removes data from the database based on the age of the data. If this purge does not bring the database size below the Database Size Threshold, then the job begins purging data from the database in bulk regardless of the age of the data. The Purge Margin is the percentage of data that the job can remove during a single purge. For example, if you set the Purge Margin to 5%, then the purge job can remove 5% of data from the database regardless of the age of the data.

**Table 48:** *Tabs for setting emergency database purge options*

## Enabling an emergency database purge

To enable an emergency database purge:

- In the left pane, select the group that contains the Site Database.  
In the **Go to** list, select **Agent**.
- In the right pane, right-click the **Site Database**, and then select **Properties**.  
The Site Database Properties tab appears.
- Click the **Database Maintenance** icon.  
The Database Maintenance tabs appear.
- Select the **Purge** tab, and then select the Emergency Purge check box.

5. Set the following options:

<b>Option</b>	<b>Description</b>
Database Size Threshold	The percentage full the database size must exceed before the emergency database purge job begins.
Purge Margin	The emergency database purge job first removes data from the database based on data age. If this purge does not bring the database size below the Database Size Threshold, then the job begins purging data from the database in bulk regardless of the age of the data. The Purge Margin is the percentage of data that the job can remove during a single purge. For example, if you set the Purge Margin to 5%, then the purge job can remove 5% of data from the database regardless of the age of the data.

6. Click **Save All**.
7. Right-click the **Site Database Properties** tab, and then select **Close Tab** from the pop-up menu.



# Configuring Database Notifications

## Introduction

In enterprise environments, the Site database can reach capacity long before you expect it. To stay abreast of these changes, you can configure the SiteProtector system to alert you when the SiteProtector system purges the database or when the database size thresholds that you specify are exceeded.

Use the procedure in this topic to specify database notifications and the way in which these notifications are communicated to your security staff, including email and SNMP responses.

## Component rules

You must configure a component rule to specify database notifications. The Database Status Notification option is a preconfigured response that is available in the Component Rules tab of your site's Central Responses policy.

## Procedure

To configure a database notification:

1. Select the **Policy** view.
2. Check to make sure **Central Responses** is selected in the **Agent Type** list.
3. Select the Site group in the grouping tree.
4. In the right pane, right-click **Response Rules**, and then select **Open Policy** from the pop-up menu.  
The contents of the Response Rule policy is displayed in the right pane.
5. Select the **Component Rules** tab, and then click the **Add** icon.  
The Add Component Rule window appears.
6. Select the **Enabled** box, and then select the **Filters** tab.
7. Type the name of this response rule in the **Name** box, and then select **Database Status Notification** from the list.
8. Do the following:

If you want the SiteProtector system to notify you when the Site database...	Then...
reaches a specified size	select <b>Enable Size Threshold Exceeded Notification</b> box, and then use the slider to specify the database size limit that will enable this notification
is automatically purged	select the <b>Purge</b> box

9. Select the **Responses** tab.
10. Select the **Response Frequency** check box, and then type or select the appropriate values for **Send at most [n] responses within [n] [time period]**.  
**Note:** The default is one response within 60 seconds. If you do not specify a response frequency, then the SiteProtector system sends a notification every time the rule is matched.
11. Complete one or more of the following tasks:  
**Note:** If you do not see the e-mail, SNMP, or user-specified information you want to associate with this rule in the list, click **Manage Responses** to add it to the list. See

Section B, “Configuring Site-level Responses” in the *SiteProtector System Policies and Responses Configuration Guide*.

- Select the **Email** tab, and then select the check box in the **Enabled** column for the e-mail response to associate with this rule.
- Select the **SNMP** tab, and then select the check box in the **Enabled** column for the SNMP response to associate with this rule.
- Select the **User-Specified** tab, and then follow the instructions for “Configuring Log Evidence Settings in the Response Objects Policy” in the *SiteProtector System Policies and Responses Configuration Guide*.

# Automatic Database Backup

## Introduction

The automatic database backup job is designed to archive data in the Site Database called RealSecureDB only. The backup does not include data from the following databases:

- MasterDB
- model
- msdb

**Important:** IBM ISS strongly recommends that you implement a system to back up these databases.

Backing up the database can help you restore the following:

- data that is purged during automatic database maintenance
- databases that are damaged or corrupted

## Requirements

Before you schedule or run the database backup job, you must set up a backup device. If you do not set up the backup device before you run the backup job, then the SiteProtector system cannot write the files to the correct location and the backup job will fail. You must also add the backup device each time the backup part drive is changed.

For instructions on how to add a backup device, see the procedure called *Adding a backup device* in this topic.

## Default Settings

Table 49 lists the default settings for the automatic database backup job by installation type.

Installation Type	Default Settings
Express	The automatic database backup job is disabled by default.
Recommended	The automatic database backup job is disabled by default.

**Table 49:** *Default settings for database table purge*

## Tabs

Table 50 describes the tabs where you set automatic database backup options.

Tab	Description
Time	Use the Time tab to set the time of day that the job runs <sup>a</sup> .
Daily Backup	Use the Daily Backup tab to set the following options: <ul style="list-style-type: none"> <li>● The location where you want to save the backup files (Backup Path)</li> <li>● The recovery model you want to use to restore the database if necessary (simple, full, or bulk logged)<sup>b</sup></li> <li>● The log backup threshold</li> </ul>

**Table 50:** *Tabs for setting automatic database backup options*

- a. Schedule automatic database backups to run during off-peak hours to prevent a negative impact on SiteProtector system performance.
- b. The recovery model determines the types of database backups created and the frequency the backups are created. See Recovery Models.

**Recovery models**

Table 51 describes the SQL database recovery models that the automatic database backup job supports.

Model	Description	Backups and Frequency
Simple	This method has the following advantages: <ul style="list-style-type: none"> <li>• fast database performance</li> <li>• low space requirements for backup files and transaction logs</li> <li>• easy to implement</li> <li>• low processing requirements</li> </ul>	A full backup is created once daily every day.
Full	This method has the following disadvantages: <ul style="list-style-type: none"> <li>• high space requirements for routine operations</li> <li>• high space requirements for backup files and transaction logs (up to four times the size of the database)</li> </ul>	Backups are created as follows: <ul style="list-style-type: none"> <li>• A full backup is created once weekly.</li> <li>• Differential backups are created once a day every day.</li> </ul>
Bulk Logged	This method has the following advantages and disadvantages: <ul style="list-style-type: none"> <li>• moderate space requirements for routine operations</li> <li>• high space requirements for backup files and transaction logs (up to four times the size of the database)</li> </ul>	Backups are created as follows: <ul style="list-style-type: none"> <li>• A full backup is created once weekly.</li> <li>• Differential backups are created once a day every day.</li> </ul>

**Table 51:** *SQL recovery models*

**Reference:** For more information about the three recovery models, including the advantages and disadvantages of each, refer to the Microsoft SQL documentation.

**Adding a backup device**

This procedure describes how to add a backup device to the SQL Server database. You must be an SQL Server System Administrator (SA) to perform this procedure. If you are using MSDE, then you do not have a full version of SQL Server and you must use the Command prompt to run the SQL Server script in this procedure. To add a backup device:

1. Log on as SQL Server System Administrator (SA) on the Site Database computer.
2. Open the SQL Server Analyzer tool on the Site Database computer.
3. In the SQL Server window, type the following:

```
USE RealSecureDB
Go
EXEC iss_AddBackupDevice
```

4. Click the **Execute** icon.

The output appears in the bottom window and lists the devices removed and added.

5. Close the window.
6. Start the SiteProtector Console, and then login the Site that you want to backup.
7. In the left pane, select the group that contains the Site Database.
8. Verify that the **Status** field for the SiteProtector Database is **Active**.

9. On the Site Database computer, select **Start**→**Programs**→**Microsoft SQL Server**→**Query Analyzer**.
10. Run the `exec sp_helpdevice` command.
11. On the bottom of the page, locate the files beginning with `RealSecureDB_`.  
**Note:** These are the backup files for the database.
12. Verify that the files are pointing to the correct location.



## Chapter 12

# Configuring User Permissions

## Overview

### Introduction

This chapter provides details about the different methods of managing user permissions in a SiteProtector system, including information about the following:

- SiteProtector system user groups
- global permissions
- group-level permissions
- policy permissions

### Requirement

A SiteProtector system includes one default administrator group which contains the Application Server's local Administrators group as member. This is the same user who installs the SiteProtector system. Before other users can connect to Sites and use the Console, you must add the users to your SiteProtector system.

**Note:** IBM ISS recommends that you set up group-level permissions and policy permissions *after* you set up groups, agents, and policies. For more information about these types of permissions, see the following:

- See "Setting up Group-Level Permissions" on page 235.
- See the *SiteProtector System Policies and Responses Configuration Guide*.

### In this chapter

This chapter contains the following sections:

Section	Page
Section A, "SiteProtector System Permission Management"	153
Section B, "SiteProtector System User Groups"	161
Section C, "Global Permissions"	167





# SECTION A: SiteProtector System Permission Management

## Overview

**Introduction** This section provides information about the SiteProtector system's permission management features.

**In this section** This section includes the following topics:

<b>Topic</b>	<b>Page</b>
Methods for Managing Permissions	154
Searching for Users and Groups	156
Permissions Affected by Upgrades	157
Working with Policy Permissions	159

## Methods for Managing Permissions

### Introduction

This topic provides information about the methods available in the SiteProtector system to manage permissions.

### Methods

Table 52 describes the methods for managing permissions in the SiteProtector system and provides examples of each.

Method <sup>a</sup>	Description
SiteProtector system user groups	<p>Use SiteProtector system user groups to assign a set of permissions to a user or group or users. When you add an individual user or group of users to a SiteProtector system user group, the user or users automatically receive all the permissions assigned to that user group. This method provides a quick way to grant an entire set of permissions to a user or group of users. IBM ISS recommends that you manage most user permissions with SiteProtector system user groups.</p> <p><b>Example:</b> Add a user called <i>jsmith</i> to the SiteProtector system user group called <i>Operator</i>. The <i>jsmith</i> user automatically receives all the permissions assigned to the <i>Operator</i> user group. You do not have to assign the permissions individually.</p>
Global permissions	<p>Use global permissions to assign Site-wide permissions to a user or group of users. Global permissions are set at the Site level.</p> <p><b>Example:</b> Grant the global permission called <i>Clear/Restore Events</i> to a user called <i>jsmith</i>. The <i>jsmith</i> user can clear and restore events in the entire Site.</p>
Group-level permissions	<p>Use group-level permissions to assign permissions that are specific to a group of assets. Group-level permissions are set at the asset group level.</p> <p><b>Example:</b> For a group of assets called <i>Atlanta Servers</i>, grant the group-level permission for Network Internet Scanner called <i>Scan-Control</i> to a user called <i>jsmith</i>. The <i>jsmith</i> user can run scans on the assets in this group and/or the <i>jsmith</i> user can run scans using Network Internet Scanner in this group. See "Setting up Group-Level Permissions" on page 235.</p>
Policy permissions	<p>Use the Modify Policy permission to give users the ability to modify an individual policy or response. The Modify Policy permission is granted for individual policies and responses only. See the following for more information: See the <i>SiteProtector System Policies and Responses Configuration Guide</i>.</p>

**Table 52:** *Methods for managing permissions*

- a. Although not recommended, you can use any combination of the methods described here to manage permissions. For example, the user *jsmith* can be a member of a SiteProtector system user group, have global permissions, and have group-level permissions.

### Failover solution

If you plan to set up domain users and domain groups to the SiteProtector system or implement a failover solution, then you must install the Application Server on a computer that has access to the domain. When the Application Server has access to the domain, you can do the following:

- add domain users and domain groups to the SiteProtector system
- look up domain users and domain groups with the Check Names feature

- implement a failover solution

If you do not install the Application Server on a computer with access to the domain, then you can only add local users and local groups to the SiteProtector system.

**Note:** When the SiteProtector system fails over to the secondary Site, only domain users and domain groups stored in the Site Database fail over to the secondary Site Database. If you do not have any domain users or domain groups set up in the SiteProtector system, then you will not be able to log on to or use the secondary Site.

## Searching for Users and Groups

### Introduction

The SiteProtector system provides the Check Names feature to help you search for the following:

- local users and groups
- domain users and groups.

This feature is available when you are performing the following tasks:

- adding members to the SiteProtector system user groups
- assigning global permissions to members
- assigning group-level permissions to members

### Search options

Table 53 describes the search options available with the Check Names feature.

If you want to...	Then...
display all the users and groups in a specific domain	type <i>domain name</i> \, and then click <b>Check Names</b> . <b>Example:</b> us\ This search displays all the domain users and groups that exist in the <i>us</i> domain.
display all the users and groups that begin with a specific letter	type <i>the letter</i> , and then click <b>Check Names</b> . <b>Example:</b> a This search displays all domain users and groups that begin with the letter <i>a</i> in all domains.

**Table 53:** *Searching for members with Check Names*

---

# Permissions Affected by Upgrades

- Introduction** This topic describes how the SiteProtector system users and permissions are affected by upgrading to the SiteProtector system 2.0, Service Pack 6.0, or later.
- Background** In previous releases, the SiteProtector system included an editable file called `security.xml`. This file included the following default SiteProtector system user roles and the default permissions for each role:
- Administrator
  - Analyst
  - Operator
- You could manually edit this file to customize user permissions in the SiteProtector system, such as add user roles and change the default permissions assigned to user roles.
- What is not retained in the `security.xml` file** The SiteProtector system 2.0, Service Pack 6.0, or later does not support or implement changes or edits you make to the `security.xml` file. Excluded changes include the following:
- custom user roles that you created in addition to the three default user roles
  - any users that you added to custom user roles
  - changes you made to the default user roles, such as renaming, adding permissions, and deleting permissions
- What is retained in the `security.xml` file** The SiteProtector system *does* retain the following:
- The `security.xml` file with your changes, but the file is not used in the SiteProtector system. You can still access it and print for permission set up purposes in the new system.
  - The three default user roles (administrator, operator, and analyst) with their original permissions
- Note:** *Original* means the permissions assigned to the user roles before you edited them.
- For example, if you added or removed permissions to the user role called Operator, then none of these changes are kept in the upgrade process. If you created a custom user role called *Atlanta Server Administrators*, then this role is lost in the upgrade.
  - Any users you added to the three default user roles, their user role assignment, and the original permissions assigned to the user role

For example, if you added a user call *jsmith* to the *Operator* user role, then the upgrade process automatically sets up *jsmith* as a member of the SiteProtector system user group called Operator. The user *jsmith* will have the original permissions assigned to the Operator user role, not any changes you made to the role.

**Recreating custom user roles** If you created custom user roles in the `security.xml` file, then you must recreate the user roles in the SiteProtector system as custom SiteProtector system user groups. The SiteProtector system retains the edited version of the `security.xml` file in the same location. You can print this file and recreate the custom permissions in the SiteProtector system.

For information about creating custom SiteProtector system user groups, see “Creating SiteProtector System User Groups” on page 163.

---

# Working with Policy Permissions

<b>Introduction</b>	This topic provides information about the permissions needed to create, edit, and deploy policies in the SiteProtector system.
<b>Deploy Policy permission</b>	Permissions to deploy policies are set at the group level. So, if a user has the Deploy Policy permission for a group, he or she can deploy policies to, or remove deployments from, that group. Group permissions are hierarchical, so if you grant Deploy Policy permissions to a group, that user or user group will have the same permissions in any subgroups unless you set different permissions specifically for the subgroup.
<b>Assigning Deploy Policy permissions</b>	<p>To grant Deploy Policy permissions for a user or group of users:</p> <ol style="list-style-type: none"><li>1. Select a group, and then click <b>Object</b> → <b>Properties</b>.</li><li>2. Click the <b>Permissions</b> icon.</li><li>3. In the Users and/or Groups area, select the user or user group you want to assign Deploy Policy permissions.</li><li>4. For the Deploy Policy permission, click the circle in the <b>Control</b> column. A black circle indicates that the user or user group can deploy policies to this group. A white circle indicates that the user cannot deploy policy to this group.</li><li>5. Click the <b>Save All</b> icon.</li></ol>
<b>Modify policy permissions</b>	Permissions to edit, create, and delete policies are set by agent type. They are also at the group level, but since all policies live in the repository, they must be set for the group that contains the repository they reside in. For example, you can assign permissions to one user group to modify Proventia Network IPS policies, but not to modify Proventia Desktop policies in the same repository. If you use multiple repositories, you could also grant a user or user group permissions to modify Proventia Network IDS policies in one group's repository, but not in another.
<b>Control policy permissions</b>	<p>The Control permission allows users or user groups to assign policy subscription groups to an agent type. They are also set for the group containing the repository they reside in. For example, you can assign permissions to one user group to change policy subscription groups for Proventia Network IPS agents, but not for Proventia Desktop agents.</p> <p><b>Note:</b> Proventia Network Enterprise Scanner has several policy types that also allow a View permission. For more information, please see the Enterprise Scanner documentation.</p>
<b>Shared policy types</b>	<p>Some policies are shared by different agent types. A user with permissions to a shared policy type for one agent can edit that policy for all agent types.</p> <p><b>Example:</b> The Group Settings policy is a shared policy. If you try to access Group Setting Policy from a repository in which you have Modify permissions for at least one of the following agents, you are allowed access:</p> <ul style="list-style-type: none"><li>● RealSecure Desktop</li><li>● Proventia Network MFS</li><li>● X-Press Update Server</li></ul>

- Proventia Network IPS
- Event Archiver
- Proventia Server IPS

**Note:** You are not allowed access if you do not have Modify permissions for at least one of these agents.

**Assigning Modify or Control policy permissions**

To grant users or user groups permissions to modify policies for an agent type:

1. Select a group, and then click **Object**→**Properties**.
2. Click the **Permissions** icon.
3. In the Users and/or Groups area, select the user or user group you want to assign the permissions.
4. Expand the Agent type for which you want to grant permissions.
5. In the Policy permission, click the circle in the **Modify** or **Control** column.
6. Click the **Save All** icon.



## SECTION B: SiteProtector System User Groups

### Overview

**Introduction** This section provides information about setting up and managing SiteProtector system user groups.

**In this section** This section includes the following topics:

<b>Topic</b>	<b>Page</b>
What is a SiteProtector System User Group?	162
Creating SiteProtector System User Groups	163
Adding Members to SiteProtector System User Groups	164

## What is a SiteProtector System User Group?

### Introduction

A SiteProtector system user group is a group of users in the SiteProtector system who all have the same set of global and group-level permissions. The SiteProtector system user groups are useful because they allow you to control the permissions for an entire group of users simultaneously according to the user's role within your organization.

When you add an individual user or group of users to a SiteProtector system user group, the user or users automatically receive all the permissions assigned to that user group. This method provides a quick way to grant an entire set of permissions to a user or group of users. IBM ISS recommends that you manage most user permissions with SiteProtector system user groups.

**Important:** It is very important to understand the differences and similarities between SiteProtector system user groups and local groups or domain groups. SiteProtector system user groups are managed entirely independently from local groups and domain groups.

### Predefined user groups

The SiteProtector system provides the following predefined user groups, each with a specific set of permissions designed for different roles within a security organization:

- Administrator
- Analyst
- Operator
- Network Manager
- Desktop Manager
- Server Manager
- Assessment Manager

### Custom user groups

If the predefined SiteProtector system user groups do not provide the permission sets that you need, then you can create custom SiteProtector system user groups to meet your requirements. Table 54 describes the tasks for setting up a custom SiteProtector system user group.

Task	Description
1	Create the SiteProtector system user group. See "Creating SiteProtector System User Groups" on page 163.
2	Add members to the SiteProtector system user group. See "Adding Members to SiteProtector System User Groups" on page 164.
3	Assign global permissions to the SiteProtector system user group. See "Assigning and Removing Global Permissions" on page 170.
4	Assign group-level permissions to the SiteProtector system user group. <b>Important:</b> Make sure you give the SiteProtector system user group the permission called <i>Group-View</i> at the <i>Site Group</i> level. If you do not, then none of the users in this group can login to a Site. See "Setting up Group-Level Permissions" on page 235.

**Table 54:** Tasks for setting up a custom SiteProtector system user group

---

# Creating SiteProtector System User Groups

**Introduction** This topic explains how to create a SiteProtector system user group.

**Procedure** To create a SiteProtector system user group:

1. In the left pane, select the *Site Node*.
2. Select **Tools** → **Manage User Groups**.  
The Manage User Groups window appears.
3. In the left pane, click **Add**, and then type the name for the new user group.
4. Click **OK**.

The left pane displays the SiteProtector system user group. The right pane is empty until you add members to the SiteProtector system user group. See “Adding Members to SiteProtector System User Groups” on page 164.

## Adding Members to SiteProtector System User Groups

### Introduction

This topic provides information about adding members to SiteProtector system user groups. You can add the following to a SiteProtector system user group:

- local users
- local groups
- domain users
- domain groups

### Definition: member

The term *member* refers to individual users as well as groups of users. For example, the domain group called *Server Administrators* and all the members in that domain group are collectively referred to as a one member in the SiteProtector system.

### Windows permission management

Permission management in Windows has a large impact on permission management in the SiteProtector system. For example, when you add a member to a Windows group and that Windows group is also a member of a SiteProtector system user group, you automatically add the member to the SiteProtector system user group.

### Example

In the SiteProtector system, you add a domain group called *Server Administrators* to the SiteProtector system user group called *Administrators*. This action gives all members of the domain group called *Server Administrators* all of the permissions assigned to the *Administrators* SiteProtector system user group.

In Windows Computer Management, you add a member called *jsmith* to the domain group called *Server Administrators*. This action automatically gives *jsmith* all of the permissions assigned to the *Administrators* SiteProtector system user group.

### Before you begin

Before you add members to a SiteProtector system user group, you must complete the following tasks:

- Verify that the member exists in Windows.  
**Note:** You can only add members to the SiteProtector system that already exist in Windows.
- For local users and local groups, obtain the exact account information from Windows about the local user or local group, including the computer name and user name. You cannot look up local users or local groups in the SiteProtector system. You can look up domain users and domain groups.

### Procedure

To add members to SiteProtector system user groups:

1. In the left pane, select the *Site Node*.
2. Select **Tools** → **Manage User Groups**.  
The Manage User Groups window appears.
3. In the left pane, select the SiteProtector system user group that you want to add members to.
4. In the **Members** section, click **Add**.

5. Use the following table to determine your next step:

If you want to add...	Then...
local users or groups to the SiteProtector system user group	type the complete account using the following syntax, and then click <b>OK</b> : <ul style="list-style-type: none"> <li>• <i>machine name\user name</i></li> <li>• <i>machine name\group name</i></li> </ul> If you do not know the complete account information, then you must look it up using Windows Computer Management.
domain users or groups to the SiteProtector system user group	type the complete account name using the following syntax, and then click <b>OK</b> : <ul style="list-style-type: none"> <li>• <i>domain name\user name</i></li> <li>• <i>domain name\group name</i></li> </ul> If you do not know the complete account name, then you must look it up using Check Names.

The Select User and Groups window appears.

6. Select the member in the list you want to add to the user group, and then click **OK**.

The Members section list the member you added to the SiteProtector system user group.

### Removing members from SiteProtector system user groups

To remove a member from a SiteProtector system user group:

1. In the left pane, select the *Site Node*.
2. Select **Tools** → **Manage User Groups**.

The Manage User Groups window appears.

3. In the **User Group** list, select the user group that contains the member you want to remove.

The Members section displays the current members of the SiteProtector system user group.

4. In the **Members** section, select the individual member you want to remove, and then click **Remove**.

**Tip:** To select multiple members at the same time, press and hold the CTRL key while you select the members.

The SiteProtector system displays a confirmation message.

5. Click **Yes**.

The selected members are removed from the SiteProtector system user group.



## SECTION C: **Global Permissions**

### Overview

**Introduction** This section defines global permissions and provides instructions for granting and removing global permissions.

**In this section** This section contains the following topics:

<b>Topic</b>	<b>Page</b>
What are Global Permissions?	168
Assigning and Removing Global Permissions	170

## What are Global Permissions?

### Introduction

Global permissions are Site-wide permissions that you can provide to any of the following:

- SiteProtector system user groups
- local users
- local groups
- domain users
- domain groups

A global permission allows the user to perform the related actions anywhere in the Site.

### List of permissions

The SiteProtector system provides a fixed set of global permissions that you can grant and remove for users. You cannot create additional global permissions in the system. Table 55 describes the global permissions included with the SiteProtector system.

Permission	Description
Active Directory	This permission allows users to do the following: <ul style="list-style-type: none"> <li>• import assets and groups from Active Directory</li> <li>• retrieve login information for agents</li> </ul>
Auditing Setup	This permission allows user to enable/disable auditing for most actions in the console
Central Responses	This permission allows user to create/edit central response rules and create/edit network objects and response objects policies
Clear/Restore Events	This permission allows users to clear and restore security events on the Analysis view.
Database Maintenance Setup	On the Agent view at the Site level, set Database maintenance options, including the following: <ul style="list-style-type: none"> <li>• schedule regular maintenance</li> <li>• set database purge options</li> <li>• set database backup options</li> </ul>
Export Analysis Data	This permission allows users to do the following on the Analysis view: <ul style="list-style-type: none"> <li>• print data</li> <li>• export data</li> <li>• schedule data export job</li> </ul>
Full Access to All Functionality	This permission allows users to perform all SiteProtector system functions.
Import Policy/Response	This permission allows the user to import policies and/or responses. <p><b>Note:</b> The SiteProtector system allows you to grant the Import Policy/Response global permission to non-administrative users, however, IBM ISS strongly advises against this. In some cases restricted permissions are circumvented when you grant non-administrative users the Import Policy/Response global permission.</p>
Launch Event Viewer	On the Agent view at the Site level, open the Event Viewer.

**Table 55:** *Global permissions*



Permission	Description
Manage Global Permissions	This permission allows users to assign and remove global permissions to users and groups.
Manage Global Responses	This permission allows users to manage global responses.
Manage Health	This permission allows users to manage system health settings.
Manage Incidents and Exceptions	This permission allows users to create and edit incidents and exceptions on the Analysis view.
Manage Licenses	At the Site level, do the following: <ul style="list-style-type: none"> <li>• Add and remove products licenses</li> <li>• View license information, including warnings and summary information</li> <li>• View available OneTrust tokens and license information for Proventia OneTrust Licensing</li> </ul>
Manage SecureSync	At the Site level, use the SecureSync features, including the following: <ul style="list-style-type: none"> <li>• Use the Site Management Transfer Wizard</li> <li>• Distribute keys</li> <li>• Manage agents</li> <li>• Release agents</li> </ul>
Manage Session Properties	This permission allow users to set up a session properties file in order to scan using Network Internet Scanner.
Manage Ungrouped Assets	This permission allows you to do the following: <ul style="list-style-type: none"> <li>• see ungrouped assets, agents, and analysis events in the site ranges.</li> <li>• add or delete site ranges</li> <li>• perform the Auto Group Hosts function on ungrouped items.</li> </ul>
Manage User Groups	This permission allows users to do the following: <ul style="list-style-type: none"> <li>• create SiteProtector system user groups</li> <li>• delete SiteProtector system user groups</li> <li>• add members to SiteProtector system user groups</li> <li>• remove members from SiteProtector system user groups</li> </ul>
Ticketing Setup	At the Site level, set and change ticketing options, including the following: <ul style="list-style-type: none"> <li>• Email notification settings, including when to send emails and the email addresses of recipients</li> <li>• Ticket status categories</li> <li>• Ticket priority categories</li> <li>• Custom categories for tickets</li> </ul>

Table 55: Global permissions (Continued)

## Assigning and Removing Global Permissions

### Introduction

This topic provides information about assigning and removing global permissions for the following:

- SiteProtector system user groups
- local users
- local groups
- domain users
- domain groups

**Note:** For products that use the Site-level Policy Editor, the SiteProtector system does not allow you to assign multiple permissions at once. Assigning permissions individually can decrease the likelihood that you will inadvertently assign a critical permission to the incorrect user.

### Before you begin

Before you assign or remove global permissions, you must complete the following tasks:

- Verify that you have permission to manage global permissions; if you are a member of the SiteProtector system user group called Administrators, then you have this permission by default. If not, then you must obtain the global permission called Manage Global Permissions from your administrator.
- If you are assigning global permissions to a Windows member, then verify that the member exists in Windows.
- If you are assigning global permissions to a SiteProtector system user group, verify that the SiteProtector system user group exists in the SiteProtector system.
- If you are assigning global permissions to Windows local users or Windows local groups, obtain the exact account information from Windows about the local user or local group, including the machine name and user name. You cannot look up local users or local groups in the SiteProtector system. You can look up domain users and domain groups.

### Assigning Global Permissions

To assign global permissions:

1. In the left pane, right-click the *Site Node*, and then select **Properties** from the pop-up menu.  
The Site Properties tab appears.
2. Click the **Permissions** icon.
3. In the **Manage Global Permissions** section, right-click the global permission you want to assign, and then select **Open Permission**.  
The Manage Users and/or Groups window appears.
4. Click **Add**.  
The Search Users/Groups to Add window appears.

5. Use the following table to determine your next steps:

If you want to add...	Then...
local users or groups to the SiteProtector system user group	type the complete account using the following syntax, and then click <b>OK</b> : <ul style="list-style-type: none"> <li>• <i>machine name\user name</i></li> <li>• <i>machine name\group name</i></li> </ul> If you do not know the complete account information, then you must look it up using Windows Computer Management.
domain users or groups to the SiteProtector system user group	type the complete account name using the following syntax, and then click <b>OK</b> : <ul style="list-style-type: none"> <li>• <i>domain name\user name</i></li> <li>• <i>domain name\group name</i></li> </ul> If you do not know the complete account name, then you must look it up using Check Names.

6. Click **OK**.

The member name appears next to the global permission. If you assigned the global permission to a SiteProtector system user group, local group, or domain group, then any member you add to those groups automatically receives this global permission. If more than one member has this permission, then the member names are separated by semicolons (;).

## Removing global permissions

To remove a global permissions from a user or group:

1. In the left pane, right-click the *Site Node*, and then select **Properties** from the pop-up menu.

The Site Properties tab appears.

2. Click the **Permissions** icon.

3. In the **Manage Global Permissions** section, right-click the global permission you want to remove from a user or group, and then select **Open Permission**.

The Manage Users and/or Groups window appears.

4. Select the member you want to remove the permission from, and then click **Remove**.

**Tip:** To select multiple members at the same time, press and hold the CTRL key while you select the members in the list.

The SiteProtector system displays a confirmation message.

5. Click **Yes**.

The Manager Users and/or Groups window appears. The member is no longer listed under the permission.

6. Click **OK**.

The member name no longer appears next to the global permission.



## Chapter 13

# Configuring the Event Archiver

## Overview

### Introduction

The Event Archiver archives event data on a separate computer so that the Site database is not required to store this data. Use the background information and procedures in this chapter to control the way in which the Event Archiver archives events and to configure multiple Event Archivers.

### Event archival component

The Event Archiver is a stand-alone component that archives events in a predefined directory that you can access and view easily. The Event Archiver begins collecting events after you install it with no additional setup from you.

**Note:** The Event Archiver is not included in all SiteProtector system pricing plans. For more information, refer to the pricing plan that applies to your configuration.

### Related documentation

See the *SiteProtector System Installation Guide* for information about installing the Event Archiver.

### In this chapter

This chapter contains the following topics:

Topic	Page
Important Requirements and Considerations	174
Event Rules	175
Creating Event Rules that Filter by IP Address	176
Creating Event Rules That Filter by Event Type	179
Setting the Order of Event Rules	180
Viewing Archived Events	181
Modifying the Event Archiver Directory Structure	182

## Important Requirements and Considerations

<b>Introduction</b>	This topic gives you requirements and considerations for configuring the Event Archiver. Review these items before you configure the Event Archiver.
<b>Requirements</b>	You must install the Event Archiver and configure it to communicate with the SiteProtector system. See the <i>SiteProtector System Installation Guide</i> for more information.
<b>Determining which events to archive</b>	By default, the Event Archiver stores all the events that are collected by the Event Collector. You can use Event Filter Rules to filter the events you are archiving according to several criteria.
<b>Multiple Event Archivers</b>	You can use Event Rules to help divide the work of archiving events among multiple Event Archivers. For example, you could create a rule that forwards IDS events to an Event Archiver and another rule that forwards vulnerability events to a different Event Archiver.
<b>Performance considerations</b>	The Event Archiver may impact network performance because it increases traffic between components. The Event Archiver may impact the performance of the Event Collector, especially if the Event Archiver policies are configured to archive duplicate events. Consider configuring Event Archiver policies so that they do not archive duplicate events. See “Event Rules” on page 175.
<b>Updating Event Archivers</b>	The Event Archiver uses the X-Press Update Server that is installed by default on the Application Server to retrieve updates from xpu.iss.net (Download Center). You can change these updated settings, including the X-Press Server that Event Archiver is configured to communicate with. See “Configuring X-Press Update Servers” on page 71.

## Event Rules

### Introduction

Event Rules can help you control the types of events you archive and help you divide the work of archiving events among multiple Event Archivers. Use the information in this topic to familiarize yourself with Event Rules.

### What are Event rules?

Similar to the filters in the Central Responses policy, Event Rules let you filter archived events according to event type, port, source, and destination addresses, and user-defined parameters. You can configure a single rule to filter using up to four criteria. For example, you could configure an Event Rule to archive events, according to the criteria specified in Table 56.

Criteria	Values
Event Type	http
Source IP	290.222.111
Destination IP	191.111.222
Source Port	8080
Destination Port	8081

**Table 56:** *Example of an Event Rule that uses multiple criteria*

### Rule order

Event Rules appear in a list in the Add Event Rules window. By default, the SiteProtector system orders this list according to when the rule was created, from earliest to latest. You can change this order by moving rules up or down in the list.

### How do Event Rules filter events?

The SiteProtector system tries to match each event that is collected with the Event Rules in the list, starting with the first rule in this list, and so on. If it detects a match, the SiteProtector system forwards and saves the event to the Event Archiver.

## Creating Event Rules that Filter by IP Address

### Introduction

Use the procedures in this topic to create Event Rules that filter by the following:

- source IP address
- destination IP address

### Filtering events by source IP address

To filter archived events by source address:

1. In the **Agent** view, right-click the Event Archiver component, and then select **Manage Policy** from the pop-up menu.

The **Policy** tab appears in the right pane.

2. Open the **Event Filter Rules** policy for the Event Archiver to receive the events.

**Note:** If the policy does not already exist, you must create it.

The **Event Rules** tab appears in the right pane.

3. Click **Add**.

The Add Event window appears.

4. Select the **Enable** box.

5. Type the rule name in the **Name** box, and then type an optional description in the **Comment** box.

**Note:** If you want to use a Network Object to define an address or range of addresses, click the Network Objects icon.

6. Select the **Source** tab.

7. Do you want to include events from all source addresses?

- If *yes*, then select **Any**, and then go to Step 10. (This is the default option.)
- If *no*, select **Use specific source addresses**, and then go to Step 8.

8. Select one of the following options from the **Mode** list:

- **From to**, to include events only from the source IP addresses that you specify.
- **Not From** to exclude events from the source IP addresses that you specify.



9. Select one of the following options:

If you want to specify...	Then select...
a single source IP address	<b>Single IP Address</b> , click <b>Add</b> , and then type the IP address in the box provided.
a range of source IP addresses as a network mask	<b>Network Address/#Network Bits (CIDR)</b> , and then type an IP address followed by the number of bits in the boxes provided.
a range of source IP addresses	<b>IP Address Range</b> , and then type the range in the boxes provided.
an IP address from your address list	<b>Address List Entry</b> , then select the address from the <b>Address List Entry Name</b> list.

10. If you want to include events that are originate from certain ports, then specify one of the following:

If you want to specify...	Then do this...
a single port	select <b>Single Port</b> , and then type the <b>Port Number</b> .
a range of ports	select <b>Port Range</b> , and then type the range in the boxes provided.
a port or port range from your address list	select <b>Port List Entry</b> , then select the address from the <b>Port List Entry Name</b> list.

11. Click **OK**.

### Filtering events by destination IP addresses

To filter archived events by destination IP address:

- In the **Agent** view, right-click the Event Archiver, and then select **Manage Policy** from the pop-up menu.  
The **Policy** tab appears in the right pane.
- Open the **Event Filter Rules** policy for the Event Archiver to receive the events.  
**Note:** If the policy does not already exist, you must create it.  
The **Event Rules** tab appears in the right pane.
- Click **Add**.  
The Add Event window appears.
- Select the **Enable** box.
- Type the rule name in the **Name** box, and then type an optional description in the **Comment** box.  
**Note:** If you want to use a Network Object to define an address or range of addresses, click the Network Objects icon.
- Select the **Destination** tab.
- Do you want to include events from all destination addresses?
  - If *yes*, then select **Any**, and then go to Step 10. (This is the default option.)
  - If *no*, select **Use specific destination addresses**, and then go to Step 8.
- Select one of the following options from the **Mode** list:

- **From to**, to include events that are destined to the destination IP addresses that you specify.
  - **Not From** to exclude events from the destination IP addresses that you specify.
9. Select one of the following options in the Specific section:

<b>If you want to specify...</b>	<b>Then do this...</b>
a single destination IP address	select <b>Single IP Address</b> , click <b>Add</b> , and then type the IP address in the box provided.
a network mask that specifies a range of destination IP addresses	select <b>Network Address/#Network Bits (CIDR)</b> , and then type an IP address followed by the number of bits in the boxes provided.
a range of destination IP addresses	select <b>IP Address Range</b> , and then type the range in the boxes provided.
an destination IP address from your address list	select <b>Address List Entry</b> , then select the address from the <b>Address List Entry Name</b> list.

10. If you want to include events that destined for certain ports, then specify one of the following:

<b>If you want to specify...</b>	<b>Then do this...</b>
a single port	select <b>Single Port</b> , and then type the <b>Port Number</b> .
a range of ports	select <b>Port Range</b> , and then type the range in the boxes provided.
a port or port range from your address list	select <b>Port List Entry</b> , then select the address from the <b>Port List Entry Name</b> list.

11. Click **OK**.

---

# Creating Event Rules That Filter by Event Type

**Introduction** Event filters are options in the Event Rules window that let you let you filter archived events according to the SecurityFusion module statuses or appliance statuses. Event Filters provide more precise filtering than rules that filter by IP address.

**Procedure** To add event filters:

1. In the **Agent** view, right-click the Event Archival component, and then select **Policy** from the pop-up menu.  
The **Policy** tab appears in the right pane organized.
2. Open the **Event Filter Rules** policy for the Event Archiver to receive the events.  
**Note:** If the policy does not already exist, you must create it.  
The **Event Rules** tab appears in the right pane.
3. Click the **Add** icon.  
The Add Event Rules window appears.
4. Select the **Enabled** box.
5. Type the rule name in the **Name** box, and then type an optional description in the **Comment** box.
6. Select the **Events** tab, and then click **Add**.  
The Add Event Filters window appears.
7. Select the **Enabled** box.
8. Type the name of the event in the **Event** box.  
**Tip:** To filter for a group of events that belong to the same category, type the prefix or partial name plus the wildcard symbol (\*), such as http\* or ftp\*.
9. If you want to filter events by **Priority** (High, Medium, and Low), select an option from the list.
10. If you want to filter events by a SecurityFusion module or appliance statuses, select the check boxes that apply from the **Status** list.  
**Note:** All check boxes are selected by default.
11. Click **OK**.

## Setting the Order of Event Rules

- Introduction** You can change the order of Event Rules on your Site. This topic includes background information and a procedure for setting the order of Event Rules.
- Guideline for setting the order of Event Rules** To improve the performance of Event Rules, consider changing the order so that rules that filter on broader criteria appear first in the list. For example, you would position an Event Rule that filters an entire domain of IP addresses higher than a rule that filters a single address.
- Event rule order** When you create a new rule, it appears in the list above the rule you had selected. If you had no rule selected, the new rule appears at the bottom of the list. You can change the order of any rule in the list.
- Procedure** To set the order of Event Rules:
1. In the **Agent** view, right-click the Event Archival component, and then select **Policy** from the pop-up menu.  
The **Policy** tab appears in the right pane.
  2. Open the **Event Filter Rules** policy for the Event Archiver to receive the events.  
**Note:** If the policy does not already exist, you must create it.  
The **Event Rules** tab appears in the right pane.
  3. Select an Event Rule in the list, and then use the up or down arrow to reorder the rule.  
The **Order** box in the Add Event Rules window is updated to reflect the rule's position in the list.

## Viewing Archived Events

**Introduction** Use the background information and procedures in this topic to view archived events and verify that the Event Archiver is collecting events correctly.

**How are archived events organized?** The SiteProtector system stores archived events in text files on the Event Archiver computer. By default, a new file is created every 60 minutes. The file name contains the time and date the events were archived. Table 57 describes the directory structure for these files.

Column	Description
First	IP address of the Sensor that sent the event year the event was archived
Second	year the event was archived
Third	month the event was archived
Fourth	the day the event was archived

**Table 57:** Archived events file naming convention

**Scripts used to access archived events** If you are accessing archived events often, consider using a third-party scripting tool, such as Perl, to create a script that can browse and search these files. A script can help you locate files quickly and manage archived events more efficiently.

**Prerequisite** You must be able to access the Event Archiver computer before you can view archived events.

**Procedure** To view archived events:

1. On the computer where the Event Archiver is installed, locate the following:  
C:\Program Files\ISS\SiteProtector\EventArchiver\
2. Open the EventLogDir folder, and then locate the IP address of the sensor that sent the events that you want to view.
3. Browse the individual event files, and then locate the file that corresponds with the date and time of the event you are searching for.

**Example:**

```
C:\Program
Files\ISS\SiteProtector\EventArchiver\192.111.111\2005\08\EventLog_2
005_8_3_16.49.28
```

## Modifying the Event Archiver Directory Structure

### Introduction

You can customize the location of your Event Archiver log files by modifying the Event Archiver directory structure. Information related to performing this task is included in this topic.

### Modifying the directory structure

To modify the Event Archiver directory structure:

1. Stop the Event Archiver service.

For information about how to stop the Event Archiver service, see the Starting or stopping the SiteProtector Event Archiver service section in this topic.

2. Open the EventArchiver.policy file using Notepad.

The EventArchiver.policy file's default location is the following:

```
C:/Program Files/ISS/SiteProtector/Event Archiver/
```

3. To see all the parameters that are available for you to use, go to "Listing your available parameters," later in this topic.
4. To see how to add or remove parameters to the EventArchiver.policy file, go to "Adding a parameter" or "Removing a parameter", later in this topic.
5. In the policy file, add or remove the parameters to create the desired directory structure.
6. Save your changes, and then close the policy file.
7. Start the Event Archiver service.

For information about how to start the Event Archiver service, see "Starting or stopping the SiteProtector Event Archiver service" next in this topic.

### Starting or stopping the SiteProtector Event Archiver service

To start or stop the SiteProtector Event Archiver service:

1. Open Administrative Tools in the Control Panel, and then double-click Services. The Services utility appears.
2. In the Name column of the right pane, right-click **SiteProtector Event Archiver**, and then do one of the following:
  - Click **Start** on the pop-up menu.
  - Click **Stop** on the pop-up menu.

### Listing your available parameters

The parameters that are available to you depends on the agent(s) you are using with the SiteProtector system. Some parameter names, such as SensorAddress and AlertDateTime, are common to all agents, but many parameter names not common to all agents. You can see the parameters available to you by viewing the EventLog file.

The following tips can assist you in determining your available parameters:

- In the log file, the parameter names are located between the R| and = symbols. For example, the AlertFormatVersion parameter appears as R|AlertFormatVersion=85 in the log file. (In this case, the value for AlertFormatVersion is 85.)
- It is easier for you to see the available parameters in Notepad when the word wrap feature is turned off.

**Adding a parameter** To add a parameter in the EventArchiver.policy file:

1. Locate the following section near the bottom of the file:

```
[\\Event Archiver\\DirectoryStructure];
```

**Note:** The parameter structures appear after the line shown above. Each parameter structure consists of three lines. By default, the Event Archiver lists two parameters, SensorAddress and AlertDateTime.

2. Cut and paste any three-line parameter structure to the desired location in the list, and then update the parameter number.

**Tip: How do I determine the “desired location”?** A parameter number appears at the end of the first line of each three-line structure. This number represents the directory level for the parameter. For example, if the number is `\3`, then the parameter is located within two other directories, making it third in the directory structure. If you want this parameter to appear sixth in the directory structure, replace the `\3` with `\6`.

**Note:** You must number your parameter numbers sequentially, i.e., you should not skip any numbers. For example, don't use `/3` as a parameter number if you don't use `/1` and `/2` as the parameter numbers in the two previous parameter structures.

**Note:** The Event Archiver creates the directory structure based on the parameter number, not on the order that the parameter is listed in the policy file. It is better, however, to list the parameters in the order of their parameter numbers to avoid confusion.

3. In the second line of the structure you just pasted, change the old parameter to the desired parameter name.

**Note:** For more information about how to find the parameters that are available to you, see “Listing your available parameters” earlier in this topic.

### Example: Adding a parameter

To add the AlertFormatVersion parameter to the third position in your directory structure, you would do the following:

First, cut and paste the following parameter structure so that it is listed third in the EventArchiver.policy file:

```
[\\Event Archiver\\DirectoryStructure\\2];
```

```
Field =S AlertDateTime;
```

```
ParameterLoc =S Required;
```

then, change the first line from `[\\Event Archiver\\DirectoryStructure\\2];` to `[\\Event Archiver\\DirectoryStructure\\3];` to list the new parameter third in the directory.

to use the AlertFormatVersion parameter instead of the AlertDateTime parameter, next change the second line from `Field =S AlertDateTime;` to `Field =S AlertFormatVersion.`

### Removing a parameter

To remove a parameter in the EventArchiver.policy file:

1. Locate the following line near the bottom of the file:

```
[\\Event Archiver\\DirectoryStructure];
```

**Note:** The parameter structures appear after the line shown above. Each parameter structure consists of three lines. By default, the Event Archiver lists two parameters, SensorAddress and AlertDateTime.

2. Locate the parameter you want to delete, and then delete its entire three-line structure.

**Note:** Be sure to renumber the parameter numbers in the remaining structures, if needed. The parameter numbers appear at the end of the first line of each three-line parameter structure.



## Chapter 14

# Configuring Ticketing

## Overview

**Introduction** This chapter provides information about configuring the ticketing function in the SiteProtector system and working with tickets.

**What is ticketing?** You can use the SiteProtector system's ticketing function to assign problem tickets/issues, events, agents, and assets to a SiteProtector system user. When you have an issue with an event, agent, or asset, the system creates a ticket and then forwards it to the person who is assigned to the ticket. The user then investigates and resolves the issue. During this time, the user can change the status of a ticket, such as from "New" to "Open" to "In Progress" to "Closed."

**Writing a plug-in** The SiteProtector system contains a built-in ticketing system and includes a third-party ticketing API. With the API, a third-party plug-in writer can create a plug-in that allows tickets created in the SiteProtector system to be managed by a third-party ticketing system. The ticketing API was used to implement a plug-in for the BMC® Remedy® Action Request System®.

**Reference:** *Programmer's Guidelines for Writing a Third-Party Ticketing Plug-In* at <http://www.iss.net/support/documentation/>.

**In this chapter** This chapter contains the following topics:

Topic	Page
Working with the Remedy Action Request System (Remedy)	187
Working with Tickets	190
Working with Vulnerability Auto Tickets	192
Working with Ticketing Logs	196
Defining Notification Settings	197
Defining Ticket Priorities	198
Defining Ticket Status	200
Defining Custom Categories	202
Managing Ticketing Plug-ins	203

<b>Topic</b>	<b>Page</b>
Defining Response Settings	205
Defining Auto Ticketing Settings	207

## Working with the Remedy Action Request System (Remedy)

- Introduction** This topic discusses Remedy, the IBM ISS-supported third-party ticketing system. The SiteProtector system works with Remedy to streamline your event tracking and remediation processes. This topic explains how to access information to set up this product to use with the SiteProtector system.
- What is Remedy?** Remedy is a web-accessible workflow automation organizer that tracks tasks and records items, or tickets, of importance. For more information about Remedy, see <http://www.remedy.com>.
- Support for Remedy** For more information about using the plug-in, download the Integration Notes document for IBM Internet Security Systems from the partners pages on the BMC Software, Inc., Web site.
- Configuring the SiteProtector system to use Remedy** You can configure the SiteProtector system to use Remedy to track tickets. This integration allows users to create Remedy tickets from the SiteProtector system Console. For information on how to set up the build-in plug-in for Remedy, see <http://www.bmc.com/remedy/ppp/request.cfm>.
- The SiteProtector system and Remedy are integrated at the server level using a Remedy/Java application programming interface (API). When you save a ticket in the SiteProtector system, the information is also saved in the Remedy server. You can then use Remedy to edit, maintain, and track the tickets. If you use Remedy to maintain tickets, then you cannot edit them in the SiteProtector system; however, a copy of each ticket created in the SiteProtector system is saved in the SiteProtector system Database.
- Requirements** The following IBM ISS software and Remedy products must be installed and operating correctly prior to the integration:
- Remedy Action Request System 6.3
  - SiteProtector system 2.0 Service Pack 6 or later
- Remedy integration process** Table 58 describes the stages of the Remedy integration process.

Stage	Description
1	Import SiteProtector system definitions to the Remedy server.
2	Create a Remedy user with a fixed license.
3	Set Remedy options (server name, user name and password).
4	Modify the RemedyPluginConfig.xml file.
5	Open the SiteProtector system Console and log into your Site.
6	Add the Remedy ticketing plug-in to the SiteProtector system.

**Table 58:** *Stages of the Remedy integration process*

### Importing SiteProtector system definitions to the Remedy server

To import the SiteProtector system definitions to the Remedy server:

1. Log on to the Remedy server through the Remedy Administrator.
2. From the **Tools** menu, select **Import Definitions** → **From Definition File**.
3. Select `SP_Remeddy_Plugin.def` (provided by IBM ISS and located on your SiteProtector system server in `Program Files\ISS\SiteProtector\Application Server\config`)
4. Click **Open**.

The Import Definition window appears.

5. Select **Forms and Active Links**, and then click **Add** to move the definitions into Objects to Import.
6. Click **Import**.

**Note:** These forms will be used to interact with the Remedy system. They will not overwrite the current forms you are using for Remedy.

### Integrating the SiteProtector system with Remedy

To integrate the SiteProtector system with Remedy:

1. Create a Remedy user with a fixed license.
2. Open the `RemedyPluginConfig.xml` file from `Program Files\ISS\SiteProtector\Application Server\config`.
3. Set the server entry to the server name or IP address.
4. Set the user entry to the user name to login to the Remedy server.
5. If you are using a non-encrypted password, do the following:
  - Set the encrypted-password to false.
  - Change the value of the password entry to the password for the user.
  - Go to Step 7.
6. If you are using an encrypted password, do the following:
  - Change the encrypt-password to true.
  - Change the password to `Remedy.Password`.
  - Go to the DOS prompt at `Program Files\ISS\SiteProtector\Application Server\bin`.

**Note:** For SiteProtector system software updated from a version earlier than 2.0 (Service Pack 6), the directory is `Program Files\ISS\RealSecure SiteProtector\Application Server\bin`

- Type `CCEngine -setremedy password`, and then type the password you are using for Remedy.
  - Press ENTER.
7. Save the `RemedyPluginConfig.xml` file.

### Adding the Remedy ticketing plug-in to the SiteProtector system

To add the Remedy ticketing plug-in to the SiteProtector system:

1. Open the SiteProtector system Console and log into your Site.
2. On the **Tools** menu, select **Ticketing Setup**.

The Ticketing Setup window appears.

3. Select the **Plug-in** tab.
4. Click **Add**.
5. Type the following information:
  - **Name**—Remedy
  - **Description**—Ticketing
  - **Class Name**—  
`net.iss.rssp.ticketing.plugin.impl.RemedyTicketingPlugin`
6. Click **OK**.
7. Select the Remedy Ticketing plug-in you just added.
8. Click **Activate**.

## Working with Tickets

### Introduction

This topic explains how to create, view, open, and edit tickets for the following:

- agents
- assets
- events

### Tickets

A *ticket* is a work request created in response to a situation that requires further investigation. Here are some examples of possible tickets:

- patching a range of assets against vulnerabilities
- investigating a new asset that recently appeared on the network, and dealing with it as appropriate
- locating an asset that is running an unapproved operating system, and updating it or removing it from the network

### Creating tickets

To create a ticket for an agent, asset, or event:

1. In the left pane, select the group that contains the agent, asset, or event.
2. In the **Go to** list, select **Agent**, **Asset**, or **Analysis**.
3. In the right pane, right-click the agent, asset, or event and then select **New Ticket**.  
The New Ticket tab appears.
4. Select the following options:
  - Priority
  - Responsibility
  - Category

**Note:** The SiteProtector system creates the Due Date automatically based on the priority that you select. You can change the Due Date if necessary.
5. In the **Synopsis** section, type a summary of the issue.
6. In the **Actions** section, type the steps required to resolve the issue.
7. Did you select a custom category for the Category option?
  - If *yes*, then click the **Custom Category** icon in the left pane, type text in the user-defined fields, and then go to Step 8.
  - If *no*, then go to Step 8.
8. Select **Action** → **Save All**.  
The SiteProtector system displays a message that the ticket is created, and provides the ticket ID number.
9. Click **OK** at the prompt to close the New Ticket tab.

### Viewing tickets

To view the tickets for an agent, asset, or event:

1. In the left pane, select the group that contains the agent, asset, or event.
2. In the **Go to** list, select **Agent** or **Asset**.

3. In the right pane, right-click the agent, and then select **List Tickets**.  
The Tickets for Selected Items tab appears and lists the tickets for the item.

### Opening tickets

To open a ticket for an agent, asset, or event:

1. In the left pane, select the group that contains the agent, asset, or event.
2. In the **Go to** list, select **Agent** or **Asset**.
3. In the right pane, right-click the agent or asset and then select **List Tickets**.  
The Tickets for Selected Items tab appears and lists the tickets for the item.
4. In the right pane, right-click the ticket, and then select **Open Ticket**.  
The Ticket ID tab appears and displays the ticket information.

### Editing tickets

To edit a ticket for an agent, asset, or event:

1. In the left pane, select the group that contains the agent, asset, or event.
2. In the **Go to** list, select **Agent** or **Asset**.
3. In the right pane, right-click the agent or asset, and then select **List Tickets**.  
The Tickets for Selected Items tab appears and lists the tickets for the item.
4. In the right pane, right-click the ticket, and then select **Open Ticket**.  
The Ticket ID tab appears and displays the ticket information.
5. Edit the following information as necessary:
  - Priority
  - Responsibility
  - Due Date
  - Category
6. In the **Synopsis** section, edit the summary of the issue.
7. In the **Actions** section, edit the steps required to resolve the issue.
8. Select **Action** → **Save All**.
9. Click **OK** at the prompt to close the New Ticket tab.

**Note:** You can only edit tickets that have been created in the SiteProtector system. Tickets that have been created in Remedy must also be edited in Remedy.

## Working with Vulnerability Auto Tickets

### Introduction

Use the SiteProtector system vulnerability auto ticketing feature to create auto ticketing rules that apply to vulnerable events in a group. When a vulnerable event matches an auto ticketing rule during a vulnerability assessment scan, the SiteProtector system automatically generates a new ticket.

**Note:** Only users with global ticketing permissions can create and modify auto ticketing rules.

### Auto ticketing rule criteria

For each group of assets, you can create vulnerability auto ticketing rules to specify the criteria by which the SiteProtector system auto-generates tickets. These criteria include:

- Severity of the vulnerability
- Asset criticality
- Asset function
- Asset operating system
- Common Vulnerability Scoring System (CVSS) value of the vulnerability

Vulnerability auto ticketing rules also allow you to configure the ticket priority and the person responsible for addressing the ticket.

### Auto ticketing rule eligibility


You must create auto ticketing rules for vulnerable events at the group level. When you create a rule, it will apply to all the assets in the group. You can group the assets so that the SiteProtector system generates only one auto ticket for a each asset, rather than creating individual tickets for each vulnerability.

**Note:** You cannot create auto ticketing rules for ungrouped assets.

Vulnerability auto ticketing rules apply to vulnerable events identified by either IBM Proventia Network Enterprise Scanner or IBM Internet Scanner.

### Auto ticketing process

Table 59 describes the stages of the auto ticketing process.

Stage	Description
1	<p>Create and enable auto ticketing rules for vulnerable events at the group level.</p> <p><b>Note:</b> When auto ticketing rules are enabled for a group, an auto ticketing icon  appears on the group folder in the left pane.</p>
2	<p>Specify the Default Responsible Party in the Auto Ticketing tab on the Ticketing Setup window.</p> <p><b>Note:</b> Once auto ticketing rules are created, you can click the <b>Link to Auto Ticketing tab</b> link in the Vulnerability Auto Ticketing Properties tab to open the Auto Ticketing tab on the Ticketing Setup window.</p>

**Table 59:** Stages of the SiteProtector system auto ticketing process



Stage	Description
3	<p>Use the up and down arrows to order the auto ticketing rules in the Vulnerability Auto Ticketing Properties tab.</p> <p><b>Important:</b> The sequence of vulnerability auto ticketing rules is important. During the ticket auto-generation process, the SiteProtector system applies rules in the order which they appear in the Vulnerability Auto Ticketing Properties tab. If a vulnerable event meets the criteria established in a rule, the SiteProtector system creates a ticket with the ticket priority and responsible user defined in the rule, and stops further rule processing for the event.</p>
4	<p>When a vulnerable event matches an auto ticketing rule, the SiteProtector system automatically generates a new ticket.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• If an asset is in multiple groups, the SiteProtector system creates a ticket based on the first auto ticketing rule that matches in the group that was created.</li> <li>• Once the ticket is generated, the SiteProtector system removes the vulnerable event from the Analysis view. To view the vulnerability, select the Show Incidents check box in the Analysis view.</li> <li>• You can view auto tickets in the Ticket view. The Creator for auto tickets is "Auto Ticket" and the Synopsis field describes which auto ticketing rule matched to generate the ticket.</li> </ul>

**Table 59:** *Stages of the SiteProtector system auto ticketing process*

## Rule inheritance

Auto ticketing rule inheritance occurs when a subgroup inherits the auto ticketing rules from a group of assets in the next higher group in your Site structure (if the subgroup does not have any auto ticketing rules).

### Example

The asset group Atlanta Servers contains a subgroup of assets called Accounting Servers. If you create auto ticketing rules for the Atlanta Servers group, the Accounting Servers subgroup (that does not have any auto ticketing rules applied) inherits the auto ticketing rules from the Atlanta Servers group.

**Note:** You can override the auto ticketing rule inheritance by creating auto ticketing rules for individual groups.

## Responsibility rules

When multiple vulnerabilities with different responsible asset owners or SiteProtector system users are included in a single ticket, the SiteProtector system applies the following rules:

- If an asset owner and a SiteProtector system user are both selected as the responsible parties, the SiteProtector system assigns the ticket to the asset owner.
- If different SiteProtector system users or different asset owners are selected as the responsible parties, the SiteProtector system assigns the ticket to the Default Responsible Party identified in the Auto Ticketing tab on the Ticketing Setup window.

## Creating auto ticketing rules

To create a vulnerability auto ticketing rule:

1. Right-click a group, and then select **Properties** from the pop-up menu.
2. Click the **Vulnerability Auto Ticketing** icon.

- To group the rules by asset, select the **Group By Asset** check box.

**Note:** Select this check box if you want the SiteProtector system to generate only one auto ticket for a single asset, rather than creating individual tickets for each vulnerability. You can modify the number of vulnerabilities per ticket in the Auto Ticketing tab in the Ticketing Setup window.

- Click the **Add** icon.

The Define Rule window appears.

- Ensure the **Enable Rule** check box is selected.
- Type a **Rule name** for the auto ticketing rule.
- Set the following rule options:


Option	Description
Vuln Severity	The severity level of the vulnerable event to match.
Asset Criticality	The Criticality field in the asset to match.
Asset Function	The Function field in the asset to match.
Asset OS	The OS Name (operating system name) field in the asset to match.
CVSS Value	The Common Vulnerability Scoring System (CVSS) score value to match.

**Note:** The **Criticality**, **Function**, and **OS Name** fields are defined in the asset properties.

- In the Ticket Values section, select the **Ticket Priority** level for tickets generated based on this rule.
- Select the **Responsibility**:

Option	Description
Asset Owner	The asset owner responsible for handling the ticket once it is created.
SiteProtector system User	The SiteProtector system user responsible for handling the ticket once it is created

- Click **OK**.

**Note:** When auto ticketing rules are enabled for a group, an auto ticketing icon  appears on the group folder in the left pane.

### Editing auto ticketing rules

To modify a vulnerability auto ticketing rule:

- Right-click a group, and then select **Properties** from the pop-up menu.
- Click the **Vulnerability Auto Ticketing** icon.
- Select an existing rule, and then click the **Edit** icon.

4. Do you want to disable the rule, but not delete it?  
If *yes*, then clear the **Enable Rule** check box and then go to Step 5. The SiteProtector system saves the rule for the group so you can enable it later.  
If *no*, go to Step 5.
5. Edit the following options as necessary:
  - Rule Name
  - Vuln Severity
  - Asset Criticality
  - Asset Function
  - Asset OS
  - CVSS Value
  - Ticket Priority
  - Responsibility
6. Click **OK**.

### Deleting auto ticketing rules

To delete a vulnerability auto ticketing rule:

1. Right-click a group, and then select **Properties** from the pop-up menu.
2. Click the **Vulnerability Auto Ticketing** icon.
3. Select the existing rule, and then click the **Delete** icon.

**Note:** If you just want to disable the rule, open the rule and clear the **Enable Rule** check box. The SiteProtector system saves the rule for the group so you can enable it later.

## Working with Ticketing Logs

### Introduction

The Response Logs tab shows you all the operations the system has performed on behalf of the ticket. For example, if the system sent an email, which was then forwarded to another person through the system, all of these steps would appear. The Log tab may also show pending system statuses.

### Viewing response logs for tickets

To view the response logs for a ticket:

1. In the left pane, select the group that contains the agent, asset, or event.
2. In the **Go to** list, select **Agent** or **Asset**.
3. In the right pane, right-click the agent or asset, and then select **List Tickets**.

The Tickets for Selected Items tab appears and lists the tickets for the item.

4. In the right pane, right-click the ticket, and then select **Open Ticket**.

The Ticket ID tab appears and displays the ticket information.

5. In the left pane, click the **Response Logs** icon.

The following response log information appears:

- Time stamp
- Reason
- Action
- Status
- Error
- Error Count

# Defining Notification Settings

## Introduction

The SiteProtector system can notify persons by email when certain aspects of a ticket change. For example, when a ticket status is updated, the SiteProtector system can notify the person who created the ticket. This feature provides a means of communicating ticket changes to persons associated with the ticket.

## Notification settings

Notification settings control the following:

- when the system notifies the person who creates the ticket
- when the system notifies the person responsible for the ticket
- the email addresses of SiteProtector system users

## Procedure

To define notification settings:

1. In the left pane, select the *Site Node*.
2. On the **Tools** menu, select **Ticketing Setup**.  
The Ticketing Setup window appears.
3. Select the **Notification** tab.
4. In the **E-mail Ticket Creator** section, select the following options:

Option	Description
on latent ticket	Notify the ticket creator when the ticket is past due.
on change to the ticket status	Notify the ticket creator when the ticket status changes.
on change to the ticket due date	Notify the ticket creator when the ticket due date changes.
on change to the ticket priority	Notify the ticket creator when the ticket priority changes.

5. In the **E-mail Responsible Party** section, select the following options:

Option	Description
on latent ticket	Notify the person responsible for the ticket when the ticket is past due.
on change to ticket status	Notify the person responsible for the ticket when the ticket status changes.
on change to ticket due date	Notify the person responsible for the ticket when the ticket due date changes.
on change to ticket priority	Notify the person responsible for the ticket when the ticket priority changes.
when a ticket is assigned	Notify the person responsible for the ticket when the ticket is assigned to that person.

6. Click **Apply**, and then click **OK**.

## Defining Ticket Priorities

### Introduction

Ticket priority provides a means of categorizing tickets by the amount of time allocated to resolve the ticket. The less time allocated to resolve the ticket, the higher its priority. This topic explains the following:

- the default ticket priorities available in the SiteProtector system
- how to create new ticket priorities
- how to delete ticket priorities
- how to update the attributes for a ticket priority

### Default ticket priorities

The SiteProtector system provides four default ticket priorities. You can edit the time allocations associated with the default ticket priorities, but you cannot delete the default ticket priorities. Table 60 describes the default ticket priorities.

Priority	Description
Critical	Ticket must be resolved within a week.
High	Ticket must be resolved within a month.
Medium	Ticket must be resolved within two months.
Low	Ticket must be resolved within six months.

**Table 60:** *Default ticket priority descriptions*

### Adding ticket priorities

To add a ticket priority:

1. In the left pane, select the *Site Node*.
2. On the **Tools** menu, select **Ticketing Setup**.  
The Ticketing Setup window appears.
3. Select the **Priority** tab, and then click **Add**.  
The Add a new priority window appears.
4. Type the following ticket attributes:

Attribute	Description
Priority	Name of the priority.
Maximum latency (in hours)	The amount of time allocated to resolve tickets assigned this priority, such as 24 hours.
Description	Textual description of the priority, such as ticket must be resolved within 24 hours.

5. Click **OK**.

**Deleting ticket priorities**

To delete a ticket priority:

1. In the left pane, select the *Site Node*.
2. On the **Tools** menu, select **Ticketing Setup**.  
The Ticketing Setup window appears.
3. Select the **Priority** tab.
4. Select the priority you want to delete, and then click **Delete**.  
The SiteProtector system displays a confirmation message.
5. Click **OK**.

**Updating ticket priority attributes**

To update the attributes for a ticket priority:

1. In the left pane, select the *Site Node*.
2. On the **Tools** menu, select **Ticketing Setup**.  
The Ticketing Setup window appears.
3. Select the **Priority** tab.
4. Select the priority you want to update, and then click **Modify**.  
The Update priority attributes window appears.
5. Edit the following attributes:

Attribute	Description
Priority	Name of the priority. <b>Note:</b> You cannot modify the name of the four default SiteProtector system ticket properties: Critical, High, Medium, and Low.
Maximum latency (in hours)	The amount of time allocated to resolve tickets assigned this priority such as 24 hours.
Description	Textual description of the priority such as ticket must be resolved within 24 hours.

6. Click **OK**.

## Defining Ticket Status

### Introduction

Ticket status describes the condition of a SiteProtector system ticket. This topic explains the following:

- the default ticket statuses available in the SiteProtector system
- how to add new ticket statuses
- how to modify the attributes for a ticket status
- how to delete ticket statuses

### Default ticket statuses

The SiteProtector system provides eight default ticket statuses. Each status is composed of the status name, tracking and reporting options (Working, Resolved, and Purgeable), and a description.

You can modify the tracking and reporting options or the description of a default status value, but you cannot rename or delete the status. Table 61 describes the default ticket statuses.

Status	Description
New	The ticket was just entered into the SiteProtector system.
Open	The ticket has been modified since being created.
In Progress	The ticket is currently being addressed.
Closed	Work required for the ticket has been completed.
Verified Closed	Ticket verification has been completed.
Pending System Verification	Vulnerabilities have been fixed. <b>Note:</b> Use this ticket status to verify fixes with the next scan.
System Verified Still Vulnerable	Vulnerabilities still exist after rescanning.
System Verified Success	Vulnerabilities have been fixed.

**Table 61:** *Default ticket status descriptions*

### Adding ticket statuses

To add a ticket status:

1. In the left pane, select the *Site Node*.
2. On the **Tools** menu, select **Ticketing Setup**.  
The Ticketing Setup window appears.
3. Select the **Status** tab, and then click **Add**.  
The Add a new status window appears.
4. Type a **Status** name.



- Select tracking and reporting options for the status:

Option	Description
Working	Keeps the ticket active and stored in the SiteProtector system Site database.
Resolved	Sets the ticket as inactive but stored in the SiteProtector system Site database. <b>Note:</b> The time a ticket is in this state will not add to the total working time of the ticket.
Purgeable	Allows the ticket to be removed from the SiteProtector system Site database. <b>Note:</b> Ticket purging is based on the database maintenance schedule you define. To modify the database schedule, click the Database Maintenance icon in the System view.

- Type a **Description** of the status.
- Click **OK**.

### Modifying ticket statuses

To update the attributes for a ticket status:

- In the left pane, select the *Site Node*.
- On the **Tools** menu, select **Ticketing Setup**.  
The Ticketing Setup window appears.
- Select the **Status** tab.
- Select the status you want to edit, and then click **Modify**.  
The Update status attributes window appears.
- Edit the status name, tracking and reporting options, and description as necessary.  
**Note:** You cannot modify the name of a default ticket status.
- Click **OK**.

### Deleting ticket statuses

To delete a ticket status:

- In the left pane, select the *Site Node*.
- On the **Tools** menu, select **Ticketing Setup**.  
The Ticketing Setup window appears.
- Select the **Status** tab.
- Select the priority you want to delete, and then click **Delete**.  
The SiteProtector system displays a confirmation message.  
**Note:** You cannot delete a SiteProtector system default status.
- Click **OK**.

## Defining Custom Categories

### Introduction

This topic explains how to create, edit, and delete custom categories.

### Creating custom categories

To create a custom category:

1. In the left pane, select the *Site Node*.
2. On the **Tools** menu, select **Ticketing Setup**.  
The Ticketing Setup window appears.
3. Select the **Custom Category** tab, and then click **Add**.  
The Add a new category window appears.
4. Type the category name and description.
5. In the **Custom Fields** section, click the **Add New Field** button.  
The Custom Category Field Attributes window appears.
6. Type the field name and description, and then select the **Is very large** option if the field will contain more than 3000 characters.
7. Repeat Step 5 through Step 6 to create additional custom fields, as necessary.  
**Note:** You can add a maximum of five custom category fields.
8. To change the order of the custom fields, select the custom field, and then click **Move up** to move the field up or **Move down** to move the field down.
9. Click **OK**.

### Editing custom categories

To edit a custom category:

1. In the left pane, select the *Site Node*.
2. On the **Tools** menu, select **Ticketing Setup**.  
The Ticketing Setup window appears.
3. Select the **Custom Category** tab.
4. In the **All Categories** section, select the category, and then click **Modify**.  
The Update Category Attributes window appears.
5. Edit the category name, description, and custom fields as necessary.
6. Click **OK**.

### Deleting custom categories

To delete a custom category:

1. In the left pane, select the *Site Node*.
2. On the **Tools** menu, select **Ticketing Setup**.  
The Ticketing Setup window appears.
3. Select the **Custom Category** tab.
4. In the **All Categories** section, select the category, and then click **Delete**.  
The SiteProtector system displays a confirmation message.
5. Click **OK**.

---

# Managing Ticketing Plug-ins

## Introduction

The SiteProtector system allows you to add and modify third-party software plug-ins that integrate ticketing into the SiteProtector system. For example, the SiteProtector system supports the Remedy Action Request System. The Site Protector system ticketing plug-in is enabled by default and you cannot modify it.

**Important:** Since only one plug-in at a time can be active in the SiteProtector system, after you activate a third-party plug-in, any new SiteProtector system tickets you create will be viewable only in the third-party ticketing system.

**Reference:** For more information about integrating the SiteProtector system with Remedy, see “Working with the Remedy Action Request System (Remedy)” on page 187.

## Adding plug-ins

To add a ticketing plug-in:

1. In the left pane, select the *Site Node*.
2. On the **Tools** menu, select **Ticketing Setup**.  
The Ticketing Setup window appears.
3. Select the **Plug-in** tab.
4. Click **Add**.
5. Type the plug-in **Name**.

**Example:** For the Remedy plug-in, type *Remedy*.

6. Type a **Description** of the plug-in.

**Example:** For the Remedy plug-in, type *Ticketing*.

7. Type the **Class Name**.

**Example:** For the Remedy plug-in, type  
`net.iss.rssp.ticketing.plugin.impl.RemedyTicketingPlugin`.

8. Click **OK**.
9. Select the plug-in you just added and click **Activate**.
10. Click **OK**.

## Modifying plug-ins

To modify a ticketing plug-in:

1. In the left pane, select the *Site Node*.
2. On the **Tools** menu, select **Ticketing Setup**.  
The Ticketing Setup window appears.
3. Select the **Plug-in** tab.
4. Select the plug-in you want to edit, and then click **Modify**.

The Update plug-in attributes window appears.

**Note:** You cannot modify the default SiteProtector system ticketing plug-in.

5. Edit the name, description, and class name fields as necessary.
6. Click **OK**.
7. Select the plug-in you just modified and click **Activate**.

8. Click **OK**.

# Defining Response Settings

## Introduction

Ticket response settings control the content and frequency of ticketing email notifications.

## Default response settings

You can modify the descriptions of the default SiteProtector system response settings. Table 62 describes the default ticket statuses.

Response setting	Description
Latent Response Scheduler Interval (hours)	Frequency that the SiteProtector system checks tickets to determine if they are latent. <b>Note:</b> Tickets are considered latent if the current date/time is past the due date/time.
Email content for latent ticket notification	The text that appears in the body of latent notification emails.
Email subject for latent ticket notification	The text that appears in the Subject line of latent ticket notification emails.
Maximum attempts	The number of times the SiteProtector system attempts to send an email response.
System email address	The email address that appears in the From field of outgoing emails.
System email server	The name or IP address of the outgoing mail server.
Email content for ticket change notification	The text that appears in the body of ticket change notification emails.
Email subject for ticket change notification	The text that appears in the Subject line of ticket change notification emails.
Email content for ticket creation notification	The text that appears in the body of ticket creation notification emails.
Email subject for ticket creation notification	The text that appears in the Subject line of ticket creation notification emails.
Validation response scheduler interval (hours)	How often the SiteProtector system checks tickets with a status of "pending system verification" to determine if they should be updated to a status of "system verified success" or "system verified still vulnerable."

**Table 62:** *Default ticket response settings*

## Modifying response settings

To modify a response setting:

1. On the **Tools** menu, select **Ticketing Setup**.  
The Ticketing Setup window appears.
2. Select the **Response** tab.
3. Select the response setting you want to edit, and then click **Modify**.  
The Modify Response Option window appears.  
**Note:** You cannot modify the response setting Attribute Name.

4. Type the new description for the attribute in the **Attribute Value field**, and then click **OK**.
5. Click **Apply**, and then click **OK**.

# Defining Auto Ticketing Settings

## Introduction

This topic explains how to modify the vulnerability auto ticketing settings. These settings control the processes associated with the automatic generation of tickets for vulnerabilities identified in a vulnerability assessment scan.

**Note:** You cannot modify attribute names.

**Reference:** For more information about vulnerability auto ticketing, see “Working with Vulnerability Auto Tickets” on page 192.

## Modifying auto ticketing settings

To modify auto ticketing settings:

1. In the left pane, select the *Site Node*.
2. On the **Tools** menu, select **Ticketing Setup**.

The Ticketing Setup window appears.

3. Select the **Auto Ticketing** tab.
4. Select an auto ticketing attribute to modify:

Attribute	Description
Default Responsible Party	<p>The user that the SiteProtector system assigns as the responsible party for auto-generated tickets if not specified in the auto ticketing rule.</p> <p><b>Important:</b> When you create an auto ticketing rule, you must also specify the Default Responsible Party.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• To edit the list of SiteProtector system users, select <b>Tools</b> → <b>User Groups</b>.</li> <li>• To add an email address, click <b>Tools</b> → <b>User Email Addresses</b>.</li> </ul>
Scheduler interval for running all group rules	The frequency that the SiteProtector system applies the auto ticketing rules.
System Validity Period	<p>The number of days that the SiteProtector system will not generate more than one auto ticket for the same vulnerability.</p> <p><b>Note:</b> If the SiteProtector system creates an auto ticket for a vulnerability within this time period, it will not generate another auto ticket for the same vulnerability. For example, if this is set to 30, and the vulnerability still exists, on the 31st day the SiteProtector system will create a new auto ticket.</p>

<b>Attribute</b>	<b>Description</b>
Vulnerabilities per Ticket	The number of vulnerabilities included in one auto ticket when the auto tickets are grouped by asset. <b>Notes:</b> <ul style="list-style-type: none"><li>• Once this maximum is reached, the SiteProtector system creates a new ticket. For example, if you set this to 40, when there are 41 vulnerabilities in an asset, the SiteProtector system creates two separate tickets when you group by asset.</li><li>• If you want the SiteProtector system to generate only one auto ticket for a single asset (rather than creating individual tickets for each vulnerability), select the Group By Asset check box in the Vulnerability Auto Ticketing pane in the Properties tab.</li></ul>

5. Click **Modify**.
6. Type the new value for the attribute in the **Attribute Value** field, and then click **OK**.
7. Click **Apply**, and then click **OK**.



## Setting Up Groups



## Chapter 15

# The Group Setup Stage

## Overview

### Introduction

The second stage of the SiteProtector system setup process is the Group Setup stage. In this stage, you create groups that appear in the left pane of the Console and implement a system for populating the groups with assets and agents. This chapter provides an overview of the Group Setup stage.

**Note:** The SiteProtector system automatically organizes and groups the SiteProtector system components, such as the Agent Manager and Site Database, into the Site Node. You cannot move these components out of this group, so there is no need to regroup these components. The procedures in this stage are intended to group other assets and agents.

### In this chapter

This chapter contains the following topics:

Topic	Page
Overview of this Stage	212
Checklist for this Stage	213

## Overview of this Stage

### Introduction

This topic provides an overview of the Group Setup stage.

### Group structure

Before you begin the process of creating the groups, you should develop a plan for organizing the groups that is based on your environment and security requirements. The SiteProtector system supports any group structure that meets your security management needs. The plan can guide you in the Group Setup stage.

**Note:** If you import assets from Active Directory, then the Active Directory structure, including the groups and subgroups, will appear in the Console. You cannot edit or change imported Active Directory groups. If you want to be able to edit and change the groups and still retain the Active Directory structure, then you must replicate the Active Directory structure in the Console.

### Group properties

During the Group Setup stage, you configure properties for the groups you create, such as the following:

- *Group Membership Rules* that help the SiteProtector system automatically populate the groups with network assets identified by agents.

When the SiteProtector system and the other IBM ISS products integrated with it begin to identify security events and assets on your network, the amount of information entering the SiteProtector system can be significant. *Group Membership Rules* work together the *Group Ungroup Assets* job to automatically organize this information as it enters the system. Setting up Group Membership rules in advance can eliminate the cumbersome tasks of manually grouping assets after they enter the system.

- *Group-Level User Permissions* that control the tasks a SiteProtector system user can perform on the assets and agents in the group.

The number assets, agents, and tasks required to manage a group can be significant. This variety can require different users to perform different tasks on the same group. The SiteProtector system provides you with the ability to control and restrict a user's actions at the very specific group level. For example, you can grant one user the ability to run scans on a group of assets, and you can grant another use the ability to apply policies to the agents in the same group.

### Group tuning

After you set up the groups in the Console, you can add, delete, and edit groups and group properties later to meet your changing security requirements.

## Checklist for this Stage

### Introduction

This topic provides a checklist for setting up groups.

### Checklist

Table 63 provides a task checklist to ensure that you perform all the tasks required to set up groups for your assets and agents.

✓	Task
<input type="checkbox"/>	Develop a plan and structure for organizing your network assets and the agents that monitor them into groups. See “Organizing Groups and Subgroups” on page 223.
<input type="checkbox"/>	Create the groups based on this structure, and then define the properties for the groups, including Membership Rules. See “Creating Groups” on page 225.
<input type="checkbox"/>	Set up permissions for users to perform tasks with the assets and agents in the groups. See “Setting up Group-Level Permissions” on page 235.

**Table 63:** *Checklist for setting up groups*



## Chapter 16

# Setting Up Groups

## Overview

### Introduction

This chapter provides information about setting up groups.

### Requirement

After installation, the SiteProtector system includes the default groups only. You must set up additional groups for your assets and other IBM ISS products. The SiteProtector system does not create these groups for you.

### In this chapter

This chapter contains the following topics:

<b>Topic</b>	<b>Page</b>
What are Groups?	216
Default Group Names	219
Organizing Groups and Subgroups	223
Creating Groups	225
Creating System Scanner Vulnerability Assessment Application Groups	228

## What are Groups?

### Introduction

A group is a collection of network assets and the SiteProtector system components or agents that reside on those assets. For example, you create a group called *Atlanta Servers* with an IP range of 175.12.13.15-175.20.30.50. This group includes the following members:

- the assets with an IP address within the IP range
- the agents installed on the assets

A subgroup is a group that exists beneath another group.

### Importance of groups

Groups are important because they provide the following:

- A method for organizing, accessing, and managing important information about the network assets monitored by the SiteProtector system and other IBM ISS products.
- A method for organizing and managing the other IBM ISS products that work with the SiteProtector system.
- A method for performing SiteProtector system tasks on groups of assets and agents, such as applying policies to agents in a group or viewing the security events for a specific group of assets.
- A navigational tool in the Console that you can use to move between different groups of network assets and agents as you perform your security management tasks.

### Default group names

The SiteProtector system includes some default groups after initial installation. For a complete list of these groups and descriptions of each, see “Default Group Names” on page 219.

### How are assets and agents added to groups?

Table 64 describes how assets and agents are added to groups. Group contents

The SiteProtector system Console provides several different views into the contents of a group. Table 64 lists the views and describes the group contents that you can see with each view.

View	Contents
Agent View	Shows the agents and the SiteProtector system components <sup>a</sup> installed on the assets in this group.
Asset View	Shows the assets <sup>b</sup> , including computers, servers, and other devices, that are members of the group.
Analysis View	Shows the security events generated by agents in this group; events are related to the assets in the group.
Policy View	Shows the security policies and responses set for the agents in the group.
Reporting View	Provides options for generating reports about the group such as a report showing events generated by a Desktop Protection agent in the group.
Ticketing View	Shows the open and closed tickets for agents, components, and assets in the group; also shows ticket activity and history; also provide options for managing tickets for the group.

**Table 64:** *Viewing group contents*



View	Contents
Properties	<p>Shows the following:</p> <ul style="list-style-type: none"> <li>• For agents that are members of the group, it shows properties such as details and command jobs for the agents.</li> <li>• For components that are members of the group, it shows properties such as details and command jobs.</li> <li>• For the group itself, it shows properties such as the permissions set on the group and the membership rules set for the group.</li> <li>• For the <i>Site Node</i> group, it shows properties such as global Site permissions and command jobs for the entire Site.</li> <li>• For the group called <i>Site Group</i>, it shows properties such as command jobs and policies for any “Site-level policy” agents that are members of the group.</li> </ul> <p><b>Note:</b> You must choose an agent, component, group, or Site to view the Properties View. It is not listed as a choice in the Go to list.</p>

**Table 64:** *Viewing group contents*

- a. The SiteProtector system keeps the Site components, including Site Database, Event Collector, Application Server, and Agent Manager, in the Site Group. You cannot move the components out of this group, but you can copy them to other groups. The Site Group is the top level group in the Site and has a user-defined name. IBM ISS recommends that you manage the SiteProtector system components in the Site Group.
- b. An asset can be a member of multiple groups.

**Group properties**

Table 65 describes the group properties that you can set and manage.

<b>Property</b>	<b>Description</b>
Details	Used to manage detailed information about the group, including group name and description.
Membership Rules	Used when you run an Group Ungrouped Assets job to automatically group ungrouped assets; before the SiteProtector system can add an asset to the group, the asset must meet the criteria you set in the membership rules for the group.
Permissions	Used to control a user's ability to view, modify, and control the assets in the group.
Command Jobs	Used to view information about SiteProtector system jobs such as scan jobs that you run on the group, including the following: <ul style="list-style-type: none"><li>• SiteProtector system jobs that are scheduled to run on the group</li><li>• SiteProtector system jobs that have completed running on the group</li><li>• the progress of SiteProtector system jobs currently running on the group</li></ul>

**Table 65:** *Group properties*

# Default Group Names

**Introduction** This topic describes the default groups that appear in the left pane after you first install the SiteProtector system.

**Default group name** Table 66 describes the default groups displayed in the left pane of the Console; the table lists the names in the order that they appear in the left pane.

Name	Description
My Sites	<p>Includes all active Sites appear below <i>My Sites</i>. For example, if you log on to five sites, then you see the five sites listed under <i>My Sites</i>. The <i>My Sites</i> name is created by default at the time you install the SiteProtector system and cannot be changed or deleted.</p> <p><b>Contents</b>  <i>My Sites</i> contains all active Sites.</p> <p><b>Tasks Allowed</b>            You can perform Console-level tasks such as configuring Console options at the <i>My Sites</i>-level.</p> <p><b>Node Name</b>  <i>My Sites</i> is referred to as the root node.</p> <p><b>Icon</b>            The IBM ISS icon represents <i>My Sites</i>.</p>
Site Node	<p>The <i>Site Node</i> is the name of the computer where the Site resides. The name of the <i>Site Node</i> is system-generated at the time you install the SiteProtector system and cannot be changed or deleted. You can log on to multiple Sites in the Console. If you are logged on to multiple Sites, then you will see multiple <i>Site Nodes</i> in the left pane of the Console.</p> <p><b>Contents</b>            The <i>Site Node</i> contains SiteProtector system components only. You cannot remove the components from the <i>Site Node</i>, but you can copy them to other groups.</p> <p><b>Tasks Allowed</b>            You can perform Site-level tasks at the <i>Site Node</i>-level such as managing global permissions and policies for some IBM ISS products.</p> <p><b>Node Name</b>  <i>Site Node</i> is referred to as Site node.</p> <p><b>Icon</b>            The building icon represents the <i>Site Node</i>.</p> <p><b>Examples</b></p> <ul style="list-style-type: none"> <li>• 125.1.4.50</li> <li>• Atlanta Computer_01</li> <li>• Localhost</li> </ul>

**Table 66:** *Default group descriptions*

Name	Description
Site Group	<p>The <i>Site Group</i> is the first group created in the Site. It is automatically created by the SiteProtector system during installation. The name of the <i>Site Group</i> is user defined at the time you install the SiteProtector system. You can change the <i>Site Group</i> name in the <i>Site Group Properties</i>, but you cannot delete the <i>Site Group</i>.</p> <p><b>Contents</b></p> <p>The <i>Site Group</i> can contain SiteProtector system components and other network assets.</p> <p><b>Tasks Allowed</b></p> <p>You can perform group-level tasks at the <i>Site Group</i>-level such as setting group permissions and applying policies.</p> <p><b>Node Name</b></p> <p><i>Site Group</i> is referred to as the Site Group node.</p> <p><b>Icon</b></p> <p>The folder icon represents the <i>Site Group</i>.</p> <p><b>Examples</b></p> <ul style="list-style-type: none"> <li>• Atlanta Site</li> <li>• Site 01</li> <li>• Site East</li> </ul>
Group	<p>A <i>Group</i> is any group that you create in the SiteProtector system to hold assets. No groups exist in the Site until you create them. All groups are subgroups to the <i>Site Group</i>. The <i>Group</i> name is user defined at the time you create the group. You can create an unlimited number of groups in the Site as well as name and organize them based on your requirements.</p> <p><i>Subgroups</i> are exactly like groups except they exist below another group.</p> <p><b>Contents</b></p> <p><i>Groups</i> can contain SiteProtector system components and network assets monitored by the SiteProtector system, such as servers, routers, and other network devices. <i>Groups</i> do not contain SiteProtector system components.</p> <p><b>Tasks Allowed</b></p> <p>You can perform group-level tasks at the <i>Group</i>-level such as setting group permissions and applying policies.</p> <p><b>Node Name</b></p> <p><i>Group</i> is referred to as the Group node.</p> <p><b>Icon</b></p> <p>The folder icon represents a <i>Group</i>.</p> <p><b>Examples</b></p> <ul style="list-style-type: none"> <li>• DMZ</li> <li>• Web Servers</li> <li>• Event Collectors</li> <li>• Desktop Agents</li> </ul>

Table 66: Default group descriptions (Continued)

Name	Description
Site Group	<p>The <i>Site Group</i> is the first group created in the Site. It is automatically created by the SiteProtector system during installation. The name of the <i>Site Group</i> is user defined at the time you install the SiteProtector system. You can change the <i>Site Group</i> name in the <i>Site Group</i> Properties, but you cannot delete the <i>Site Group</i>.</p> <p><b>Contents</b></p> <p>The <i>Site Group</i> can contain SiteProtector system components and other network assets.</p> <p><b>Tasks Allowed</b></p> <p>You can perform group-level tasks at the <i>Site Group</i>-level such as setting group permissions and applying policies.</p> <p><b>Node Name</b></p> <p><i>Site Group</i> is referred to as the Site Group node.</p> <p><b>Icon</b></p> <p>The folder icon represents the <i>Site Group</i>.</p> <p><b>Examples</b></p> <ul style="list-style-type: none"> <li>• Atlanta Site</li> <li>• Site 01</li> <li>• Site East</li> </ul>
Group	<p>A <i>Group</i> is any group that you create in the SiteProtector system to hold assets. No groups exist in the Site until you create them. All groups are subgroups to the <i>Site Group</i>. The <i>Group</i> name is user defined at the time you create the group. You can create an unlimited number of groups in the Site as well as name and organize them based on your requirements.</p> <p><i>Subgroups</i> are exactly like groups except they exist below another group.</p> <p><b>Contents</b></p> <p><i>Groups</i> can contain SiteProtector system components and network assets monitored by the SiteProtector system, such as servers, routers, and other network devices. <i>Groups</i> do not contain SiteProtector system components.</p> <p><b>Tasks Allowed</b></p> <p>You can perform group-level tasks at the <i>Group</i>-level such as setting group permissions and applying policies.</p> <p><b>Node Name</b></p> <p><i>Group</i> is referred to as the Group node.</p> <p><b>Icon</b></p> <p>The folder icon represents a <i>Group</i>.</p> <p><b>Examples</b></p> <ul style="list-style-type: none"> <li>• DMZ</li> <li>• Web Servers</li> <li>• Event Collectors</li> <li>• Desktop Agents</li> </ul>

Table 66: Default group descriptions (Continued)

Name	Description
Ungrouped Assets	<p>The <code>Ungrouped Assets</code> group is created and named by default at the time you install the SiteProtector system and cannot be changed or deleted. As the SiteProtector system detects assets on your network, they are typically moved to other groups and subgroups during jobs to Group Ungrouped Assets. Any asset that remains ungrouped is stored in <code>Ungrouped Assets</code>.</p> <p><b>Contents</b></p> <p><code>Ungrouped Assets</code> contains <i>site ranges</i>, which contain ungrouped assets listed by their IP address.</p> <p><b>Tasks Allowed</b></p> <p>You can perform the following tasks at the <code>Ungrouped Assets</code>-level:</p> <ul style="list-style-type: none"> <li>• Run a Group Ungrouped Assets job to automatically move ungrouped assets to other groups and subgroups based on group membership rules</li> <li>• Create Site ranges</li> </ul> <p><b>Node Name</b></p> <p><code>Ungrouped Assets</code> is referred to as the <code>Ungrouped Assets</code> node.</p> <p><b>Icon</b></p> <p>The world icon represents <code>Ungrouped Assets</code>.</p> <p><b>Note:</b> IBM ISS recommends that you move ungrouped assets into groups and subgroups with more meaningful names as soon as possible in the set up.</p>
Site Range	<p>A <i>site range</i> is a unique type of subgroup in <code>Ungrouped Assets</code>. The first site range is created and named by default at the time you install the SiteProtector system. You can delete this site range or create additional site ranges as necessary.</p> <p><b>Contents</b></p> <p><i>Site ranges</i> contain ungrouped assets listed by their IP address.</p> <p><b>Examples</b></p> <ul style="list-style-type: none"> <li>• 120.5.6.70 - 120.5.6.90</li> <li>• 125.4.5.60 - 125.4.5.90</li> </ul>

Table 66: Default group descriptions (Continued)

# Organizing Groups and Subgroups

## Introduction

Before you create groups and subgroups, you should develop a plan for organizing the groups. This topic provides information about organizing groups.

## Strategies

Most strategies for organizing groups are based on categories of assets that reflect the asset's purpose, function, and security position in your organization. Table 67 lists some of these categories and provides examples of group names based on the categories.

Category <sup>a</sup>	Example
Department	<i>Site Node</i> <i>Site Group</i> Human Resources Accounting Customer Support Manufacturing
Geography	<i>Site Node</i> <i>Site Group</i> Atlanta Dallas Los Angeles
Business Purpose	<i>Site Node</i> <i>Site Group</i> Development Web Sales
Asset Type	<i>Site Node</i> <i>Site Group</i> Servers Desktops Databases Routers
Agent Type	<i>Site Node</i> <i>Site Group</i> Network Sensors Network Internet Scanners Event Collectors Appliances
Command Jobs	<i>Site Node</i> <i>Site Group</i> Monitor Scan

**Table 67:** *Strategies for organizing groups*

Category <sup>a</sup>	Example
Combination	<i>Site Node</i> <i>Site Group</i> Network Sensors Network Internet Scanners Event Collectors Appliances Scan Analyze Atlanta Servers Dallas Servers
Combination with subgroups	<i>Site Node</i> <i>Site Group</i> Sensors Network Sensors Server Sensors Scanners System Scanner vulnerability assessment application Network Internet Scanners Appliances Proventia Network IPS Proventia Network MFS Atlanta Servers Routers Dallas Servers Routers

**Table 67:** *Strategies for organizing groups (Continued)*

a. An asset can be a member of multiple groups. For example, an asset might be a member of Scan and Web Servers.



# Creating Groups

## Introduction

After you develop a plan for organizing your assets into groups, you should create the groups, define the properties for the groups, and structure them to reflect the organizational plan. For example, if you choose to organize assets into groups by geography, then you should create groups for each geographic region.

## Task overview

Table 68 describes the tasks for creating groups.

Task	Description
1	Create the group.
2	Assign an Agent Manager to the group.
3	Define membership rules for the group.
4	Set group-level permissions for the group.

**Table 68:** *Tasks for creating groups*

## Creating groups

To create a group:

1. In the left pane, right-click a group, and then select **New** → **Group** from the pop-up menu.

**Note:** If you are adding groups to the SiteProtector system for the first time, then you must select the top level group to begin. After you add the first group, you can add other groups as subgroups of these groups.

The *New Group* folder appears below the selected group.

2. Type the group name in the highlighted box, and then press ENTER.  
The group appears in the left pane.

## Assigning Agent Managers

To assign an Agent Manager to the group:

1. In the left pane, right-click the group, and then select **Properties** from the pop-up menu.

The Properties tab appears.

2. In the left pane, select **Group Settings**.

The Group Settings window appears in the right pane.

3. Select the **Agent Manager List** tab.

4. Select an Agent Manager from the list.

**Note:** If the Agent Manager you want to assign does not appear in the list, then click **Add** to add the Agent Manager to the list.

5. Click **OK**.
6. Right-click the **Properties** tab, and then select **Close** from the pop-up menu.

## Membership rules

You can run or schedule a Group Ungrouped Assets job to automatically move assets out of Ungrouped Assets to other groups in the Site. The job uses membership rules to

determine where to relocate the assets. You must set up membership rules before you run or schedule a Group Ungrouped Assets job.

When you define membership rules, you must choose only one type per group. Table 69 describes the available types and provides the allowed formats and examples for each type.

Type	Description	Formats	Examples
IP Address	Use this type to restrict membership based on an asset's IP address.	Single IP address	125.4.5.60
		IP address range	120.4.5.50-120.4.5.53
		IP address with wildcard	126.4.5.*
DNS Name	Use this type to restrict membership based on an asset's DNS name.	Single DNS name	HR_01.Atlantabran.ch.com
		DNS name with wildcard	AP_*.Atlantabran.ch.com
NetBIOS Name	Use this type to restrict membership based on an asset's NetBIOS name.	Single NetBIOS name that includes any of the following characters: <ul style="list-style-type: none"> <li>• 0-9</li> <li>• A-Z</li> <li>• a-z</li> <li>• the dash (-)</li> <li>• !@#%&amp;^&amp;()._~{}</li> </ul>	AT-US_9A0Z@
		Single NetBIOS name that includes wildcards	AT-*
Operating System Name	Use this type to restrict membership based on an asset's operating system.	Any operating system name that includes any characters	Windows 2000
		Operating system name that includes wildcards	Windows*

**Table 69:** *Types of membership rules*

## Defining membership rules

To define membership rules for a group:

- In the left pane, right-click the group, and then select **Properties** from the pop-up menu.  
The Properties tab appears.
- Click the **Membership Rules** icon.
- In the **Type** list, select the type of membership rules to use to for this group:
  - IP Address
  - DNS Name
  - NetBIOS Name
  - Operating System Name

**Note:** You can use only one type per group, but you can define multiple rules of that type. For example, if you choose IP address, then you can define ten membership

---

rules based on IP address. You cannot define one rule based on IP address and one rule based on operating system.

4. Type a **Rule** in the row that has an asterisk in the first column, and then press ENTER.

**Tip:** For more information about rules, see Table 69, “Types of membership rules” on page 226 or the help below the Type box in the Console.

**Note:** For IP address types, if you type an invalid rule, the asterisk changes to a red X. You must correct the membership rule before you continue.

5. Right-click the **Properties** tab, and then select **Close** from the pop-up menu.

# Creating System Scanner Vulnerability Assessment Application Groups

## Introduction

When the SiteProtector system receives the first event from the System Scanner Databridge, it automatically creates a *System Scanner vulnerability assessment application* group. This topic explains how to perform the following tasks on this group:

- move the group
- rename the group

## Default subgroup structure

The SiteProtector system automatically creates the following subgroup structure for the System Scanner vulnerability assessment application group in the Enterprise Groups pane.

Level	Description
1	System Scanner vulnerability assessment application
2	<i>SystemScannerDNSName_SystemScannerDatabaseName</i>
3	System Scanner vulnerability assessment application group names that appear in the System Scanner Console.

**Table 70:** *System Scanner vulnerability assessment application subgroups*

## Moving the group

To move the System Scanner vulnerability assessment application group:

1. In the left pane, delete the default System Scanner vulnerability assessment application group.
2. Create a new group named **System Scanner**.

The SiteProtector system creates the new group structure as it receives new events, such as when you scan an asset.

## Renaming the group

To rename the System Scanner vulnerability assessment application group:

1. In the left pane, create a new group.
2. Run the following SQL command in the SQL Query Analyzer:

```
INSERT INTO VERSION (ATTRIBUTENAME, ATTRIBUTEVALUE)
VALUES ('SystemScannerGroupName', 'Custom_Group_Name')
```

**Example:** To change the name of your System Scanner group to "SystemScannerevents," run the following command:

```
INSERT INTO VERSION (ATTRIBUTENAME, ATTRIBUTEVALUE)
VALUES ('SystemScannerGroupName', 'SystemScannerevents')
```

The SiteProtector system creates the new group structure as it receives new events, such as when you scan an asset.

## Chapter 17

# Setting Group-Level Permissions

## Overview

### Introduction

This section provides information about setting group-level permissions.

### Recommendation

The default SiteProtector system user groups have some default group-level permissions. If you add users to these groups, then the users automatically have the default group-level permissions. You must set group-level permissions in the following situations:

- The group-level permissions set for the SiteProtector system user groups do not meet your security requirements.
- You create custom SiteProtector system user groups and want to set group-level permissions for the user groups.
- You want to implement very specific control over a users actions at the asset group level.
- You want to provide a user with very limited and restricted access to the SiteProtector system.

### In this chapter

This chapter contains the following topics:

Topic	Page
What are Group-Level Permissions?	230
Working with the Permissions Property Window	233
Setting up Group-Level Permissions	235
Working with Permission Inheritance	238
Setting Permissions with Show Subgroups Enabled	241

## What are Group-Level Permissions?

### Introduction

Group-level permissions are different from global permissions, which provide Site-wide functionality to users, such as the ability to manage licenses or manage global security responses in the entire Site. Group-level permissions do not provide Site-wide functionality. Group-level permissions provide control over the actions a user can perform with the assets and agents in an individual group or groups.

### Definition: group

The term group in group-level permissions refers to SiteProtector system groups that contain assets and agents. For example, you might set up group-level permissions for an Atlanta Servers group. The term does not refer to user groups as in the Administrator user group.

### Who has group-level permissions?

All SiteProtector system users, including individual users, groups of users, and members of SiteProtector system user groups, have group-level permissions. The permissions assigned to the SiteProtector system users groups vary depending on the role of the users in the group. You can also assign group-level permissions to individual users or groups of users who are not members of a SiteProtector system user group.

### What do group-level permissions control?

Group-level permissions provide very specific control over users actions in the SiteProtector system. For example, group-level permissions control users ability to perform actions such as the following:

- log on to the Site
- change group properties, such as name and membership rules
- add, modify, and remove assets in a group
- add, modify, and remove agents in a group
- apply updates and policies to agents in a group
- view properties and log files for assets and agents in a group
- print report about the assets and agents in a group
- start, stop, restart, and refresh agents in a group

Because the SiteProtector system supports many agents and group related tasks, there are many individual group-level permissions. Each permission controls a very specific action in the SiteProtector system.

**When do you set group-level permissions?**

You can set group-level permissions at any time. For example, you can set group-level permissions before you populate the group with assets or agents, or you can wait until after you populate the group to set the group-level permissions. IBM ISS recommends that you set up the groups and populate the groups before you configure permissions for the group.

Table 71 provides information about the tasks required to set group-level permissions at different times in the SiteProtector system setup process.

If you want to...	Then...
set group-level permissions before you set up the actual groups and populate them with agents	set the group-level permissions at the top-level group, called the <i>Site Group</i> , and then turn on the Inherit Permissions options for all subgroups. <b>Note:</b> This action replicates the top-level group permissions on all subgroups in the Site. Because all groups in the Site are subgroups of the <i>Site Group</i> , this action essentially replicates the top-level group permissions on all groups in the Site.
set group-level permissions after you set up the actual groups and populate them with agents	complete the tasks described in the following sections before you set up group-level permissions: <ul style="list-style-type: none"> <li>• “Setting Up Groups” on page 209.</li> <li>• “Setting Up Agents” on page 255.</li> </ul> <b>Note:</b> IBM ISS recommends that you set group-level permissions after you set up the groups and populate them.

**Table 71:** *When to set group-level permissions*

**Who manages group-level permissions?**

The group owner sets and manages group-level permissions for a specific group. You specify the group owner at the time you create the group or in the group properties after you create the group. The group owner can perform the following tasks:

- grant and remove group-level permissions
- change the group owner

By default, the user or user group that creates the group is the group owner. The group owner can be any of the following:

- an individual local user
- a local user group
- an individual domain user
- a domain user group
- a SiteProtector system user group

**Note:** There is no limit to the number of actual users who can be group owner, but you can only assign a maximum of one individual user or one user group as group owner. For example, you create a SiteProtector system user group called *Atlanta Administrators* and put five individual users in the group. You then assign Atlanta Administrators as group owner to a group. All five individual users are considered group owner.

**Where do you manage group-level permission?**

You set and manage group-level permissions in the properties for the group on the Permission Property window.

**Reference:** See “Working with the Permissions Property Window” on page 233.

**How many users can have group-level permissions?**

There is no limit to the number of different users who can have group-level permissions for the same group. You can also set different permissions for the different users in the same group. For example, you can set group-level permissions so that three users have different permissions on the same group as follows:

- One user called *jsmith* has permission to view the assets in the group and run reports about the assets in the group.
- Another user called *ataylor* has permission to run scans on the assets in the group.
- Another user called *pharris* has permission to update the agents in the group.

**How do I pass down permissions to subgroups?**

After you set group-level permissions for one group, you can pass the permissions to all the subgroups in that group. This feature is called permission inheritance. For more information, see “Working with Permission Inheritance” on page 238.



# Working with the Permissions Property Window

## Introduction

This topic provides information about the Permissions Property window and instructions for the following tasks:

- understanding color indicators on the Permissions Property window
- selecting and deselecting permissions in the permissions list
- expanding and collapsing permissions in the permissions list

## Permissions Property window description

For each group of assets and agents, the SiteProtector system provides a Permission Property window. You can view and manage all the group-level permissions for that group in this window.

## Areas of the window

Table 72 lists all the possible agents such as Network Internet Scanner that might be present in the group and the group-level permissions for each agent.

Area	Description
Left pane	<ul style="list-style-type: none"> <li>• Lists all the users and user groups who have permissions for this group.</li> <li>• Provides options for adding and removing users from the group.</li> </ul>
Right pane	Lists all group-level permissions. This lists includes all possible permissions, including permissions for agents that might not be in the group.

**Table 72:** *Areas of the Permissions Property window*

In the permissions property sheet, you can define all types of access to that group and set up multiple access profiles for different users, groups or SiteProtector system groups. For example, you can set up two access profiles for a group:

- one that provides a user group read only access to the group of assets and access to some reports
- one that provides the user group with the ability to update the group and run agents in the group.

If a specific type of asset is not present in the group, then the related group-level permission is not applicable to that group. For example, if there are no Network Internet Scanners in a group, then the group-level permissions related to Network Internet Scanner are not applicable to that group.

**Understanding color indicators**

Table 73 describes the color indicators that appear on the Permission Property window.

Circle Color	Description
Black	<p>This color indicates one of the following:</p> <ul style="list-style-type: none"> <li>• If it appears next to an individual permission, then the permission is assigned to the user or group.</li> <li>• If it appears next to a top level permission, meaning that there are sub-permissions within that main category, then all individual permissions in that category are assigned to the user or group.</li> </ul> <p>You can edit the permissions.</p>
White	<p>This color indicates one of the following:</p> <ul style="list-style-type: none"> <li>• If it appears next to an individual permission, then the permission is not assigned to the user or group.</li> <li>• If it appears next to a top level permission, meaning that there are sub-permissions within that main category, then none of the individual permissions in that category are assigned to the user or group.</li> </ul> <p>You can edit the permissions.</p>
Half black, half white	<p>This color combination can only appear next to a top level permission. A top level permission is one that contain sub-permissions. This combination indicates that some of the individual permissions in that category are assigned to the user or group, but not all.</p> <p>You cannot edit the permission.</p>
Grey	<p>This color indicates that permission inheritance is turned on for this asset group.</p> <p>You cannot edit the permissions.</p>

**Table 73:** *Color indicators on the permission property window*

**Selecting or deselecting permissions**

- To select or deselect permissions from the permissions list:
  - Select the circle that corresponds to the permission.

The color of the circle changes depending upon whether the permission is selected.

**Expanding the permissions list**

- To expand the permissions list for an individual report or agent:
  - Click the plus sign (+) next to the permission.
- To expand all permissions:
  - Right-click any permission, and then select **Expand All**.

**Collapsing the permissions list**

- To collapse the permission list for an individual report or agent:
  - Click the minus sign (-) next to the permission.
- To expand all permissions:
  - Right-click any permission, and then select **Collapse All**.

---

# Setting up Group-Level Permissions

<b>Introduction</b>	<p>This topic explains how to set group-level permissions for the following:</p> <ul style="list-style-type: none"><li>● SiteProtector system user groups</li><li>● local users and groups</li><li>● domain users and groups</li></ul> <p><b>Important:</b> If you turn on the “inherit permissions from parent group” when you grant a group-level permissions, then the permissions set on the group’s parent are transferred to this group.</p>
<b>Group owner</b>	<p>Only the group owner or Administrator can set up group-level permissions.</p>
<b>Group levels in the left pane</b>	<p>You can grant group-level permissions at the following group levels in the left pane:</p> <ul style="list-style-type: none"><li>● <i>Site Group</i> level</li><li>● <i>Group</i> level</li></ul> <p>You cannot grant group-level permissions at the following group levels in the left pane:</p> <ul style="list-style-type: none"><li>● <i>Site Node</i> level</li><li>● <i>Ungrouped Assets</i> level</li></ul> <p>Only users in the SiteProtector system user grouped called Administrator can work with the Ungrouped Assets group.</p> <ul style="list-style-type: none"><li>● <i>Site Range</i> level</li></ul>
<b>Requirement</b>	<p>All SiteProtector system users <i>must</i> have the permission called Group-View at the <i>Site Group</i> level before they can login to a Site. This requirement applies to all of the following:</p> <ul style="list-style-type: none"><li>● local users and local groups</li><li>● domain users and domain groups</li><li>● SiteProtector system user groups</li></ul>
<b>Before you begin</b>	<p>IBM ISS recommends that you set up groups before you configure group-level permissions. See “Creating Groups” on page 225.</p>
<b>Setting permissions before you setup assets and agents</b>	<p>You can set up group-level permissions before set up agents and assets. Setting group-level permissions before you set up agents and assets is recommended in the following situations:</p> <ul style="list-style-type: none"><li>● You can anticipate exactly the assets and agents that will be members of the group.</li><li>● You want to set the permissions at the <i>Site Group</i> level (top level group in the Site) and force all groups and subgroups in the Site to inherit the permissions.</li></ul>

Without agents or assets present in the Site, it is very difficult to anticipate the permission requirements for the groups in the Site. If you want to set up agent and assets first, then go to these topic and complete these tasks before you set up group-level permissions:

- “Setting Up Agents” on page 255.
- “Adding Assets” on page 293.

**Permissions required for Enterprise Scanner policies**

For users to effectively run scans with Proventia Network Enterprise Scanner, one of the permissions they must have is the View permission on the Network Locations policy. You must assign this permission at the group they need to scan, as well as any group above this one in the hierarchy.

**Suggestion:** Grant View Network Locations Policy permissions and do not remove inheritance, so the user will have this permission at the Site group level and each child group within the Site.

**Task overview**

Table 74 describes the tasks for setting up group-level permissions.

Task	Description
1	Add the user or group to the asset group.
2	Grant and remove group-level permissions for the user or group.

**Table 74:** Tasks for setting up group-level permissions

**Adding users or groups to asset groups**

To add a user or group to the asset group:

1. In the left pane, right-click the *Site Group* or another *group*, and select **Properties**.  
The Group Properties tab appears.
2. Click the **Permissions** icon.  
The Group-level permissions management window appears.
3. In the **Users and/or Groups** column, click **Add**.  
The Search Users/Groups to Add window appears.
4. Use the following table to determine your next steps:

If you want to add...	Then...
local users or groups to the SiteProtector system user group	type the complete account using the following syntax, and then click <b>OK</b> : <ul style="list-style-type: none"> <li>• <i>computer name\user name</i></li> <li>• <i>computer name\group name</i></li> </ul> If you do not know the complete account information, then you must look it up using Windows Computer Management.
domain users or groups to the SiteProtector system user group	type the complete account name using the following syntax, and then click <b>OK</b> : <ul style="list-style-type: none"> <li>• <i>domain name\user name</i></li> <li>• <i>domain name\group name</i></li> </ul> If you do not know the complete account name, then you must look it up using Check Names.

5. Click **OK**.  
The Select Users and/or Groups window appears.
6. Select the member you want to add to the asset group, and then click **OK**.  
The member appears in the Users and/or Groups column. You can assign group-level permissions to this member.
7. Click **Save**.

### Granting group-level permissions

To grant group-level permissions to an user or group:

1. In the left pane, right-click the Site Group or another group, and then select **Properties**.  
The Group Properties tab appears.
2. Click the **Permissions** icon.  
The Group-level permissions management window appears.
3. In the Users and/or Groups column, select the user or group.
4. In the **Manage Security** section, select the circle that corresponds to the permission you want to grant.  
A black circle indicates that the permission is granted.
5. Click **Save**.
6. Close the **Properties** tab.

### Removing group-level permissions

To remove group-level permissions from a user or group:

1. In the left pane, right-click the *Site Group* or another *group*, and select **Properties**.  
The Group Properties tab appears.
2. Click the **Permissions** icon.  
The Group-level permissions management window appears.
3. In the **Users and/or Groups** column, select the user or group.
4. In the **Manage Security** section, clear the circle that corresponds to the permission you want to grant.  
A white circle indicates that the permission is removed.
5. Click **Save**.
6. Right-click the **Group Properties tab**, and then select **Close** from the pop-up menu.

## Working with Permission Inheritance

### Introduction

This topic defines permission inheritance and provides information about how permission inheritance works. It also provides instructions for the following tasks:

- turning on permissions inheritance
- turning off permission inheritance
- determining whether permissions are inherited
- editing inherited permissions
- removing inherited permissions

### Definition: permission inheritance

Permission inheritance occurs when a subgroup of assets inherits its permission settings from a group of assets above it in the hierarchy. For example, the asset group *Atlanta Servers* contains a subgroup of assets called *Accounting Servers*. Permission inheritance occurs when the subgroup called *Accounting Servers* inherits its permission settings from the group called *Atlanta Servers*.

Permission inheritance is a powerful permission management tool because it provides a quick means of setting permissions on subgroups of assets and eliminates the cumbersome and repetitive task of setting permissions on all subgroups.

### Example 1

You configure the permissions for a group of assets called *Atlanta Servers*. There are 40 subgroups in the *Atlanta Servers* group. With permission inheritance, you can pass the permission settings from the *Atlanta Servers* group to all 40 subgroups automatically. This approach is much quicker than configuring the permission settings on all 40 subgroups.

### Example 2

You provide a user named *jsmith* permission to scan the assets in a group called *Atlanta Servers*. You then create a subgroup in the *Atlanta Servers* called *Accounting Servers* and turn on permission inheritance for this subgroup. The user named *jsmith* can run scans on the assets in the *Accounting Servers* subgroup. This approach provides an easy way to pass the permissions for *jsmith* from one asset group to another.

### Default setting

By default, the SiteProtector system enables the permission inheritance option for all groups and subgroups.

Disable this option if you want to prevent a group from inheriting permission settings from its parent group. When you turn off permission inheritance for a group, the SiteProtector system provides you with the opportunity to either copy the permission settings from the parent group into the subgroup or clear the permission settings from the group.

### Permission inheritance

If you turn off permission inheritance, it affects all the subgroups in the group. When you do this, the SiteProtector system provides you with an opportunity to copy permission settings from the parent group into the subgroup or clear the permission settings for the subgroup. If you copy the permission settings into the subgroup, then the SiteProtector system displays the permission indicator in black, which indicates that you can change or remove them.

## Turning off permission inheritance

To turn off permission inheritance for a group:

1. In the left pane, right-click select the group, and then select **Properties**.  
The Group Properties tab appears.
2. Click the **Permissions** icon.  
The Permissions Property window appears.
3. Click **Advanced**.  
The Advanced Properties window appears.
4. Uncheck the **Inherit from Parent Group** check box.
5. Choose one of the following:
  - Click **Copy** to copy the inherited permissions to the group before you turn off permission inheritance.
  - Click **Remove** to clear all permissions settings on the group before you turn off permission inheritance.
6. Click **OK**.  
The SiteProtector system either copies the inherited permissions to the group or clears them, and then turns off permission inheritance.
7. Click **Save**.
8. Right-click the **Group Properties** tab, and then select **Close** from the pop-up menu.

## Turning on permission inheritance

To turn on permission inheritance for a group:

1. In the left pane, right-click select the group, and then select **Properties**.  
The Group Properties tab appears.
2. Click the **Permissions** icon.  
The Permissions Property window appears.
3. Click **Advanced**.  
The Advanced Properties window appears.
4. Check the **Inherit from Parent Group** check box.
5. Click **OK**.
6. Click **Save**.
7. Right-click the **Group Properties** tab, and then select **Close** from the pop-up menu.

## Determining permission inheritance on Permissions Property

To determine permission inheritance on the Permissions Property window:

1. In the left pane, right-click the group, and then select **Properties** from the pop-up menu.
2. Click the **Permissions** icon.  
The Permissions Property window appears. If the circle indicators are grey, then the permissions are inherited. If they are any other color, then the permissions are not inherited.

**Determining permission inheritance on Advanced Properties**

To determine permissions inheritance on the Advanced Properties tab:

1. In the left pane, right-click the group, and then select **Properties** from the pop-up menu.
2. Click the **Permissions** icon.

The Permissions Property window appears.

3. Click **Advanced**.

The Advanced Properties window appears. The Permissions tab indicates whether the permissions are inherited. If the Inherit from Parent Group check box is selected, then the permissions are inherited. If not, then the permissions are not inherited.

**Editing and removing inherited permissions**

To edit an inherited permission:

1. Locate the group's parent group in the left pane.
2. Edit the group-level permissions on that asset group as needed.

See "Setting up Group-Level Permissions" on page 235.

**Remove an inherited permission at parent level**

To remove an inherited permission at the parent level:

1. Locate the group's parent group in the left pane.
2. Remove the permission at the parent group level.

**Remove an inherited permission at group level**

To remove an inherited permission at the group level:

1. Turn off permission inheritance.
2. Remove the permission from the group.

**Reference:** See "Setting up Group-Level Permissions" on page 235.



---

# Setting Permissions with Show Subgroups Enabled

**Introduction** This topic provides information about setting group-level permissions when you enable the Show Subgroups option.

**Showing subgroups** The Show Subgroups option was formerly called “Recursion.” This option, when enabled, allows you to view all of the assets and agents in all subgroups.

## Example

You turn on the option called Show Subgroups. In the left pane of the Console, you have a group called *Atlanta*. There are two subgroups in the Atlanta group:

- one group called *Servers*
- one group called *Routers*

You select the Atlanta group, and then select the Agent view. The Console shows you all of the agents in all three groups.

When you are setting group-level permissions with this option enabled, it can be difficult to determine where you are actually setting the permission. In the above example, you have a Network Sensor installed on an asset in the Servers group. The Console shows you the Network Sensor as part of the Atlanta group because Show Subgroups is enabled. You give a user permission to apply policies to the Network Sensor. You assign the permission at the Atlanta group even though the actual Network Sensor resides on an asset in the Servers group. The SiteProtector system sends this permission down to the group where the agent is installed.

These principles apply to all group-level permissions.



## Chapter 18

# Working with Components

## Overview

### Introduction

This chapter provides information about the following tasks:

- stopping, starting, and refreshing SiteProtector system components
- determining SiteProtector system component status
- viewing and editing SiteProtector system component properties
- resetting passwords for SiteProtector system components
- distributing required encryption keys manually to SiteProtector system components

**Note:** None of the tasks described in this chapter are required to initially set up the SiteProtector system. These tasks are designed for troubleshooting and maintenance purposes.

### In this chapter

This chapter contains the following topics:

Topic	Page
Stopping, Starting, and Refreshing Components	244
Resetting Component Passwords	246
Distributing Keys to SiteProtector System Components	250

# Stopping, Starting, and Refreshing Components

## Introduction

This topic provides instructions for the following tasks:

- stopping a component, which stops the issDaemon
- starting a component, which starts the issDaemon
- refreshing a component

**Note:** Components are referred to as “agents” in the SiteProtector system interface.

## Before you begin

Before you stop, start, or refresh a SiteProtector system component, view all command jobs in the Site to make sure there are no command jobs in progress for the component. If you stop, start, restart, or refresh a component while a command job is running, then you will interrupt and cancel the command job.

## Viewing all command jobs in the Site

To view all command jobs in a Site:

1. In the left pane, right-click the *Site Node*, and then select **Properties** from the pop-up menu.

The Properties tab for the Site appears.

2. Click the **Command Jobs** icon.

The right pane lists all the scheduled and running command jobs for all components and agents in the entire Site.

## Stopping components

To stop a component:

1. In the left pane, select the *Site Node*.
2. In the **Go to** list, select **Agent**.
3. In the right pane, right-click the component, and then select **Stop Agent** from the pop-up menu.

The Stop Agent command job window appears.

4. In the **Command Details** section, verify the action, asset, and agent name.
5. Click the **Schedule** icon.
6. Do you want to stop the agent immediately?
  - If *yes*, select **Run Once**.
  - If *no*, then schedule a job to stop the agent.
7. Click **OK**.

## Starting components

To start a component:

1. In the left pane, select the *Site Node*.
2. In the **Go to** list, select **Agent**.
3. In the right pane, right-click the component, and then select **Start Agent** from the pop-up menu.

The Start Agent command job window appears.

4. In the **Command Details** section, verify the action, asset, and agent name.
5. Click the **Schedule** icon.
6. Do you want to start the agent immediately?
  - If *yes*, select **Run Once**.
  - If *no*, then schedule a job to start the agent.
7. Click **OK**.

### Restarting components

To restart a component:

1. In the left pane, select the *Site Node*.
2. In the **Go to** list, select **Agent**.
3. In the right pane, right-click the component, and then select **Restart Agent** from the pop-up menu.

The Restart Agent command job window appears.
4. In the **Command Details** section, verify the action, asset, and agent name.
5. Click the **Schedule** icon.
6. Do you want to restart the agent immediately?
  - If *yes*, select **Run Once**.
  - If *no*, then schedule a job to restart the agent.
7. Click **OK**.

### Refreshing components

To refresh a component:

1. In the left pane, select the *Site Node*.
2. In the **Go to** list, select **Agent**.
3. In the right pane, right-click the component, and then select **Refresh Agent** from the pop-up menu.

The Refresh Agent command job window appears.
4. In the **Command Details** section, verify the action, asset, and agent name.
5. Click the **Schedule** icon.
6. Do you want to refresh the agent immediately?
  - If *yes*, select **Run Once**.
  - If *no*, then schedule a job to refresh the agent.
7. Click **OK**.

## Resetting Component Passwords

### Introduction

The SiteProtector system maintains a user account for each SiteProtector system component. The Site Database uses this account to identify the component, and the component uses the account to login to the Site Database. The user account includes the following details:

- a user name for the component based on the name of the computer where the component is installed

**Example:**

The user name for an Event Collector installed on a computer named ATL1000 is "EventCollector\_ATL1000."

- an encrypted system-generated password for the component  
You cannot access the system-generated password. You can reset component passwords with the password maintenance utilities.

This topic provides information about resetting the password for the following components:

- Event Collectors
- Agent Managers
- SecurityFusion module
- Application Server

### When do I reset the password?

In some situations, you must reset the password for the components as in the following examples:

- You want to change the system-generated password to one that you know.
- You must change the passwords for security management purposes.
- You are preparing the SiteProtector system for failover.

### Component password maintenance utilities

Table 75 describes the password maintenance utilities for SiteProtector system components.

Utility	Description
Event Collector Login Utility	Use this utility to reset the password for the Event Collector.
Agent Manager Login Information Utility	Use this utility to reset the password for the Agent Manager.
SecurityFusion module Database Password Changing Utility	Use this utility to reset the password for the SecurityFusion module.

**Table 75:** Password maintenance utilities for SiteProtector system components

**Resetting Event Collector passwords**

To reset the Event Collector password:

1. On the Event Collector computer, stop the issDaemon service.
2. Start the Event Collector login utility.

The utility is located in the following directory:

```
\Program Files\ISS\SiteProtector\Event Collector\ECLogin.exe
```

The SiteProtector Event Collector Login Utility window appears. The Login text box shows the user name for the Event Collector.

3. Type the new password in the **Password** box.
4. Type the new password again in the **Confirm** box.
5. Click **Save**.
6. On the primary Site Database computer, select **Start**→**Programs**→**Microsoft SQL Server**→**Enterprise Manager**.  
The SQL Server Enterprise Manager window appears.
7. Select **Microsoft SQL Servers** → **SQL Server Group**→**(local) (Windows NT)**→**Security**→**Logins**.
8. In the right pane, right-click the **Event Collector name**, and then select **Properties**.
9. In the **Password** box, type the new password for the Event Collector.
10. On the **General** tab, click **OK**.  
The Confirm Password window appears.
11. In the **Confirm new password** box, retype the password for the Event Collector, and then click **OK**.  
SQL Server Enterprise Manager resets the password.
12. Restart the issDaemon service on the Event Collector.

**Resetting Agent Manager passwords**

To reset the Agent Manager password:

1. On the Agent Manager computer, stop the issDaemon service.
2. Start the Agent Manager Login Information Utility located in the following directory:

```
\Program Files\ISS\SiteProtector\Agent Manager\AMLogin.exe
```

The Agent Manager was formerly called Desktop Controller. If you installed the utility before the name change, then the path name to the utility is as follows:

```
\Program Files\ISS\RealSecure SiteProtector\Desktop Controller\
```

3. Select the **Update database login** check box.
4. Type the new password in the **Password** box.
5. Type the new password again in the **Confirm** box.
6. Click **Save**.
7. On the primary Site Database computer, select **Start**→**Programs**→**Microsoft SQL Server**→**Enterprise Manager**.  
The SQL Server Enterprise Manager window appears.
8. Select **Microsoft SQL Servers**→**SQL Server Group**→**(local) (Windows NT)**→**Security**→**Logins**.

9. In the right pane, right-click the **Agent Manager name**, and then select **Properties**.
10. Type the new password for the Agent Manager in the **Password** box.
11. On the **General** tab, click **OK**.  
The Confirm Password window appears.
12. In the **Confirm new password** box, retype the password, and then click **OK**.  
SQL Server Enterprise Manager resets the password.
13. On the Agent Manager computer, restart the issDaemon service.

### Resetting SecurityFusion module passwords

To reset the SecurityFusion module password:

1. On the SecurityFusion module computer, stop the issDaemon service.
2. Start the SecurityFusion module Database Password Changing Utility in the following directory:  
`\SiteProtector\SecurityFusionModule\ChangeFusionPassword.exe`  
The SecurityFusion module Database Password Changing Utility window appears.
3. Type the new password for SecurityFusion module in the **New Password** box.
4. Type the new password again in the **Re-enter new password** box.
5. Click **OK**.
6. On the primary Site Database computer, select **Start** → **Programs** → **Microsoft SQL Server** → **Enterprise Manager**.  
The SQL Server Enterprise Manager window appears.
7. Select **Microsoft SQL Servers** → **SQL Server Group** → **(local) (Windows NT)** → **Security** → **Logins**.
8. In the right pane, right-click the **SecurityFusion module name**, and then select **Properties**.
9. In the **Password** box, type the new password for the Event Collector.
10. On the **General** tab, click **OK**.  
The Confirm Password window appears.
11. In the **Confirm new password** box, retype the password for the Event Collector, and then click **OK**.  
SQL Server Enterprise Manager resets the password.
12. On the SecurityFusion module computer, restart the issDaemon service.

### Resetting Application Server passwords

To reset the Application Server password:

1. Click **Start** on the taskbar, and then select **Settings** → **Control Panel** → **Administrative tools** → **Services**.  
The Component Services window appears.
2. Right-click **SiteProtector Application Service**, and then click **Stop** on the pop-up menu.
3. Right-click **SiteProtector Sensor Controller Service**, and then click **Stop** on the pop-up menu.



4. Click **Start** on the taskbar, and then select **Programs**→**Accessories**→**Command Prompt**.  
The Command Prompt window appears.
5. Change to the bin directory where the Application Server is installed.  
For example, if the Application Server is installed in the default location, you should type the following, and then press ENTER:  

```
cd "\Program Files\ISS\SiteProtector\Application Server\bin"
```
6. At the command prompt, type the following command:  

```
ccengine.bat -encrypt <your new password>
```
7. Click **Start** on the taskbar, and then select **Settings**→**Control Panel**→**Administrative tools**→**Services**.  
The Component Services window appears.
8. Right-click **SiteProtector Application Service**, and then select **Start** from the pop-up menu.
9. Right-click **SiteProtector Sensor Controller Service**, and then select **Start** from the pop-up menu.
10. Change the ISSapp user password in the Site Database.

# Distributing Keys to SiteProtector System Components

## Introduction

This topic explains how to distribute the required encryption keys manually to the following components:

- Agent Manager
- Deployment Manager
- Event Collector
- SecurityFusion module
- Third Party Module

The topic also explains how to apply Event Collector keys to a component. You can use this procedure in cases where you must replace existing keys on a component.

## Background

The SiteProtector system uses public-key encryption to securely communicate with other SiteProtector system components. Before the components can communicate with a Site, the components must have copies of the public keys for that Site. The required keys are automatically distributed to the components when you install the component with Deployment Manager.

## When do I manually distribute keys?

In some cases, you must manually distribute the required keys to the components. The following are examples of when you might need to distribute the required encryption keys manually to components:

- You install the component from a separate installation package.
- You install the component before you install the SiteProtector system.
- The key is not present on the component computer for any reason.
- For the Application Server keys, the date of the key on the component computer does not match the date of the key on the Application Server.
- For the Event Collector keys, the date of the key on the component computer does not match the date of the key on the Event Collector.

## Required keys

### Application Server (Sensor Controller) Keys

- `\Program Files\ISS\SiteProtector\Application Server\Keys\RSA\sp_con_computer_name_1024.PubKey`
- `\Program Files\ISS\SiteProtector\Application Server\Keys\RSA\sp_con_computer_name_1536.PubKey`

### Event Collector Keys

- `\Program Files\ISS\SiteProtector\Event Collector\Keys\RSA\rs_eng_computer_name_1024.PubKey`
- `\Program Files\ISS\SiteProtector\Event Collector\Keys\RSA\rs_eng_computer_name_1536.PubKey`

**Distribution methods**

The methods for distributing the required encryption keys to SiteProtector system components are as follows:

- Copy the required keys to the correct directories on the computers where the components are installed.
- Edit the crypt.policy file to allow the component to receive the required keys automatically from the Site the next time it connects to the Site.
- Use the Public Configuration Tool.  
See “Using the Public Key Configuration Tool” on page 285.

**Copying keys to components**

To distribute the RSA keys on the Application Server and Event Collector to SiteProtector system components.

Copy...	To the...
the following key subdirectories on the Application Server and Event Collector: <ul style="list-style-type: none"> <li>● \Program Files\ISS\SiteProtector\Application Server\Keys\RSA</li> <li>● \Program Files\ISS\SiteProtector\Event Collector\Keys\RSA</li> </ul>	<b>Agent Manager:</b> \Program Files\ISS\SiteProtector\Agent Manager\Keys
	<b>Deployment Manager:</b> \Program Files\ISS\SiteProtector\Deployment Manager\Keys
	<b>Event Collector:</b> Program Files\ISS\SiteProtector\Event Collector\Keys
	<b>SecurityFusion module:</b> \Program Files\ISS\SiteProtector\SecurityFusionModule\Keys\ <b>Note:</b> Copy the RSA keys to the SecurityFusion module.
	<b>Third Party Module (CheckPoint):</b> \Program Files\ISS\issSensors\ThirdPartyModule_CheckPoint_1\Keys\
	<b>Third Party Module (Cisco):</b> \Program Files\ISS\issSensors\ThirdPartyModule_Cisco_1\Keys\

**Editing the crypt.policy file**

To reset the component’s Allow First Connection setting manually and allow the SiteProtector system to send the required encryption keys to the component:

1. Locate, and then delete the following folders on the component:
  - \Program Files\ISS\issSensors\<sensor\_name>\Keys\CerticomNRA
  - \Program Files\ISS\issSensors\<sensor\_name>\Keys\RSA
 This action removes all encryption keys from the component computer.
2. From a command prompt, type net stop issdaemon.
3. Edit the crypt.policy file located in the following directory:
  - \Program Files\ISS\issDaemon\crypt.policy

4. In the crypt.policy file, change the 0 to a 1 in the following string:  
 String before edit: "allowfirstconnection<tab> =L<tab>0;"  
 String after edit: "allowfirstconnection<tab> =L<tab>1;"
5. Save the file.
6. From a command prompt, type net start issdaemon.
7. From the SiteProtector Console, start the component.  
 The component attempts to connect to the SiteProtector system. This change should allow the component to connect to the Site and receive the required encryption keys.
8. Verify that the required keys are stored on the component computer. See Key Location below.

**Key locations**

The specific directory where the SiteProtector system components store encryption keys varies depending on the component. Table 76 lists the directories where the SiteProtector system components store encryption keys.

Component	Example Directory
Any SiteProtector system component	\Program Files\ISS\SiteProtector\ComponentName\Keys
Agent Manager	\Program Files\ISS\SiteProtector\Agent Manager\Keys
Deployment Manager	\Program Files\ISS\SiteProtector\Deployment Manager\Keys
Event Collector	\Program Files\ISS\SiteProtector\Event Collector\Keys
SecurityFusion module	\Program Files\ISS\SiteProtector\SecurityFusionModule\Keys
Third Party Module (for Check Point)	\Program Files\ISS\issSensors\ThirdPartyModule_CheckPoint_1\Keys
Third Party Module (for Cisco)	\Program Files\ISS\issSensors\ThirdPartyModule_Cisco_1\Keys

**Table 76:** Directories where components store encryption keys

**Applying keys to an component**

To apply the Event Collector keys to a component:

1. In the left pane, select the Site Node.
2. In the **Go to** list, select **Agent**.
3. In the right pane, stop the Event Collector, and then wait until the Event Collector status changes to *Stopped*.
4. In the right pane, right-click the component, and then select **Properties** from the pop-up menu.
5. Click **None** in the **Event Collector** box, and then click **OK**.
6. Start the Event Collector, and then wait until the Event Collector status is *Active*.
7. Right-click the component, and then select **Properties** from the pop-up menu.
8. Click **Edit Agent Properties**.

9. Change the **Event Collector** box from **None** to the appropriate Event Collector, and then click **OK**.

The component status changes to “Active.”

**Tip:** Review the key directories on the component computer to verify that the keys are present and in the correct location.



## Setting Up Agents





## Chapter 19

# The Agent Setup Stage

## Overview

### Introduction

The third stage in the SiteProtector system setup process is the Agent Setup stage. In this stage, you install and configure other IBM ISS products to work with the SiteProtector system. After they are set up, these products become agents in the SiteProtector system, and you can manage them in the Console and view security events generated by them.

**Note:** You can add additional IBM ISS products to your environment at any time after the initial setup. You can use the process and procedures described in this chapter to implement the products.

**Note:** For information about using agent builds to install Proventia Desktop (version 10.0 and later) and Proventia Server IPS for Windows (version 2.0 and later), see the *Administrator Guide for Proventia Server for Windows* at <http://www.iss.net/support/documentation/>.

### In this chapter

This chapter contains the following topics:

Topic	Page
Overview of this Stage	258
Appliance Setup Checklists	261
Scanner Setup Checklists	262
Network Sensor and Server Sensor Setup Checklists	264

## Overview of this Stage

<b>Introduction</b>	This topic provides an overview of the Agent Setup stage.
<b>Licenses</b>	Before you can use other IBM ISS products with the SiteProtector system, you must ensure that you have the required licenses for this purpose. You must set up the licenses in the SiteProtector system before the products can work together properly.
<b>Installation and configuration</b>	<p>The SiteProtector system provides two methods for installing other IBM ISS products:</p> <ul style="list-style-type: none"><li>● Use the Deployment Manager to install all IBM ISS products, except for appliances and Desktop Protection agents.</li><li>● Use the Agent Manager method, Agent Builds, to install Desktop Protection agents and Proventia Server IPS for Windows.</li></ul> <p>IBM ISS strongly recommends that you install the SiteProtector system first, and then use these methods to install your products. These methods eliminate many manual tasks such as registering the product with the SiteProtector system and distributing required encryption keys.</p>
<b>Product registration</b>	Regardless of the method you choose to install your IBM ISS products, the products must be registered with the SiteProtector system before you can manage them in the SiteProtector Console. If you choose to install your other IBM ISS products before you install the SiteProtector system or if you choose to install the products using other methods, then you will have to register the products with the SiteProtector system manually.
<b>Grouping</b>	<p>The SiteProtector system uses groups to organize your IBM ISS products. Groups provides a method of organizing the products into manageable units and performing tasks on related products.</p> <p>IBM ISS strongly recommends that you install the SiteProtector system and set up groups for your IBM ISS products before you install the products themselves. After you install the products, the SiteProtector system can automatically group the products into the groups you have already set up based on the IP address where the agent is installed. For appliance agents and for Proventia Server IPS for Linux, the group for the agent is added to the SiteProtector system when the agent sends its first heartbeat to the SiteProtector system.</p>
<b>Key distribution</b>	<p>The SiteProtector system cannot communicate with other IBM ISS products unless the two products exchange the required encryption keys.</p> <p>IBM ISS strongly recommends that you install the SiteProtector system first and then use the Deployment Manager and Agent Builds to install your other products. These tools automatically exchange the encryption keys required for secure communication between the products. If you choose to install the products before you install the SiteProtector system or if you use alternative installation methods, then you must manually distribute the required encryption keys.</p>
<b>Policy configuration</b>	Policy configuration and management for IBM ISS products is a complex tasks. This guide provides basic information about how to apply a policy to the products. For detailed

information about policies for the various IBM ISS products, go to one of the following sources:

- the product documentation for the product
- the SiteProtector system help regarding policies

## Updates

IBM ISS regularly releases updates for its products, including updates that affect the performance of the product and the security content in the product. IBM ISS strongly recommends that you keep your products with the latest service packs and updates.

## Agent setup process

The exact process for setting up other IBM ISS products to work with the SiteProtector system varies depending on the product. Table 77 describes the general process for setting up other IBM ISS products.

Stage	Description
1	<p>Licenses:</p> <p>You must set up a license for the product in the SiteProtector system, which allows you to manage and update the product with the SiteProtector system.</p>
2	<p>Installation and Configuration:</p> <p>You must install and configure the product.</p> <ul style="list-style-type: none"> <li>• For Desktop Protection agents and for Proventia Server IPS for Windows agents, you can configure the product completely in the SiteProtector system and deploy it to your organization using Agent Builds.</li> <li>• For most appliances, you must install and configure the appliance using Proventia Manager on the appliance before you can integrate it with the SiteProtector system.</li> <li>• For other products, you can install the product using Deployment Manager, and then configure the product.</li> </ul>
3	<p>Registration, Grouping, and Key Distribution:</p> <p>You must register the product with the SiteProtector system, group the product into the correct asset group, and distribute the SiteProtector system's encryption keys or certificate to the product for secure communication.</p> <ul style="list-style-type: none"> <li>• For products that can be installed with Deployment Manager, such as Network Internet Scanner and Network Sensor, these tasks occur automatically when you set up your groups in advance and provide the required information during the Deployment Manager-based installation process.</li> <li>• For Desktop Protection agents and for Proventia Server IPS for Windows agents, these tasks are eliminated when you configure the product in the SiteProtector system and install it using an Agent Build.</li> <li>• For most appliances, you have to manually set user-defined options, using Proventia Manager on the appliance, so that it can connect to the SiteProtector system and perform these tasks.</li> </ul>

**Table 77:** *Process for setting up other IBM ISS products*

Stage	Description
4	<p>Policies and Responses:</p> <p>You must define policies to control how the products handle and respond to security events. For more information on Policies and Responses, see the <i>SiteProtector Policies and Responses Configuration Guide</i>.</p> <ul style="list-style-type: none"> <li>• For most products, including Desktop Protection agents, Network Internet Scanner, and Network Sensor, you can set all policies for the product in the SiteProtector system and automatically distribute them to the products.</li> <li>• For appliances, you can set only some policies for the product in the SiteProtector system and set others in the product itself.</li> </ul>
5	<p>Updates:</p> <p>You must keep the products current with the latest software releases and security updates from IBM ISS.</p> <ul style="list-style-type: none"> <li>• For appliances, you update the firmware on the appliance itself, but you can update the security content from the SiteProtector system.</li> <li>• For all other products, you can update the products with the SiteProtector system.</li> </ul>

**Table 77:** *Process for setting up other IBM ISS products (Continued)*

## Appliance Setup Checklists

### Introduction

This topic provides task checklists to ensure that you perform all the tasks required to set up the following appliances:

- Proventia Network MFS
- Proventia Network IPS

### Proventia Network MFS checklist

Table 78 provides a checklist of the tasks required to set up the Proventia Network MFS.

✓	Task
<input type="checkbox"/>	Create an Agent Manager account for the appliance. See “Creating Agent Manager Accounts” on page 69.
<input type="checkbox"/>	Create a group for the appliance, and then define the group settings. See “Creating Groups” on page 225.
<input type="checkbox"/>	Configure custom policies for the appliance. <b>Note:</b> You cannot configure all policies for the Proventia Network MFS in the SiteProtector system. You must configure some policies in the Proventia Manager. See the <i>Proventia Network Multi-Function Security Appliances User Guide</i> .
<input type="checkbox"/>	Install and configure the appliance, and then configure SiteProtector system management settings on the appliance. See the <i>Proventia Network Multi-Function Security Appliances User Guide</i> .
<input type="checkbox"/>	Update the appliance. See the <i>Proventia Network Multi-Function Security Appliances User Guide</i> .

**Table 78:** Checklist for setting up Proventia Network MFS

### Proventia Network IPS checklist

Table 79 provides a checklist of the tasks required to set up the Proventia Network IPS.

✓	Task
<input type="checkbox"/>	Create an Agent Manager account for the appliance. See “Creating Agent Manager Accounts” on page 69.
<input type="checkbox"/>	Create a group for the appliance, and then define the group settings. See “Creating Groups” on page 225.
<input type="checkbox"/>	Configure custom policies for the appliance. <b>Note:</b> You configure all policies for the Proventia Network IPS in the SiteProtector system or in Proventia Manager. See the <i>Proventia Network Intrusion Prevention System User Guide</i> .
<input type="checkbox"/>	Install and configure the appliance, and then configure SiteProtector system management settings on the appliance. See the <i>Proventia Network Intrusion Prevention System User Guide</i> .
<input type="checkbox"/>	Update the appliance. See the <i>Proventia Network Intrusion Prevention System User Guide</i> .

**Table 79:** Checklist for setting up Proventia Network IPS

## Scanner Setup Checklists

### Introduction

This topic provides task checklists to ensure that you perform all the tasks required to set up the following scanners:

- Network Internet Scanner
- System Scanner Databridge

**Note:** The databridge is required to view security events in the SiteProtector system that are generated by System Scanner vulnerability assessment application. You cannot manage System Scanner vulnerability assessment application in the SiteProtector system. You can only view System Scanner vulnerability assessment application-generated events.

### Network Internet Scanner

Table 80 provides a checklist of the tasks required to set up Network Internet Scanner.

✓	Task
<input type="checkbox"/>	Add a license to the SiteProtector system for the scanner. See “Setting Up Licenses” on page 49.
<input type="checkbox"/>	Create a group for the scanner, and then define the group settings. See “Creating Groups” on page 225.
<input type="checkbox"/>	Install the scanner with Deployment Manager. See the following for additional information: <ul style="list-style-type: none"> <li>● “Installing Agents with the Deployment Manager” on page 269</li> <li>● <i>Network Internet Scanner Installation Guide</i></li> </ul>
<input type="checkbox"/>	Update the scanner. See “Updating Agents” on page 289..

**Table 80:** Checklist for setting up Network Internet Scanner

### System Scanner Databridge

Table 81 provides a checklist of the tasks required to set up System Scanner Databridge.

✓	Task
<input type="checkbox"/>	Install System Scanner vulnerability assessment application, including the System Scanner Console and System Scanner Agent. See the <i>System Scanner Installation Guide</i> .
<input type="checkbox"/>	Add a license to the SiteProtector system for System Scanner vulnerability assessment application. See “Setting Up Licenses” on page 49.
<input type="checkbox"/>	Create a group for the databridge, and then define the group settings. See “Creating System Scanner Vulnerability Assessment Application Groups” on page 228.
<input type="checkbox"/>	Install the databridge with Deployment Manager. See “Installing Agents with the Deployment Manager” on page 269.

**Table 81:** Checklist for setting up System Scanner Databridge

✓	Task
<input type="checkbox"/>	Update the databridge. See “Updating Agents” on page 289.

**Table 81:** *Checklist for setting up System Scanner Databridge*

## Network Sensor and Server Sensor Setup Checklists

### Introduction

This topic provides task checklists to ensure that you perform all the tasks required to set up the following sensors:

- Network Sensor
- Server Sensor

### Network Sensor

Table 82 provides a checklist of the tasks required to set up Network Sensor 6.5 and 7.0.

✓	Task
<input type="checkbox"/>	Add a license to the SiteProtector system for the sensor. See “Setting Up Licenses” on page 49.
<input type="checkbox"/>	Create a group for the sensor. See “Creating Groups” on page 225.
<input type="checkbox"/>	Install the sensor with Deployment Manager. See “Installing Agents with the Deployment Manager” on page 269.
<input type="checkbox"/>	Configure custom policies for the sensor, and then apply them to the sensor. See the <i>SiteProtector Policies and Responses Configuration Guide</i> .
<input type="checkbox"/>	Update the sensor. See “Updating Agents” on page 289.

**Table 82:** Checklist for setting up Network Sensor

### Server Sensor

Table 83 provides a checklist of the tasks required to set up Server Sensor 6.5 and 7.0.

✓	Task
<input type="checkbox"/>	Add a license to the SiteProtector system for the sensor. See “Setting Up Licenses” on page 49.
<input type="checkbox"/>	Create a group for the sensor. See “Creating Groups” on page 225.
<input type="checkbox"/>	Install the sensor with Deployment Manager. See “Installing Agents with the Deployment Manager” on page 269.
<input type="checkbox"/>	Configure custom policies for the sensor, and then apply them to the sensor. See the <i>SiteProtector Policies and Responses Configuration Guide</i> .
<input type="checkbox"/>	Update the sensor. See “Updating Agents” on page 289.

**Table 83:** Checklist for setting up Server Sensor



## Chapter 20

# Setting Up Agents

## Overview

### Introduction

This chapter explains the procedures for setting up other IBM ISS products (agents) to work with SiteProtector, including the following:

- Appliances
- Network Sensor
- Scanners
- Databridges

**Note:** For information about using agent builds to install Proventia Desktop (version 10.0 and later) and Proventia Server IPS for Windows (version 2.0 and later), see the *Administrator Guide for Proventia Server for Windows* at <http://www.iss.net/support/documentation/>.

### Before you begin

Before you set up agents, you should set up groups for assets and agents. See “Setting Up Groups” on page 215.

### Requirement

SiteProtector is not preconfigured to work with any other IBM ISS products. If you want to manage your IBM ISS products with SiteProtector, then you must follow the procedures in this chapter to set up the products.

### Related documentation

For complete documentation for any of the products discussed in this chapter, go to the IBM ISS Product Documentation Web site at <http://www.iss.net/support/documentation/>.

### In this chapter

This chapter contains the following sections:

Section	Page
Section A, "Installing Agents"	267
Section B, "Registering Agents"	273
Section C, "Distributing Keys and Certificates"	281
Section D, "Updating Agents"	287



# SECTION A: Installing Agents

## Overview

### Introduction

This section provides important information about the following tasks:

- installing other IBM ISS products with Deployment Manager, which automatically registers the products with SiteProtector and distributes the required encryption keys to the products
- installing other IBM ISS products with separate installation programs

### In this section

This section contains the following topics:

Topic	Page
Installation Methods	268
Installing Agents with the Deployment Manager	269
Adding Installation Packages to the Deployment Manager	271
Installing Agents with Separate Installation Packages	272

## Installation Methods

### Introduction

This topic explains the various methods for installing IBM ISS products.

### Methods

IBM ISS provides several methods for installing IBM ISS products:

- using the Deployment Manager
- using an agent build (for Proventia Desktop Protection agents and Proventia Server IPS for Windows)
- using the a separate installation program

### Deployment Manager

IBM ISS strongly recommends that you use Deployment Manager to install all IBM ISS products after you install and configure SiteProtector. This approach performs the following setup tasks for you automatically:

- registers the product with SiteProtector when you specify a Site name during product installation, and puts the product in the correct group based on the group membership rules you defined when you configured SiteProtector

**Note:** If you use Deployment Manager to install products *before* you install and configure SiteProtector, then you will not be able to automatically register the product the Site or distribute the required encryption keys to the product.

- adds the Application Server as a key administrator on the computer where the product is installed, and distributes encryption keys to the product for secure communication between the product and SiteProtector
- assigns an Event Collector to the agent if applicable
- assigns an Agent Manager to the agent if applicable
- sets options for distributing certificates required for secure communication between the product and SiteProtector

**Important:** You cannot use Deployment Manager to install the software required for the appliances. For information on installing and configuring appliances, see the installation guides for the appliances

### Separate installation packages

IBM ISS does not recommend you use separate installation packages to install products. If you use a separate installation package to install the products, then you must manually register the products with SiteProtector and distribute the required encryption keys to the products manually.

# Installing Agents with the Deployment Manager

**Introduction** This topic explains how to install other IBM ISS products with the Deployment Manager.

**Tasks performed** In addition to installing an IBM ISS product, the Deployment Manager can perform the following tasks:

- Register the product with a Site.  
To use this feature, you must specify the *Site Group* name during the installation. After the product is installed, it will appear in the *Site Group* you specified.
- Configure the product to receive the required encryption keys from the Site when it first connects to the Site.  
To use this feature, you must enable the Auto-Import option during the installation.

**Before you begin** Before you install any product with Deployment Manager, you must complete the tasks described in Table 84.

Task	Description
1	Install and configure SiteProtector, including setting up groups for the products you are installing. <b>Reference:</b> See “The Configuration and Update Stage” on page 25.
2	Obtain the Site Group name from the Site where you want to register the agent. The Site Group name is user-defined at the time you install SiteProtector. <b>Reference:</b> See “Default Group Names” on page 219.
3	Obtain the IP address of the computer where the Site Application Server is installed.
4	Verify that the installation packages for the products you want to install are available in the Deployment Manager. If not, then download them. <b>Reference:</b> See “Adding Installation Packages to the Deployment Manager” on page 271.
5	Verify that the Deployment Manager is registered with the Site where you want to register the products. If you are not sure whether the Deployment Manager is registered with the Site, then connect a Console to the Site and ensure that the Deployment Manager is listed as a registered agent in the Site. If not, then register the Deployment Manager with the Site. <b>Reference:</b> See “Registering Agents” on page 273.
6	Verify that the computer where you are installing the product meets the system requirements. <b>Reference:</b> Go to <a href="http://www.iss.net/support/documentation">www.iss.net/support/documentation</a> .
7	Obtain and read the installation documentation for the product you are installing. This documentation provides important requirements and considerations for installing the individual products that might not be covered in the SiteProtector documentation. IBM ISS strongly recommends that you review this information before you install the product. <b>Reference:</b> Go to <a href="http://www.iss.net/support/documentation">www.iss.net/support/documentation</a> .

**Table 84:** Before you install other IBM ISS products

**Procedure**

To install a product with Deployment Manager:

1. On the computer where you want to install the product, open Internet Explorer, and then type the following address:  
`https://ip_address_or_server_name:3994/deploymentmanager`  
The Deployment Manager Main Menu appears.
2. Select **Install Agents**, and then select the product (agent) you want to install.
3. Select the version to install from the list, and then click **Next**.
4. Click **Install**.
5. Follow the on-screen instructions and provide the required information.
6. If you want Deployment Manager to automatically register the product with a Site and distribute the required encryption keys to the product, then you must do the following during the installation:
  - specify the Site Group name
  - enable the Auto-Import feature

---

# Adding Installation Packages to the Deployment Manager

## Introduction

The Deployment Manager can only install products if the installation package for that product exists in the Deployment Manager. When you install the Deployment Manager, the installation program asks you to select all the products that you will be installing with the Deployment Manager. The installation program then installs the required installation packages for the products that you selected along with Deployment Manager. In some cases, the required installation packages are not available to the Deployment Manager. In these cases, you can manually add the necessary installation packages to the Deployment Manager. This topic explains how to manually add installation packages to the Deployment Manager.

## Procedure

To download the latest installation packages and make them available in the Deployment Manager:

1. On the computer where the Deployment Manager is installed, access the IBM ISS Download Center at [www.iss.net/download/](http://www.iss.net/download/).
2. Find the download page for the specific product.
3. Download the installation package to the appropriate Deployment Manager folder:

```
\Program Files\ISS\RealSecure SiteProtector\Application  
Server\webapps\dmdocroot\packages\product_name
```

4. Stop the Application Server service, and then restart the service.

The installation package for the agent is available for installation from the Deployment Manager.

## Installing Agents with Separate Installation Packages

- Introduction** This topic describes the advantages and disadvantages of using separate installation packages to install IBM ISS products.
- Disadvantages** If you install IBM ISS products with a separate installation package, then you will not be able to do the following automatically:
- register the product with SiteProtector
  - place the product in the correct group
- Advantages** If you install IBM ISS products with a separate installation package, then you will be able to do the following:
- Designate the Application Server as the Key Administrator for the agent you are installing; this task is part of the installation process for most agents, but you must provide the name of the Application Server, unless you are installing the agent on the Application Server.
  - Turn on Auto Import / Allow First Connection, which allow SiteProtector to automatically send its authentication keys to the agent the first time it connects.



## SECTION B: Registering Agents

### Overview

#### Introduction

- use the New Agent Wizard to automatically register agents with a Site
- use the New Agent Wizard to manually register agents with a Site
- unregister agents from a Site

The information in this section only applies to agents that communicate with SiteProtector through the Event Collector. Agents that communicate with SiteProtector through the Agent Manager self-register when they initiate communication with the Site.

#### SiteProtector components

SiteProtector components should be installed with Deployment Manager except in very rare cases. SiteProtector components self-register with the Site when you install them with a registered Deployment Manager. If you must unregister and then reregister a SiteProtector component because of problems such as communication issues between the component and SiteProtector, then you can use the New Agent Wizard to register the SiteProtector component with the Site.

**Reference:** See “Installing Agents with the Deployment Manager” on page 269.

#### In this section

This section contains the following topics:

Topic	Page
New Agent Wizard	274
Automatically Registering Agents	276
Manually Registering Agents with the Site	278

## New Agent Wizard

### Introduction

You can run the New Agent Wizard to register the following agents and SiteProtector components with a Site:

#### Agents:

- System Scanner Databridge vulnerability assessment application
- Internet Scanner
- Network Sensor
- Proventia Network IPS (G series appliances)
- Server Sensor

#### SiteProtector Components:

- Deployment Manager
- Event Collector
- SecurityFusion module
- Third Party Module

### When to use the Wizard

In most cases, agents self-register when they are installed. The agent installation program asks you to provide the name of the Site where you want to register the agent, and then automatically registers the agent with that Site. In rare situations, you must use the Wizard to register an agent with the Site. Such situations are as follows:

- You install the agent from a separate installation package.
- You install the agent before you install SiteProtector.
- You install the agent with a Deployment Manager that is not registered with the Site.
- You install the agent with the Deployment Manager and do not specify the Site where you want to register the agent.

**Automatic and manual registration**

Table 85 describes the registration options available in the New Agent Wizard.

Option	Description
Automatically Register Agent	<p>Select this option if you want the Wizard to do the following:</p> <ul style="list-style-type: none"> <li>• query the host to identify all agents on the host</li> <li>• register all the agents with the Site</li> <li>• validate the registration information for the agent</li> </ul> <p><b>Important:</b> IBM ISS strongly recommends you select this option to avoid problems with registration information.</p>
Manually Register Agent	<p>Select this option if you have all the information required to register the agent, include host name, agent name, and agent type.</p> <p>When you select the Manual Registration option, the New Agent Wizard does not validate the registration information provided about the agent. For example, if you provide an incorrect Agent Type, then the New Agent Wizard registers the agent with the Site under the incorrect Agent Type. To correct the problem, you must unregister the agent, and then re-register it with the correct type. To avoid these issues, select Automatic Registration.</p>

**Table 85:** *New Agent Wizard registration options*

**Required information**

You must provide the following information when you run the New Agent Wizard:

- asset name or asset IP address
- Event Collector name

If you do not specify an Event Collector when you register the agent, then you must assign an Event Collector to the agent later. See “Assigning Event Collectors Manually” on page 123.

- agent type
- agent name

## Automatically Registering Agents

### Introduction

This topic explains how to use the New Agent Wizard to automatically register agents with the Site.

### Description

If you choose the Automatically Register Agents option when you run the New Agent Wizard, then the system does the following automatically:

- queries the assets you specify and identifies all the agents that reside on the assets
- extracts the required registration information about the agents such as Agent Name and Agent Type
- registers the agents with the Site where you run the Wizard

**Note:** The system registers all agents that it identifies on the assets. For example, if the system finds a Network Internet Scanner and a Network Sensor on the asset, then it registers both agents with the Site. Also, in some cases, the system might register an agent more than once. This action has no negative impact on the system and does not create more than one entry for the agent. For example, if the system registers a Network Internet Scanner with the Site and the Network Internet Scanner is already registered with the Site, then this action does not create two entries for the Network Internet Scanner.

### Registering agents on a single asset

To automatically register the agents on a single asset with the Site:

1. In the left pane, right-click the group where you want to add the agent, and select **New→Agent**.

The New Agent Wizard appears.

2. Type the asset name or asset IP address, and then click **Add**.

The asset appears in the list. The Wizard registers any agent installed on this asset with the Site.

3. Click **Next**.

The Choose Event Collector window appears.

4. Select one of the following:

- the Event Collector you want the agents to report
- **None** (If you choose this option, then you must assign an Event Collector to the agents later. Otherwise, the agent will appear as Not Managed in the Console).

5. Select **Automatically Register Agents**, and then click **Next**.

The Wizard queries the asset you added for agents and registers any agents that it identifies with the Site. The Wizard also assigns the Event Collector you chose to the agents.

### Registering agents on multiple assets

To automatically register the agents on multiple assets with the Site:

1. In the left pane, right-click the group where you want to add the agent, and select **New→Agent**.

The New Agent Wizard appears.

2. Type the asset name or asset IP address, and then click **Add**.

The asset appears in the list.

3. Repeat Step 2 to add additional assets to the list.

The Wizard registers any agents installed on any of these assets with the Site.

4. Click **Next**.

The Choose Event Collector window appears.

5. Select one of the following:

- the Event Collector you want the agents to report
- **None** (If you choose this option, then you must assign an Event Collector to the agents later. Otherwise, the agent will appear as Not Managed in the Console).

6. Select **Automatically Register Agents**, and then click **Next**.

The Wizard queries the assets you added for agents and registers any agents that it identifies with the Site. The Wizard also assigns the Event Collector you chose to the agents.

## Manually Registering Agents with the Site

- Introduction** This topic explains how to use the New Agent Wizard to manually register agents with the Site.
- Description** If you choose the Manually Register Agent option when you run the New Agent Wizard, then you must provide the required registration information for the agent such as Agent Name and Agent Type.
- Recommendation** During a manual agent registration, the system does not validate the information you provide about the agent, and registers the agent with the Site regardless of whether the asset or agent exists at the time of registration. For example, if you select “Databridge” as the agent type when you manually register a Network Internet Scanner, then the system registers the Network Internet Scanner with the Site as a Databridge. For this reason, IBM ISS strongly recommends that you select the Automatically Register Agent option when you run the New Agent Wizard. If you provide inaccurate information during a manual agent registration, then you must unregister the agent and re-register it with the correct information. To avoid these issues, select the Automatically Register Agent option.
- Reference:** See “Automatically Registering Agents” on page 276.
- Reasons for manually registering agents** There are very few valid reasons for manually registering an agent. The most common reason is that you want to set up an asset or an agent before you actually install the agent on the asset. This task is possible because the Manual Registration feature does not validate the information you provide. For example, if you want to add EventCollector\_01 on asset 12.12.12.12, then you can perform this task even though the Event Collector or asset might not exist at the time of manual registration.
- Registering agents on a single asset** To manually register an agent:
1. In the left pane, right-click the group where you want to add the agent, and select **New → Agent**.  
The New Agent Wizard appears.
  2. Type the asset name or asset IP address, and then click **Add**.  
The asset appears in the list.
  3. Click **Next**.  
The Choose Event Collector window appears.
  4. Select one of the following:
    - the Event Collector you want the agents to report
    - **None** (If you choose this option, then you must assign an Event Collector to the agents later. Otherwise, the agent will appear as Not Managed in the Console).
  5. Select **Manually Register Agent**, and then click **Next**.  
The Register Agent window appears.

6. Select the following, and then click **Add**:

- Agent type
- Asset
- Agent name

The agent appears in the Register the Following Agent list.

**Tip:** To find all of the agents installed on a specific asset, select the asset, and then click **Query**.

7. Click **Next**.

The Wizard registers the agent with the information you provided. It does not validate the information.





## SECTION C: **Distributing Keys and Certificates**

### Overview

**Introduction** This section discussion how to distribute the required encryption keys manually to the following agents and how to use the public key configuration tool.

**In this section** This section contains the following topics:

<b>Topic</b>	<b>Page</b>
Manually Distributing Keys	282
Using the Public Key Configuration Tool	285

## Manually Distributing Keys

### Introduction

This topic explains how to distribute the required encryption keys manually to the following agents:

- Server Sensor
- Network Sensor
- Proventia Network IDS
- Proventia Network IPS

### Background

The Application Server and the Event Collector use public-key encryption to securely communicate with some managed agents. Before the agents can communicate with these SiteProtector components, the agents must have copies of the public keys for the components. The required keys are automatically distributed to the agents when you install the agent with a registered Deployment Manager.

### When do I manually distribute keys?

You must manually distribute the required keys to the agents in some cases. You might need to distribute the required encryption keys manually in the following situations:

- you install the product from a separate installation package
- you install the product before you install SiteProtector
- the key is not present on the agent computer for any reason
- for the Application Server keys, the date of the key on the agent computer does not match the date of the key on the Application Server
- for the Event Collector keys, the date of the key on the agent computer does not match the date of the key on the Event Collector

### Required keys

#### Application Server (Sensor Controller)

- `\Program Files\ISS\RealSecure SiteProtector\Application Server\Keys\RSA\sp_con_computer_name_1024.PubKey`
- `\Program Files\ISS\RealSecure SiteProtector\Application Server\Keys\RSA\sp_con_computer_name_1536.PubKey`

#### Event Collector

- `\Program Files\ISS\RealSecure SiteProtector\Event Collector\Keys\RSA\rs_eng_computer_name_1024.PubKey`
- `\Program Files\ISS\RealSecure SiteProtector\Event Collector\Keys\RSA\rs_eng_computer_name_1536.PubKey`

**Distribution methods**

The following are methods for distributing the required encryption keys to SiteProtector components:

- Copy the required keys to the correct directories on the computers where the components are installed.
- Edit the crypt.policy file to allow the component to receive the required keys automatically from the Site the next time it connects to the Site.
- Use the Public Configuration Tool.  
See "Using the Public Key Configuration Tool" on page 285.
- Use the File Transfer Protocol (FTP).  
This method is used to distribute keys to Solaris Network Sensors only.

**Distributing RSA keys**

To distribute the RSA keys on the Application Server and Event Collector to other agents.

Copy...	To the...
the following key subdirectories on the Application Server and Event Collector: <ul style="list-style-type: none"> <li>● \Program Files\ISS\RealSecure SiteProtector\Application Server\Keys\RSA</li> <li>● \Program Files\ISS\RealSecure SiteProtector\Event Collector\Keys\RSA</li> </ul>	Network Sensor: \Program Files\ISS\issSensors\network_sensor_1\Keys
	Server Sensor: \Program Files\ISS\issSensors\server_sensor_1\Keys
	Network Internet Scanner: Program Files\ISS\issSensors\Scanner_1\Keys
	System Scanner Databridge: \Program Files\ISS\issSensors\System_Scanner_Databridge\Keys\

**Resetting the Connection**

To reset the agent's Allow First Connection setting manually and allow SiteProtector to send the required encryption keys to the agent:

1. Locate, and then delete, the following folders on the agent:
  - \Program Files\ISS\RealSecure SiteProtector\Application Server\Keys\RSA
  - \Program Files\ISS\RealSecure SiteProtector\Event Collector\Keys\RSA

This action removes all encryption keys from the agent computer.

2. From a command prompt, type `net stop issdaemon`.
3. Edit the crypt.policy file located in the following directory:  
`\Program Files\ISS\issDaemon\crypt.policy`
4. In the crypt.policy file, change the 0 to a 1 in the following string:  
 String before edit: "allowfirstconnection<tab> =L<tab>0;"  
 String after edit: "allowfirstconnection<tab> =L<tab>1;"
5. Save the file.

6. From a command prompt, type `net start issdaemon`.
7. From the SiteProtector Console, start the agent.

The agent attempts to connect to SiteProtector. This change should allow the agent to connect to the Site and receive the required encryption keys.

8. Verify that the required keys are stored on the agent computer. See Key Location below.

### Key locations

The specific directory where agents store encryption keys varies depending on the agent and the operating system. Table 86 lists the directories where agents store encryption keys.

Agent	Directory
Any Windows agent	<code>\Program Files\ISS\IssSensors\AgentName\Keys</code>
Any Linux agent	<code>/opt/ISS/issSensors/AgentName/Keys</code>
Any Nokia agent	<code>/opt/ISS/AgentName/Keys</code> <code>/opt/ISS/issSensors/AgentName/Keys</code>
Network Sensor (Windows)	<code>\Program Files\ISS\issSensors\Network_Sensor_1\Keys</code>
Network Sensor (Linux)	<code>/opt/ISS/issSensors/network_sensor_1/Keys</code>
Network Sensor (UNIX)	<code>\opt\ISS\issSensors\agent_name\Keys\encryption_provider</code>
Server Sensor (Windows)	<code>\Program Files\ISS\issSensors\server_sensor_1\Keys</code>
Server Sensor (UNIX)	<code>\opt\ISS\issSensors\agent_name\Keys\encryption_provider</code>
System Scanner Databridge (Windows)	<code>\Program Files\ISS\issSensors\System_Scanner_Databridge\Keys</code>
Network Internet Scanner (Windows)	<code>\Program Files\ISS\issSensors\Scanner_1\Keys</code>
Proventia Network IDS	<code>/opt/ISS/issSensors/network_sensor_1/Keys</code>
Proventia Network IPS	<code>/opt/ISS/issSensors/network_sensor_1/Keys</code>

**Table 86:** Directories where agents store encryption keys

---

# Using the Public Key Configuration Tool

## Introduction

The Public Key Configuration Tool is a program that performs tasks on agents that are installed and registered to SiteProtector:

- sets up an instance of SiteProtector as a Key Administrator on the agent; this allows the instance of SiteProtector to distribute encryption keys to the agent
- releases the agent from being managed by SiteProtector; this action removes SiteProtector from “Master Status,” meaning that the Site is no longer managing the agent
- enables the Auto Import option, also called Allow First Connection option, on the agent; this action allows SiteProtector to connect to the agent the first time it attempts to, and replaces old encryption keys on the agent computer

In most cases, you do not need to use the Public Key Configuration Tool on newly installed agents because the agent’s installation program automatically performs these tasks during the installation.

## Using the tool with agents

You can use this tool for the following agents:

- Server Sensor
- Network Sensor
- Proventia Network IDS
- Proventia Network IPS

## Using the tool with components

You can use this tool for the following SiteProtector components:

- Agent Manager
- Deployment Manager
- Event Collector
- SecurityFusion module
- Third Party Module

## Running the configurator program

There are two ways to run the Public Key Configuration Tool:

- You can install and run the program on the agent computer.
- You can run the program from Deployment Manager. Use this option if you do not want to install the program on the agent computer.

**When to use the Public Key Configuration Tool**

You can use the Public Key Configuration Tool under the following circumstances:

- If you installed an agent and did not set up SiteProtector as a Key Administrator on the agent, then you can use the Public Key Configuration Tool to add SiteProtector to the agent as a Key Administrator.
- If you have an agent that is registered to another instance of SiteProtector and you want to re-register the agent to different instance of SiteProtector, then you can use the Public Key Configuration Tool on the agent.

**Important:** Do not register an agent to two instances of SiteProtector.

**Running the Public Key Configuration Tool from Deployment Manager**

To set up key administrators on an agent:

1. On the agent computer, start the Deployment Manager, and then select **Install Agents**.  
The Sensor Installation page appears.
2. Select **Install the Public Key Configuration Tool on my agent or Network Internet Scanner agent**.  
The File Download window appears.
3. Select **Run this program from its current location**.  
The Security Warning window appears.
4. Click **Yes**.  
Step 1 of the Public Key Configuration Wizard appears.
5. Click **Next**.  
The program stops the issDaemon service.  
Step 2 of the Public Key Configuration Wizard appears.
6. Enter the key administrator name for the computer where the Application Server is installed, and then click **Next**.  
The agent will accept public keys from this computer.  
Step 3 of the Public Key Configuration Wizard appears.
7. Select the **Auto-Import** check box, and then click **Next**.  
The Wizard activates the Auto-Import key feature. This feature allows the agent to accept public keys automatically.  
Step 4 of the Public Key Configuration Wizard appears.
8. Click **Yes**.  
The program restarts the issDaemon service, and then Step 5 of the Public Key Configuration Wizard appears.
9. Click **Finish**.

## SECTION D: Updating Agents

### Overview

#### Introduction

After you install the products, you must apply any available updates. Updates are software releases that add new features and security updates to the products. This chapter explains how to perform the following tasks:

- determine the update status of an agent
- apply and remove updates for these agents:
  - Server Sensor
  - Network Internet Scanner
  - Proventia Network IPS
  - Network Sensor

**Note:** Other agents are self updating, which means that the agent will update itself after you set the parameters in the agent's policy.

#### Related information

For information about updates, the update process, and how to update agents when your XPU server is not configured with Internet access, see the following:

- "Update Process" on page 90
- "Update Process without XPU Server Internet Access" on page 110

#### In this section

This section contains the following topics:

Topic	Page
Determining Agent Update Status	288
Updating Agents	289
Removing Updates	291

## Determining Agent Update Status

### Introduction

This topic explains how to determine the update status of an agent.

### Update statuses

Table 87 describes the available update statuses for agents.

Agent	Status	Description
<ul style="list-style-type: none"> <li>• Server Sensor</li> <li>• Network Sensor</li> <li>• System Scanner</li> <li>• Databridge</li> <li>• Network Internet Scanner</li> <li>• Proventia Network IDS</li> <li>• Proventia Network IPS</li> </ul>	Current	No updates available for the agent.
	Out of Date	Updates are available for the agent, and you must update the agent.
	Error	An error condition exists.
	blank	The agent is not responding to SiteProtector.
<ul style="list-style-type: none"> <li>• Desktop Protection agents such as Proventia Desktop</li> <li>• Proventia Network IPS</li> <li>• Proventia Network MFS</li> <li>• Network Enterprise Scanner</li> </ul>	Current	No updates are available for the agent.
	Out of Date	Updates are available for the agent, and you must update the agent.
	Scheduled	SiteProtector is scheduled to update the agent.
	In Progress	SiteProtector is updating the agent.
	Error	An error condition exists.
	Unknown	The Sensor Controller service is attempting to refresh the agent information and is waiting for a response from the agent. This status is usually a temporary status and will either change to Active when the agent responds or Offline if the agent does not respond in a timely fashion.
blank	The agent is not responding to SiteProtector.	

**Table 87:** *Update Statuses for agents*

### Procedure

To determine the update status of an agent:

1. In the left pane, select the *Site Node*.
2. In the **Go to** list, select **Agent**.
3. Locate the agent and the update status column.

This column indicates the update status for the agent.



---

# Updating Agents

<b>Introduction</b>	<p>This topic explains how to perform the following tasks:</p> <ul style="list-style-type: none"><li>● update a single agent</li><li>● update multiple agents at the same time</li></ul>
<b>License requirement</b>	<p>You can only apply agent updates that were released before to the expiration date of your maintenance agreement for the agent.</p>
<b>Updating multiple agents</b>	<p>You can update multiple agents at the same time. All the agents must be the same type, same version, and same XPU level.</p> <p>SiteProtector can only update 20 agents at a time. So if you apply an update to more than 20 agents, then Sensor Controller processes 20 agents at a time until it completes the process.</p> <p><b>Important:</b> IBM ISS recommends that you apply the update to a single agent for testing purposes before you update all agents of the same type.</p>
<b>Procedure</b>	<p>To update an agent:</p> <ol style="list-style-type: none"><li>1. In the left pane, select the group that contains the agent you want to update.</li><li>2. In the <b>Go to</b> list, select <b>Agent</b>.</li><li>3. In the right pane, right-click the agent, and then select <b>Updates</b> → <b>Apply XPU</b>. The Schedule Update window appears.</li><li>4. Do you want to update the agent immediately?<ul style="list-style-type: none"><li>■ If <i>yes</i>, select <b>Run Once</b> in the <b>Recurrence Pattern</b> section, and then click <b>Next</b>.</li><li>■ If <i>no</i>, schedule a command job to update the agent, and then click <b>Next</b>.</li></ul>The End User License Agreement window appears.</li><li>5. Click <b>I Accept</b>. The Select XPU window appears.</li><li>6. Select the type of update to install:<ul style="list-style-type: none"><li>■ Full Upgrade</li><li>■ Service Pack</li><li>■ X-Press Update</li></ul>The updates that will be installed are listed under Install the Following Updates.</li><li>7. Verify that the updates listed are the ones you want to install. To view the release notes for a particulate update, select the Release Notes for that update, and then click <b>View Release Notes</b>.</li><li>8. When you are ready to install the updates, click <b>Finish</b>.</li></ol>

If you selected Run Once to install the update immediately, then the installation process begins. If you schedule the update to be install at later time, then the installation process will begin at that time.

For immediate installations, SiteProtector displays progress as follows:

<b>Indicator</b>	<b>Description</b>
Overall progress	Indicates progress of the entire update process
Current step progress	Indicates progress of each individual step in the update process; the text box displays a summary of the current step

---

# Removing Updates

- Introduction** This topic explains how to remove a single update from agents.
- Removing multiple updates** This procedure removes only the last update you applied. To remove multiple updates, you must repeat this procedure for each one.
- Actions allowed** You can remove XPU's from the following agents:
- Network Sensor
  - Server Sensor
  - Network Internet Scanner
  - Proventia Network IPS
- Actions not allowed** You cannot remove updates from the following agents:
- Desktop Protection agents
  - Proventia Network MFS
  - System Scanner Databridge
- Removing an update** To remove an update:
1. In the left pane, select the group that contains the agent.
  2. In the **Go to** list, select **Agent**.
  3. In the right pane, right-click the agent, and select **Updates** → **Remove Last Update**.  
The Create Command Job window appears.
  4. In the left pane, click the **Schedule** icon.
  5. Do you want to remove the update immediately?
    - If *yes*, select **Run Once** in the **Recurrence Pattern** section, and then click **OK**.
    - If *no*, schedule a command job to remove the update, and then click **OK**.
- Verifying update removal** To verify that an update is removed:
1. In the left pane, select the group that contains the agent.
  2. In the **Go to** list, select **Agent**.
  3. In the right pane, verify the Update Status for the agent is Out of Date.



## Adding Assets



# The Asset Setup Stage

## Overview

### Introduction

The fifth stage of the SiteProtector system set up process is the Asset Setup stage. In this stage, you add network assets to the SiteProtector system. The SiteProtector system supports several methods for adding network assets. Some of these methods are as follows:

- add assets from host files and asset definition files
- add assets from Active Directory
- add assets with Internet Scanner software
- add assets detected from other IBM ISS products

### In this chapter

This chapter contains the following topics:

Topic	Page
Overview of this Stage	296
What are Assets?	297

## Overview of this Stage

### Introduction

A network environment is dynamic. Assets are added and removed and can be active and inactive at various intervals. IBM ISS recommends that you use a combination of methods to add assets to the SiteProtector system. For example, you might use Network Internet Scanner to identify and add active assets and add other assets manually or from Active Directory. The process of identifying and managing assets in the SiteProtector system is ongoing and is not complete after you add assets to the SiteProtector system the first time.

### Host and asset definition files

You can import data about your network assets from host files and asset definition files directly into the SiteProtector system. This method is useful for customers who currently maintain host or asset definition files for their network assets. This method requires that the data in the files be formatted according to very specific requirements.

### Active Directory

Importing assets into the SiteProtector system from Active Directory is a powerful way to leverage data already structured and defined in Active Directory. However, the SiteProtector system does impose some limitations on the tasks that you can perform on this data after you import it into the SiteProtector system. For example, you cannot change the name of a SiteProtector system group if it was imported from Active Directory. IBM ISS recommends that you review these limitations before you import data into the SiteProtector system from Active Directory and develop a plan to address these limitations.

### Network Internet Scanner

Running discovery scans with a Network Internet Scanner that is properly configured to work with the SiteProtector system is a quick way to add active assets to the SiteProtector system. Keep in mind that Network Internet Scanner can only identify assets that respond to it. If you plan to use Network Internet Scanner to add assets, then IBM ISS recommends that you schedule the scan jobs to run on a regular basis. This approach helps to ensure that the scanner identifies newly added network assets or network assets that might alternate between active and inactive states.

### Other IBM ISS products

After your install and configure your other IBM ISS products, they will begin to detect security events in your environment and report them to the SiteProtector system. As it receives these events, the SiteProtector system also adds the asset related to the security event to the Site Database.



## What are Assets?

### Introduction

An asset is an individual computer or device on a network. The SiteProtector system organizes assets into groups and subgroups and displays them in the left pane of the Console. It also maintains information about assets in the Asset table in the Site Database and displays the detailed asset information in the Asset view. The SiteProtector system includes grouped and ungrouped assets. Grouped assets are assets that are members of a specific group in the Site. Ungrouped assets are assets identified by the SiteProtector system and stored in the *Ungrouped Assets* group.

### Assets

Table 88 lists examples of assets.

Asset	Examples
SiteProtector system components	The following are examples of SiteProtector system components: <ul style="list-style-type: none"> <li>• Site Database</li> <li>• Application Server</li> <li>• Event Collector</li> <li>• Agent Manager</li> <li>• X-Press Update Server</li> </ul>
Agents	The following are examples of agents: <ul style="list-style-type: none"> <li>• Internet Scanner software</li> <li>• Enterprise Scanner</li> <li>• Network Sensor</li> <li>• Server Sensor</li> <li>• Proventia Network IPS</li> </ul>
High priority network host	The following are examples of high priority network hosts: <ul style="list-style-type: none"> <li>• Web servers</li> <li>• Databases</li> <li>• Computers in the demilitarized zone (DMZ)</li> </ul>

**Table 88:** *Examples of different assets*

### Methods for adding assets

Table 89 describes the methods for adding assets to groups.

Method	Description
Manual	You can manually add an asset to a group. Use this method to add a single asset to a specific group. This method requires that you have the asset information before you begin. See "Adding Assets Manually" on page 301.
Host file	You can import data from a host file to add assets to groups. Use this method to add multiple assets to a specific group. This method requires an existing host file that meets the file requirements. See "Adding Assets from a Host File" on page 303.

**Table 89:** *Methods for adding assets to groups*

<b>Method</b>	<b>Description</b>
Asset definition file	You can import data about a single asset from an asset definition file to add the asset to a group. Use this method to add a single asset to a specific group. This method requires an existing asset definition file that meets the file requirements. See "Adding Assets from an Asset Definition File" on page 305.
Active Directory	You can import assets from Active Directory. Use this method to import existing Active Directory groups, structure, and content into the SiteProtector system. This method has several very important limitations. See "Adding Assets from Active Directory" on page 308.
Internet Scanner	You can run discovery scans with Internet Scanner to add active assets to the SiteProtector system. Some identified assets might appear as members of the Ungrouped Assets group. This method requires Internet Scanner. See "Adding Assets with Network Internet Scanner" on page 311.

**Table 89:** *Methods for adding assets to groups (Continued)*

## Chapter 22

# Adding Assets

## Overview

### Introduction

This chapter provides information and instructions about how to use the following methods to add assets to SiteProtector system groups:

- manual
- host file
- asset definition file
- Active Directory
- Internet Scanner

**Note:** If you use Enterprise Scanner, follow the instructions in the *Proventia Network Enterprise Scanner User Guide*.

The chapter also provides instructions for managing and grouping ungrouped assets.

**Note:** When you register an agent with a Site with the New Agent Wizard, the Wizard automatically adds the asset where the agent resides to the Site also. You cannot, however, use the New Agent Wizard to add assets to the Site. For information about registering agents and their assets with a Site, See “Automatically Registering Agents” on page 276.

### Before you begin

Before you add assets to the SiteProtector system, you should complete the following tasks:

- Create groups, and define the group properties.  
See “Creating Groups” on page 225.
- Define Group Membership Rules and schedule a Group Ungroup Assets job for the SiteProtector system to automatically group assets that you add.  
See “Grouping Ungrouped Assets” on page 316.

### In this chapter

This chapter contains the following topics:

Topic	Page
Adding Assets Manually	301
Adding Assets from a Host File	303

<b>Topic</b>	<b>Page</b>
Adding Assets from an Asset Definition File	305
Adding Assets from Active Directory	308
Adding Assets with Network Internet Scanner	311
Editing Asset Properties	313
Grouping Ungrouped Assets	316

## Adding Assets Manually

**Introduction** This topic explains how to add assets to the SiteProtector system manually.

**Procedure** To add an asset manually:

1. In the left pane, right-click the group where you want to add the asset, and then select **New** → **Asset** from the pop-up menu.  
The New Asset window appears.
2. Provide the required information as follows, and then click **OK**:

Field	Description
Inventory Tag	The Inventory Tag is an identifier that you create and assign to an asset or group of assets for tracking purposes. If you use identifiers from another tool to track assets, consider using these identifiers in the SiteProtector system.
DNS Name	The Domain Name System is a unique name assigned to the asset by a domain name server. If the host does not resolve host names using a DNS server, the DNS name for this host may not exist or may be unavailable.
IP Address	The IP address is the IPv4 address of the host. The SiteProtector system requires a valid version 4 address to display an asset in the Asset view.
NetBIOS Name	NetBIOS is the name that identifies the asset in the Network Basic Input/Output System.
NetBIOS Domain	NetBIOS Domain name is the name of the computer, and it is typically followed by a dollar sign (\$). Many client applications still use NetBIOS instead of DNS for naming hosts.
IPv6 Address	IPv6 address is the new standard for Internet Protocol that is specified by the IETF. Typically, this information appears only if the asset is associated with an IPv6 address.
OS Name	OS Name is the name of the host operating system. This field may be populated when you run a Network Internet Scanner scan, or import Active Directory or other information into the SiteProtector system.
OS Version	OS Version is the name of the version of the system specified in the <b>OS Name</b> box.
MAC address	The Media Access Control address is the unique hardware identifier for the asset.
Criticality	Criticality is an option that you can assign to an asset or groups of assets based on the asset's importance to your organization, as follows: <ul style="list-style-type: none"> <li>• critical</li> <li>• high</li> <li>• medium</li> <li>• low</li> <li>• not critical</li> </ul>

<b>Field</b>	<b>Description</b>
Owner	Owner is a user-defined field that lets you assign an owner, such as individual or department, to the asset.
Function	Function is a user-defined category that you can assign to an asset or groups of assets. Examples of function are database, router, or application server. The information that you enter in this box only appears in the Asset Event Detail report.

---

# Adding Assets from a Host File

**Introduction** This topic explains how to add assets to the SiteProtector system from a host file.

**Recommendation** This method is recommended in the following situations:

- You are adding a small number of assets.
- You have an existing host file that contains the required host information in the proper format.

**Host file** A host file contains the IP addresses of host on your network. Network Internet Scanner uses the information in this file when it runs scan jobs on your network. A host file can have one of the following extensions:

- .hst
- .csv

**Format requirements**

The entries in the host file must meet the following requirements:

- You must specify the host address as an IP address, DNS name, or NetBIOS name.
- You must put each host address either on its own separate line or start the address after a space.
- You must put a number sign (#) before any comments or data that you want ignored.
- You must indicate IP address ranges with a dash (-).

**Example entries** Table 90 lists some examples of valid entries from a host file.

Entry	Description
1.1.1.1	single IP address
WebServer01	single Domain Name System (DNS) name
1.1.1.1 1.1.1.100	two IP address on separate lines
1.1.1.1,1.1.1.100	two IP addresses separated by commas
1.1.1.1-1.1.1.100	IP address range
209.134.161.35 # Intranet Server	single IP address with comment
# IP addresses for IT	ignored comment

**Table 90:** Example entries in host file

**Adding assets from host files** To add assets to the SiteProtector system from a host file:

1. In the left pane, right-click the group where you want to add assets, and then select **New** → **Asset** from the pop-up menu.  
The New Asset window appears.

2. Click **Import**, browse, and then select the file you want to import.

**Note:** The host file you are importing must have one of the following extensions:

- .hst
- .csv

3. (Optional) Select the **Resolve DNS and Netbios Names** check box if you want the SiteProtector system to resolve the DNS and NetBIOS names of the imported assets.

4. Click **OK**.

The SiteProtector system adds the assets to the group you selected. The process for importing assets into the SiteProtector system from a host file can take a significant amount of time depending on the number of assets you are adding.

5. If you want to monitor the progress of the import job, click **Command Job**; otherwise, click **Close**.



# Adding Assets from an Asset Definition File

- Introduction** This topic explains how to add assets to the SiteProtector system from an asset definition file. This method is efficient for adding a large number of assets.
- Using LDAP** If you are importing asset information from a separate directory, such as LDAP, then you can use a scripting tool to automate the transfer of this information to the correct fields in the asset definition file.
- Group tags** The asset definition file is an XML file containing information about the groups and assets you want to import. The following tags are valid.

Tag	Description
<groups>	A top level element containing the groups or assets you want to define.
<group name='GroupName' description='Description'>	A group and its name with an optional description. If a group with this name already exists at the defined level it will use the existing group instead of creating a new one.
<asset>	Definition for an asset. The following attributes are allowed, which are the same as the Console equivalent: <ul style="list-style-type: none"> <li>• netBiosDomain</li> <li>• netBiosName</li> <li>• os</li> <li>• osVersion</li> <li>• inventoryTag</li> <li>• criticality</li> <li>• owner</li> </ul>
<nic>	Information about the nic card associated with an asset. This should be found inside an <asset> tag. The following attributes are allowed: <ul style="list-style-type: none"> <li>• ipv4</li> <li>• dnsName</li> <li>• ipv6</li> <li>• macAddress</li> </ul>
<function name='FunctionName'>	A function associated with an asset. This should be found inside an <asset> tag. If a function with this name already exists it will link it to that function. Otherwise it will create the function and link it to the new function.

**Table 91:** Valid tags in an asset definition file

- Example 1** The following example shows how to import a single asset:

```
<asset inventoryTag='LADIDA-1999-12345' os='Windows XP' osVersion='SP2'
  owner='bill' domain='WORKGROUP' netBiosName='SNOOPY' criticality='4'>
<nic ipv4='207.123.123.123' dnsName='johndoe.net'
  ipv6='1111:2222:3333:4444:5555:6666:7777:8888'
```

```

    macAddress='00:30:23:15:C9:D3' />
</function name='Web Server' />
</function name='Database' />
</asset>

```

**Example 2** The following example shows how to import multiple assets under your selected group:

```

<groups>
  <asset><nic ipv4='10.10.10.1' /></asset>
  <asset><nic ipv4='10.10.10.2' /></asset>
  <asset><nic ipv4='10.10.10.3' /></asset>
</groups>

```

**Example 3** The following example shows how to import multiple groups under your selected group:

```

<groups>
  <group name='Asia'>
  </group>
  <group name='Americas'>
    <group name='Canada'></group>
    <group name='US'></group>
  </group>
</groups>

```

**Example 4** The following example shows how to import multiple groups with assets under your selected group:

```

<groups>
  <group name='Asia'>
    <asset><nic ipv4='10.10.20.1' /></asset>
    <asset><nic ipv4='10.10.20.2' /></asset>
  </group>
  <group name='Americas'>
    <group name='Canada'>
      <asset><nic ipv4='10.10.30.1' /></asset>
      <asset><nic ipv4='10.10.30.2' /></asset>
      <asset><nic ipv4='10.10.30.3' /></asset>
    </group>
    <group name='US'>
      <asset><nic ipv4='10.10.40.1' /></asset>
    </group>
  </group>
</groups>

```

**Procedure** To add an asset to the SiteProtector system from an asset definition file:

1. In the left pane, right-click the group where you want to add assets, and then select **New** → **Asset** from the pop-up menu.

The New Asset window appears.

2. Click **Import**, browse, and then select the asset definition file you want to import.

**Note:** The asset definition file has an .xml extension.

3. Click **OK**.

The SiteProtector system adds the asset to the group you selected.

4. If you want to monitor the progress of the import job, click **Command Job**; otherwise, click **Close**.

## Adding Assets from Active Directory

### Introduction

This topic provides information and instructions about how to add assets and asset groups to the SiteProtector system from Active Directory.

### Restrictions

Adding assets to the SiteProtector system by importing them from Active Directory has the following restrictions:

- You can have only one Active Directory structure in the left pane of the Console.
- You can import Windows assets only.
- You can import only the structure, user information, and asset configuration data from Active Directory.
- You cannot move, change, or delete assets or asset groups after you import them from Active Directory. You can copy assets imported from Active Directory to other groups in the SiteProtector system, but any changes you make to the asset are global, meaning that the changes affect the asset in every group where it is a member.
- You cannot automatically update assets or asset groups in the SiteProtector system when you change them in Active Directory. You must rerun the import job to incorporate Active Directory changes into the SiteProtector system.

**Reference:** For information about using Active Directory, see the Microsoft documentation.

### Imported data

Table 92 describes the data that the job imports from Active Directory.

Information	Description
Structure	The job replicates the asset grouping structure from Active Directory into the left pane of the Console.
User data	The job imports the following user data, and the Console displays it in the Asset view: <ul style="list-style-type: none"> <li>• login name</li> <li>• full name</li> <li>• fully qualified path to a user object in Active Directory</li> <li>• phone number</li> <li>• domain</li> <li>• authenticating server</li> </ul>
Asset configuration data	The job imports the following asset configuration data, and the Console displays it in the Asset view: <ul style="list-style-type: none"> <li>• computer's distinguished name</li> <li>• DNS</li> <li>• OS</li> </ul>

**Table 92:** Data imported from Active Directory

**Before you begin**

Before you import assets from Active Directory, you must complete the following tasks:

- Ensure that the information in Active Directory is current and correct.
- Ensure that the group structure of the information in Active Directory is the structure you want to use in the SiteProtector system. If the structure is incorrect, then you can use a third-party tool to organize the information in the Active Directory before you import it into the SiteProtector system.

**Procedure**

To add assets from Active Directory information:

1. In the left pane, right-click the *Site Node*, and then select **Import Active Directory** from the pop-up menu.

The Active Directory Group Population window appears.

2. Select the **Import Active Directory** icon.
3. In the **Options** section, click **Set Credentials** (to establish login credentials for the Active Directory domain).

The Login Credentials for Active Directory window appears.

4. Type your **Server or Domain name**, your domain **User name**, and your domain **Password**.

**Tip:** Click the **Help** icon on the Login Credentials for Active Directory window for additional information.

5. If you want to change the size of groups that you get from Active Directory, type or select the number in the **Page size** box.
6. Click **OK**.

7. Do you know the name of the domain list that you want to add to the SiteProtector system?

- If *yes*, type the name of the domain in the **Starting Domain** box.

- If *no*, click **Get Domains**, and then select the domain from the **Starting Domain** list.

8. If the sensor's host is in both an Active Directory group and a SiteProtector system group, and you want to require that agents use the policy assigned to the Active Directory group, select the **Reassign sensor policy based on Active Directory grouping** check box in the **Options** section.

**Important:** If you already use the SiteProtector system, and you are adding the Active Directory information in the left pane for the first time, do not use this setting because the policies for the SiteProtector system groups may not work as scheduled. After you add the Active Directory groups to the left pane, select them, and then apply the policies you want to use.

**Reference:** See the topic about policy assignment with Active Directory.

9. If you want to display all the trees in the Active Directory forest, select the **Grow Entire Forest** check box in the **Options** section.

**Note:** The starting domain must be the forest root. The forest root is denoted by (root) if you use **Get Domains**.

10. Select the **Schedule** icon.

11. Do you want to add Active Directory information immediately?

- If *yes*, select the **Run Once** option, and then go to Step 14.

- If *no*, select the **Recurrence pattern** option you want to use.

12. In the **Event time** section, click the **Start** arrow to specify a date and time.
13. Do you want to specify an end date?
  - If *yes*, select **End by** in the **Range of recurrence** section, and then click the arrow to specify a date and time.
  - If *no*, select **No end date**.
14. Click **OK**.

The Active Directory job runs as scheduled. To view the status of the job, right-click the *Site Node*, select **Properties** from the pop-up menu, and then click the **Command Jobs** icon.
15. When the job finishes successfully, press SHIFT+F5 to refresh the left pane with the Active Directory groups.

# Adding Assets with Network Internet Scanner

## Introduction

You can use Network Internet Scanner to run discovery scans and add assets to the SiteProtector system. Network Internet Scanner places the assets in the correct asset groups based on membership rules. Discovery scans identify active assets only. The scan does not add assets that do not respond to the scan.

## Prerequisites

Before you run a scan job to add assets to the SiteProtector system, you must complete the following tasks:

- Create groups, and define the group properties.  
See “Creating Groups” on page 225.
- Create Site ranges in Ungrouped Assets, and schedule a Group Ungrouped Assets job to automatically group the assets.  
See “Grouping Ungrouped Assets” on page 316.  
**Note:** If you do not have Site ranges defined in Ungrouped Assets, then you must use one of the methods described in this chapter to add assets to the group you want to scan before you run the scan.
- Install Network Internet Scanner, and verify that it is properly configured and registered with the SiteProtector system.  
See the *Internet Scanner Installation Guide*.

## Scope of scan

You should scan only a single domain in a discovery scan. If you need to scan more than one domain, then you must perform the following tasks:

- Divide the scan into a series of scans.
- Install Network Internet Scanner on an asset in each domain.

## Information gathered

A discovery scan gathers the following information:

- IP Address
- NetBIOS Name
- DNS Name
- OS Name
- NetBIOS Domain Name

## Task overview

Table 93 describes the tasks for adding assets with Network Internet Scanner.

Task	Description
1	Add a Network Internet Scanner.
2	Set the scan policy, and then use Network Internet Scanner to run a discovery scan.

**Table 93:** Tasks for adding assets with Network Internet Scanner

### Adding a Network Internet Scanner

To add a Network Internet Scanner host:

1. In the left pane, right-click the group that you want to add the Network Internet Scanner host, and then select **New** → **Agent** from the pop-up menu.  
The New Agent Wizard appears.
2. Type the DNS name or the IP address of the Network Internet Scanner host, and then click **Add**.
3. Click **Next**.
4. From the list, select an Event Collector that you want this Network Internet Scanner to send events to, and then click **Next**.  
The Register Agent Software window appears, indicating the agent has been successfully installed.
5. Click **Finish**.

### Running a scan

To run a discovery scan:

1. In the left pane, right-click the group that you want to scan, and then select **Scan** from the pop-up menu.  
The Scan Group window appears.
2. Select **Scan Policy** icon, and then select a policy from the list.  
**Tip:** Consider using the D1 Light Discovery policy for efficiency.
3. Select the **Session Properties** icon, and then select the default properties from the list in the right pane.
4. Click **OK**.  
The scan job identifies assets on your network and puts the assets into the SiteProtector system groups based on group membership rules.



## Editing Asset Properties

### Introduction

You can edit the properties of an asset or a group of assets. This information can help you organize and track assets that you are monitoring. Consider editing asset properties in the following situations:

- you want to add assets in a piecemeal fashion because the method that you used to add or import assets did not populate all fields in the Asset table
- you want to change values of user-specified fields, such as criticality and function

**Important:** Certain fields can be overwritten if you update the Asset table after you edit Asset Properties. Use caution when you import hosts or run scans if you want to retain this information.

### New Asset window

Each asset contains a properties file with the following fields. The SiteProtector system saves this information to the Asset table in the Site database and displays it in the Asset view. Table 94 describes these fields.

Field	Description
Inventory Tag	The Inventory Tag is an identifier that you create and assign to an asset or group of assets for tracking purposes. If you use identifiers from another tool to track assets, consider using these identifiers in the SiteProtector system.
DNS Name	The Domain Name System is a unique name assigned to the asset by a domain name server. If the host does not resolve host names using a DNS server, the DNS name for this host may not exist or may be unavailable.
IP Address	The IP address is the IPv4 address of the host. The SiteProtector system requires a valid Version 4 address to display an asset in the Asset view.
NetBIOS Name	NetBIOS is the name that identifies the asset in the Network Basic Input/Output System.
NetBIOS Domain	NetBIOS Domain name is the name of the computer, and it is typically followed by a dollar sign (\$). Many client applications still use NetBIOS instead of DNS for naming hosts.
IPv6 Address	IPv6 address is the new standard for Internet Protocol that is specified by the IETF. Typically, this information appears only if the asset is associated with an IPv6 address.
OS Name	OS Name is the name of the host operating system. This field may be populated when you run a Network Internet Scanner scan, or import Active Directory or other information into the SiteProtector system.
OS Version	OS Version is the name of the version of the system specified in the <b>OS Name</b> box.
MAC address	The Media Access Control address is the unique hardware identifier for the asset.

**Table 94:** Descriptions of fields in the New Asset window

Field	Description
Criticality	Criticality is an option that you can assign to an asset or groups of assets based on the asset's importance to your organization, as follows: <ul style="list-style-type: none"> <li>critical</li> <li>high</li> <li>medium</li> <li>low</li> <li>not critical</li> </ul>
Owner	Owner is a user-defined field that lets you assign an owner, such as individual or department, to the asset.
Function	Function is a user-defined category that you can assign to an asset or groups of assets. Examples of function are database, router, or application server. The information that you enter in this box only appears in the Asset Event Detail report.

**Table 94:** Descriptions of fields in the New Asset window (Continued)

## Procedure

To edit properties for assets or groups of assets:

1. Select **Asset** from the menu.  
The **Asset** view appears in the right pane.
2. Right-click the asset you want to edit, and then select **Properties** from the menu.  
The New Asset window appears.  
**Note:** You can select multiple assets to edit simultaneously
3. In the **Inventory Tag** box, use a combination of letters, numbers, and characters to type a unique identifier for this host. Example: 3JX-7809.  
**Note:** Because the inventory tag identifies a unique asset on your network, exercise caution if you must change this tag.
4. Edit the following fields:
  - DNS Name
  - IP Address (This field is required.)
  - NetBIOS Name
  - NetBIOS Domain**Note:** If you are editing the properties of more than one asset, DNS Name, IP Address, and NetBIOS Domain do not appear in this window.
5. Use only letters and numbers to type the host's **IPv6 address**, as follows:  
xxxx : xxxx : xxxx : xxxx : xxxx : xxxx : xxxx : xxxx  
**Important:** The SiteProtector system requires a valid version 4 IP address to track and monitor an asset.
6. In the **OS Name** box, type the operating system of the asset.  
**Note:** After you edit this field, you cannot overwrite it by importing data or running a vulnerability scan.
7. In the **OS Version** box, type the version of the system you specified in Step 6.

8. From the **Criticality** list, select a category that you want to assign to this asset or group that indicates this asset's level of importance.
9. Type the individual or department that owns this asset in the **Owner** box.
10. Select the asset function from the **Function** list, or click **Add** to type the name in a separate window, and then add it to the list.

## Grouping Ungrouped Assets

**Introduction** This topic provides information and instructions for grouping ungrouped assets.

**Ungrouped asset** An ungrouped asset is any asset in the Ungrouped Assets group. These assets are identified by the SiteProtector system or one of the products that works with the SiteProtector system.

**Methods** Table 95 describes the methods for grouping ungrouped assets.

Method	Description
Manual	Move the assets from Ungrouped Assets to other groups.
Site Ranges	<p>A Site range is a special type of subgroup in Ungrouped Assets. It defines a starting and ending IP address. You can group ungrouped assets by their IP address into the Site ranges. The SiteProtector system installation creates the first Site range automatically. As agents detect security events, the assets where the events occur are automatically added to the Site and appear by IP address in <code>Ungrouped Assets:Site Range</code>.</p> <p>Create subgroups called <i>Site Ranges</i> in the Ungrouped Assets group and group these assets by IP address into the site ranges.</p>
Group Ungrouped Assets job	<p>You can run a job called <i>Group Ungrouped Assets</i> that automatically moves assets out of Ungrouped Assets into other groups. The job moves assets to other groups based on the asset IP address, DNS name, NetBIOS name, or operating system. For the job to function properly, you must define membership rules for groups. The job uses membership rules to determine where to relocate the assets.</p> <p>Before you run or schedule a Group Ungrouped Assets job, you must define membership rules for the group.</p> <p>Run or schedule a Group Ungrouped Assets job to automatically relocate ungrouped asset to other groups based on the asset's IP address, DNS name, NetBIOS name, or operating system name.</p> <p><b>Note:</b> This job only works if you define membership rules for the groups in the Site before you run the job. See "Creating Groups" on page 225 for instructions on how to set up group membership rules.</p>

**Table 95:** *Methods for grouping ungrouped assets*

**Manually grouping ungrouped assets** To manually group ungrouped assets:

1. In the left pane, expand **Ungrouped Assets**, and then select a Site range.
2. In the **Go to** list, select **Asset**.  
The assets in the Site range appear in the **Asset** view.
3. Select the asset(s) you want to move in the **Asset** view, and then drag and drop the asset(s) to the appropriate group.

**Creating site ranges** To create a Site range:

1. In the left pane, right-click **Ungrouped Assets**, and then select **New → Site Range** from the pop-up menu.

A new group appears below the **Ungrouped Assets** folder.

- Click the selected group, and then type the Site range as one of the following:

Type	Format
single IP address	x.x.x.x
IP address range	x.x.x.x-y.y.y.y or x.x.x.* * represents a wildcard.

- Press **Enter**.

### Running Group Ungrouped Assets jobs

To run a Group Ungrouped Assets job:

- In the left pane, right-click a Site Range, and then select **Group Ungrouped Assets** from the pop-up menu.

The Create Command Job: Group Ungrouped Assets window appears.

- In the **Recurrence Pattern** section, select Run Once to run the job immediately, or schedule the job to run on a recurring schedule.

**Note:** IBM ISS strongly recommends that you schedule this job to ensure that assets are regularly moved to their appropriate locations.

- Click **OK**.

The job runs based on the schedule you set.



## Setting Up the Reporting Module





## Chapter 23

# Reporting Module

## Overview

**Introduction** This chapter provides information about how to create reports.

**In this chapter** This chapter contains the following topics:

<b>Topic</b>	<b>Page</b>
Working with Reports	322
Working with Event Data Reports	323
Compliance and Summary Reports	325
Working with Compliance and Summary Reports	329

# Working with Reports

## Introduction

To ensure the security of your network, you must understand the state of your security on different levels. The SiteProtector system includes a Report Module, which creates reports as follows:

- At the event level, you can create reports from the events in analysis views.
- At the Site level, you can create preformatted summary and compliance reports.  
**Note:** These reports require a separately purchased license for SiteProtector system Reporting.
- At the enterprise level, you can create trend and summary reports for multiple Sites.

## SiteProtector system reports

Table 96 explains where to create reports in the SiteProtector system.

Type of Report	Where You Create It
Event data	Analysis view
Summary and compliance	Report view

**Table 96:** *Where to create reports in the SiteProtector system*

# Working with Event Data Reports

## Introduction

This topic provides instructions for the following tasks:

- using keyboard shortcuts
- printing event data reports
- exporting event data reports
- saving event data reports
- scheduling event data reports

## Report generation techniques

You can use any combination of the following techniques to generate the data for a report:

- Select an analysis view.
- Apply filters.
- Add, remove, or reorder columns.
- Select a guided question for the event from an Analysis view.

## Using keyboard shortcuts

Table 97 describes the keyboard shortcuts available for working with event reports.

Keyboard Shortcut	Description
CTRL+P	Prints data
CTRL+E	Exports data

**Table 97:** Keyboard shortcuts for event reports

## Printing event data reports

To print a report from event data:

1. In the left pane, select the group to use.
2. In the **Go to** list, select **Analysis**.
3. Click **Action** → **Data Export** → **Print**.

The Print window appears.

4. Select a printer and printing options, and then click **Print**.

## Saving reports

To save a report to a file:

1. In the left pane, select a group.
2. In the **Go to** list, select **Analysis**.
3. If you want to select specific rows and columns to print, select those rows and columns.
4. Choose an export option:

If you want to export...	Then...
data only	Click <b>View</b> → <b>Export View</b> .

If you want to export...	Then...
events with vulnerability help	Click <b>Action</b> → <b>Data Export</b> → <b>Export with Vulnerability Help</b> . <b>Note:</b> Available only from an Analysis tab.

5. Type or browse to the path of the file where you want to export the data.
6. Select the format of the file in the **File Type** list.
7. In the **Exported Content** area, select one of the following options:

If you want to export...	Then select...
all of the data	Entire table.
only the selected data	<b>Selection only.</b>
specific rows	<b>Rows</b> , and then select the beginning and ending rows.
specific columns	<b>These Columns</b> , and then clear any of the columns you do not want to export. <b>Note:</b> This option applies to all rows in the tab, whether selected or not.

8. Click **OK**.

**Scheduling a report** To schedule a report:

1. In the left pane, select a group.
2. In the **Go to** list, select **Analysis**.
3. Click **Action** → **Data Export** → **Schedule Export**.  
The Analysis Data Export window appears.
4. Verify the Command Details, and then click the **Parameters** icon.
5. In the **Output Parameters** area, type a File Name, select a file type, and then select the time for which you want data to appear in the file.
6. In the **Analysis Data Export Parameters** area, select the **Analysis View**.
7. If you want to display vulnerability information in the report, then select the **Display Vulnerability Help in Analysis Data Export** option.
8. To set Advanced Filters, click **Filter**, and then set the filters.
9. Click the **Schedule** icon, and then schedule the job.
10. Click **OK**.

# Compliance and Summary Reports

## Introduction

The SiteProtector system provides predefined reports on the Report tab. These reports help you identify trends across your organization, evaluate the overall effectiveness of security measures, and verify the state of your security. These reports contain the parameters needed to generate a report, including headers, footers, filters, and format.

**Note:** These reports require a separately purchased license for SiteProtector system Reporting.

## Report categories

The reports are grouped by the following categories on the Report tab:

- Assessment
- Asset
- Attack Activity
- Audit (SiteProtector system user actions)
- Content Filtering
- Mail Filtering
- Management
- Permissions
- Ticket
- Virus Activity

## Assessment reports

Table 98 describes the preformatted assessment reports.

Report Name	Description
Asset Assessment Detail	Discovered assets with detailed information about network services and vulnerabilities.
Asset Assessment Summary	Discovered assets and identifies network services and vulnerabilities for each asset.
Operating System Summary	Percentage and number of assets by operating system discovered during an automated network scan.
Operating System Summary By Asset	The operating systems detected on the network.
PCI Detail	Detailed list of vulnerabilities and services, including vulnerability remedies and references according to Payment Card Industry standards.
PCI Summary	Counts of vulnerabilities by severity, vulnerabilities by Operating System, summary of asset risk scores according to PCI standards.
Service Summary	The network services detected on the scanned assets.
Service Summary By Asset	The network services detected on each scanned asset.
Top Vulnerabilities	The top vulnerabilities by frequency for a specified group and time.

**Table 98:** *Assessment report descriptions*

Report Name	Description
Vulnerability By Asset	The top assets by number of vulnerabilities for a specified group and time.
Vulnerability By Group	Comparison of vulnerabilities across subgroups of a selected group.
Vulnerability By OS	Comparison of vulnerability counts by operating systems.
Vulnerability Counts	Detected vulnerabilities by total number and by percentage.
Vulnerability Counts By Asset	The number and severity of vulnerabilities for each asset.
Vulnerability Detail By Asset	Detected vulnerabilities by asset. Provides the DNS name, IP address, operating system type, and remediation information.
Vulnerability Differential	Summary comparison of vulnerabilities and details for each asset.
Vulnerability Names By Asset	Detected vulnerabilities by DNS name, IP address, and the name of each vulnerability detected.
Vulnerability Remedies By Asset	Detected vulnerabilities by asset and includes remediation information.
Vulnerability Summary By Asset	Detected vulnerabilities by DNS name, IP address, operating system, and the name of each vulnerability detected.
Vulnerable Assets	Lists assets by criticality for each vulnerability.

**Table 98:** *Assessment report descriptions (Continued)*

## Asset reports

Table 99 describes the preformatted asset reports.

Report Name	Description
Asset Event Details	Lists asset event and vulnerability details.
Asset Event Summary	Lists a summary of asset events and vulnerabilities.
Asset Risk Report	Displays asset risk scores trended over time and in detail.
Desktop Protection Report	Displays counts of desktop assets protected and not protected with version details.
Server Protection Report	Displays counts of server assets protected and not protected with version details.

**Table 99:** *Asset report descriptions*

## Attack activity reports

Table 100 describes the preformatted attack activity reports.

Report Name	Description
Attacks By Group	Comparison of attack counts across subgroups of a selected group.
Attacks By Protection Domain	Comparison of attack counts across protection domains of a selected group.
Security Events By Category	Displays percentage and number of events by event category for a specified group and time.

**Table 100:** *Attack activity report descriptions*

Report Name	Description
Top Attacks	The top attack names by frequency for a specified group and time.
Top Attacks By Severity	Counts the top attack names by severity for a specified group and time.
Top Sources of Attack	The top attack sources by frequency for a specified group and time.
Top Targets of Attack	The top attack targets by frequency for a specified group and time.
Top Targets of Attack By Severity	Counts the top attack targets by severity for a specified group and time.

**Table 100:** *Attack activity report descriptions (Continued)*

## Audit reports

Table describes the preformatted audit reports.

Report Name	Description
Audit Detail	Provides an audit trail of significant actions performed by SiteProtector system users.
User To Group	Membership between users and groups.

**Table 101:** *Audit report descriptions*

## Content filtering reports

Table 102 describes the preformatted content filtering reports.

Report Name	Description
Top Web Categories	Displays blocked and unblocked categories along with the number of assets and requests.
Web Requests	Indicates the top requested blocked and unblocked categories or reports that indicate the top blocked and unblocked categories.

**Table 102:** *Content filtering report descriptions*

## Mail filtering reports

Table 103 describes the preformatted mail filtering reports.

Report Name	Description
Executive Summary	Displays email trends of quarantined, released, action taken, and total emails.
Top Analysis Modules	Displays count of emails by analysis module.
Top Recipients	Displays top recipients by count or size of emails.
Top Responses	Displays count of emails by responses.
Top Senders	Displays top senders by count or size of emails.
Traffic Report	Displays email trends by hour.

**Table 103:** *Mail filtering report descriptions*

**Management reports**

Table 104 describes the preformatted management reports.

Report Name	Description
Attack Incidents	All security incidents created for a specified time.
Attack Status Summary	Attack status summary, including SecurityFusion module and blocked events.
Attack Trend	Attack activity by Day/Week/Month/Quarter/Year.
Virus Activity Trend	Virus activity by Day/Week/Month/Quarter/Year.
Vulnerability Trend	Vulnerabilities by Day/Week/Month/Quarter/Year.

**Table 104:** *Management report descriptions*

**Permission report**

The Permission Detail report displays users and the permissions assigned to each of them.

**Ticket reports**

Table 105 describes the preformatted ticket reports.

Report Name	Description
Ticket Activity Summary	Summary of the ticket count and tracks the time per ticket status.
Ticket Time Tracking	Summary of the working time put into the SiteProtector system tickets.
Ticket Trend	Trend summary of tickets.

**Table 105:** *Ticket report descriptions*

**Virus activity reports**

Table 106 describes the preformatted virus activity reports.

Report Name	Description
Top Virus Activity	Top viruses by frequency for a specified group and time.
Virus Activity by Asset	The top assets by amount of virus activity for a specified group and time.
Virus Activity by Group	Comparison of virus activity across subgroups of a selected group.
Virus Prevention Benefits	Summarizes virus infections versus infections prevented and calculates ROI cost savings.
Virus Trend Details	Charts and lists all virus activity across a specified time period.

**Table 106:** *Virus activity report descriptions*



---

# Working with Compliance and Summary Reports

- Introduction** This topic explains how to run a report on the Report tab.
- Report formats** You can print or save reports created on the Report tab in any of the following formats:
- portable document format (PDF)
  - hypertext markup language (HTML)
  - comma-separated value (CSV)
- Lengthy reports** If a report exceeds 30 pages, the HTML format causes the text in the report to overlap and become unreadable. To avoid the problem, use the PDF or CSV format when you run a report that may exceed 30 pages.
- Creating reports** To create a report from the Report tab:
1. In the left pane, select a group.  
**Note:** The selected group does not affect Permissions or Audit reports.
  2. In the **Go to** list, select **Report**.  
The SiteProtector system displays a list of reports.
  3. Right-click a report, and then select **New Report** from the pop-up menu.  
The Report window appears.
  4. On the Report Specification tab, enter the **Report Filename** and optional **Report Comments**, and then select the **Report Type**.
  5. Set report options.  
**Note:** Report options vary by report. Some categories include the following:
    - General
    - Display
    - Filters
    - Report Period
    - Report Format
    - Email Distribution
  6. Select the **Recurrence** tab, and then schedule the job.
  7. Click **OK**.
- Viewing reports** To view a report:
1. In the left pane, select a group.
  2. In the **Go to** list, select **Report**.  
The SiteProtector system displays a list of reports.
  3. Right-click a report, and then select **Properties** from the pop-up menu.  
The SiteProtector system displays the available reports.  
**Note:** You can also select more than one report at a time.

4. Double-click a report in the list to view it.

### **Saving reports**

To save a report:

1. In the left pane, select a group.
2. In the **Go to** list, select **Report**.  
The SiteProtector system displays a list of reports.
3. Right-click a report, and then select **Properties** from the pop-up menu.  
The SiteProtector system displays the available reports.  
**Note:** You can also select more than one report at a time.
4. Right-click the report, and then select **Save As**.
5. Provide the file name, and click **Save**.

## Chapter 24

# Configuring Audit Options

## Overview

### Introduction

The SiteProtector system lets you track activity for auditing purposes and then generate this information in a preformatted report. This chapter provides information about audit records and a procedure for specifying the types of records that appear in audit reports.

### In this chapter

This chapter contains the following topics:

Topic	Page
Audit Options	332
Configuring the SiteProtector System to Log Actions	339

## Audit Options

### Introduction

The SiteProtector system lets you log almost all actions that are performed in the SiteProtector system. This topic provides descriptions of these options and the specific information that appears in each log record.

### What do audit records contain?

A record appears in the Audit Detail report for each action that is logged by the SiteProtector system if the specified action was performed. Audit records typically contain the following information:

- action
- the type of action
- the time and date an action occurred
- the user or SiteProtector system component that performed the action
- location where the action was performed

**Important:** The action and the action type apply to the specific audit option that is enabled. Additional information about these items are described in the tables in this topic.

### Where does audit information appear?

Audit records appear in the Audit Detail Report. For information about configuring this report, see the Running Reports chapter in the *SiteProtector User Guide for Security Analysts*.

### Options that appear on the General tab

Table 107 describes the options that appear on the General tab of the Manage Audit window.

This option...	Adds a record to the Audit log when the following occurs...
Start [Stop] Application Server/Auditing	Application Server is started or stopped.
Console Login/Logout	user logs on or log off from the SiteProtector system Console.
Web Login/Logout	user logs on or log off from the Web console.
Update Auditing Setup	user updates options in the Manage Audit windows.
Update Site Level Permissions	user updates Site Level Permissions. Record includes the permission that was updated.
Auto Group Hosts on Site Range	An auto group job runs. Record includes the job name.
Manage SecureSync	The user configures an option on the Manage Secure Sync window. Record includes the Secure Sync option that was configured.

**Table 107:** *Options that appear on the General tab*

**Options that appear on the Group tab**

Table 108 describes the options that appear on the Group tab of the Auditing setup window.

<b>This option...</b>	<b>Adds a record to the Audit log when the following occurs...</b>
Add New Group	User adds a group to the tree. Record includes the name of the group that was added.
Update Group	User updates a group in the tree. Record includes the name of the group that was updated.
Delete Group	User deletes a group in the tree. Record includes the name of the group that was deleted.
Update Group Permissions	User updates group permissions. Record includes the permission that was changed, group name, and location of group.
Load Active Directory/Set Credentials	User updates the options on the Login Credentials for Active Directory window. Record includes the Active Directory option that was configured.
Delete Active Directory	User deletes an entire Active Directory structure.

**Table 108:** *Options that appear on the Group tab*

**Options that appear on the Agent tab**

Table 109 describes the options that appear on the Agent tab of the Auditing Setup window.

<b>This option...</b>	<b>Adds a record to the Audit log when the following occurs...</b>
Add Agent	User adds an agent to the Agent view. Record includes the agent name.
Delete Agent	User deletes agent from the Agent view. Record includes the agent name.
Force Refresh Agent	User forces an agent to refresh. Record includes the agent name.
Start [Stop] Agent	User uses the Start or Stop commands to stop or start an agent.
Start Scan	User starts a scan job. Record includes the name of the scanning agent and the scan job.
Cancel Scan	User cancels a scan job.
Pause Scan	User pauses a scan job. Record includes the name of the scanning agent and the scan job.
Resume Scan	User resumes a scan job. Record includes the name of the scanning agent and the scan job.
Update Agent Response	User updates agent responses. Record includes the response name and the agent the response was applied to.
Update Agent Property	User updates agent properties. Record includes the property updated and the agent to which the change was applied.
Update Database Maintenance	User updates database maintenance settings. Record includes the option that was updated.
Add Agent Update	User applies an X-Press Update to an agent. Record includes the agent name and the name of the update that was applied.

**Table 109:** *Options that appear on the Agent tab*

This option...	Adds a record to the Audit log when the following occurs...
Remove Agent Update	User removes an X-Press Update from an agent. Record includes the agent name of the update that was removed.
Enable SOC Event Monitoring	User enables the SiteProtector system to send network security information to IBM ISS Managed Security Services.
Disable SOC Event Monitoring	User stops the SiteProtector system from sending security information to IBM ISS Managed Security Services.

**Table 109:** Options that appear on the Agent tab (Continued)

### Options that appear on the Asset tab

Table 110 describes the options that appear on the Asset tab of the Auditing Setup window.

This option...	Adds a record to the Audit log when the following occurs...
Add Asset	User adds an asset to the tree. Record includes the name of the asset that was added.
Update Asset	User updates an asset in the tree. Record includes the name of the asset that was updated.
Delete Asset	User deletes an asset in the tree. Record includes the name of the asset that was deleted.

**Table 110:** Options that appear on the Asset tab

### Options that appear on the Policy tab

Table 111 describes the options that appear on the Policy tab of the Auditing Setup window.

This option...	Adds a record to the Audit log when the following occurs...
Create New Policy	User creates new policy in the repository. Record includes the name of the new policy.
Update Policy	User updates policy. Record includes the name of the policy that was updated.
Delete Policy	User deletes a policy. Record includes the name of the site policy that was deleted.
Create New Policy Version	User edits a policy to create a new version. Record includes the name of the policy that was edited.
Delete Policy Version	User deletes a version of a policy. Record includes the name of the policy and the version that was deleted.
Update Shared Object Policy	User edits a Shared Object policy. Record includes the name of the Shared Object that was updated.
Derive New Site Response	User derives a new site response. Record includes the name of the site response and the policy it was applied to.
Update Site Response	User updates a site response. Record includes the name of the site response and the policy it was applied to.
Delete Site Response	User deletes a site response. Record includes the name of the site response and the policy it was applied to.

**Table 111:** Options that appear on the Policy tab

<b>This option...</b>	<b>Adds a record to the Audit log when the following occurs...</b>
Manage Session Properties	User updates the Manage Session Properties window. Record includes the session name and the property that was updated.
Manage Global Responses	User updates global responses. Record includes the response name.
Update Group Policy	User updates a group policy. Record includes the name of the group policy and the policy that it was applied to.
Apply Policy To Group	User applies policy to group. Record includes the policy name and the group the policy that it was applied to.
Remove Policy Deploy on Group	User removes deployment of a policy to a group. Record includes the policy name and the group the deployment was removed from.
Update Agent Policy	User updates an agent policy. Record includes the policy name and the agent name.
Apply Policy on Agent	User applies agent policy. Record includes the policy name and the agent the policy was applied to.
Remove Policy Deploy on Agent	User removes deployment of a policy to an agent. Record includes the policy name and the agent the deployment was removed from.
Update Policy Deployment Objects Policy	User updates a Policy Deployment Object. Record includes the name of the Policy Deployment Object that was updated.
Apply Policy Deployment Objects Policy	User applies a Policy Deployment Object. Record includes the name of the Policy Deployment Object that was applied.
Create New Policy Repository	User creates a new policy repository in the Policy view. Record includes the name of the repository that was created.
Delete Policy Repository	User deletes a policy repository in the Policy view. Record includes the repository name that was deleted.
Merge Repositories	User merges a policy repository into its parent repository. Record includes the repository name that was merged and the repository it was merged into.

**Table 111:** *Options that appear on the Policy tab (Continued)*

### Options that appear on the User Group tab

Table 112 describes the options that appear on the User Group tab of the Auditing Setup window.

<b>This option...</b>	<b>Adds a record to the Audit log when the following occurs...</b>
Add New User Group	User adds a user group. Record includes the name of the user group that was added.
Update User Group	User updates user group. Record includes the name of the user group that was updated.
Delete User Group	User deletes user group. Record includes the name of the user group that was deleted.
Add User Group Member	User adds a member to a user group. Record includes the member name and the user group.

**Table 112:** *Options that appear on the User Group tab*

This option...	Adds a record to the Audit log when the following occurs...
Delete User Group Member	User deletes a member of a user group. Record includes the name of the member and the user group.

**Table 112:** Options that appear on the User Group tab

**Options that appear on the License tab**

Table 113 describes the options that appear on the License tab of the Auditing Setup window.

This option...	Adds a record to the Audit log when the following occurs...
Add License	User adds a license. Record includes the name of the license that was added.
Delete License	User deletes license. Record includes the name of the license that was updated.
Add OneTrust Token	User adds OneTrust Token. Record includes the name of the token that was added.
Delete OneTrust Token	User deletes OneTrust Token. Record includes the name of the OneTrust Token that was deleted.
Update OneTrust Token	User updates OneTrust Token. Record includes the name of the OneTrust Token.
Import OneTrust Token	User deletes a member of a user group. Record includes the name of the OneTrust Token that was updated.
Export OneTrust Token	User exports a OneTrust Token. Record includes the name of the token that was exported.
Import OneTrust Entitlement	User imports a OneTrust Token. Record includes the name of the token that was imported.
Export OneTrust Entitlement	User exports a OneTrust Entitlement. Record includes the name of the entitlement.
Automatic Download OneTrust Entitlement	User updates the document OneTrust Entitlement. Record includes the name of the entitlement.
Automatic Download Flag Set on OneTrust Entitlement	User sets the automatic download flag.
Automatic Download Interval Set on OneTrust Entitlement	User sets the Automatic Download Interval. Record includes the interval that was selected.
OnDemand Services Login	User logs in to the MSS server using their MSS account credentials to configure OnDemand Services. Record includes location of console from which the login took place, OnDemand Services user, and SiteProtector system user.

**Table 113:** Options that appear on the License tab



**Options that appear on the Analysis tab** Table 114 describes the options that appear on the Analysis tab of the Auditing Setup window.

This option...	Adds a record to the Audit log when the following occurs:
Clear Events	User clears events in the Analysis view.
Schedule Export Analysis Data	User schedules the export of analysis data.
Manage Incidents and/or Exceptions	User edits the options on the Manage Incidents and/or Exceptions window. Record includes the name of the incident or exception that was edited and the option that was changed.

**Table 114:** *Options that appear on the Analysis tab*

**Options that appear on the Notification tab** Table 115 describes the options that appear on the Notification tab of the Auditing Setup window.

This option...	Adds a record to the Audit log when the following occurs:
Delete Notification	User deletes a Notification.
Configure E-mail Notifications	User configures an e-mail Notification.

**Table 115:** *Options that appear on the Notification tab*

**Options that appear on the Health tab** Table 116 describes the options that appear on the Health tab of the Auditing Setup window.

This option...	Adds a record to the Audit log when the following occurs:
Configure Health Check Thresholds	User does one of the following: <ul style="list-style-type: none"> <li>● Changes the thresholds for a System Health check</li> <li>● Selects Ignore Health Status for a System Health check</li> <li>● Selects Enable Health Status for a System Health check</li> </ul>

**Table 116:** *Options that appear on the Health tab*

**Options that appear on the Report tab**

Table 117 describes the options that appear on the Report tab of the Auditing Setup window.

<b>This option...</b>	<b>Adds a record to the Audit log when the following occurs:</b>
Add New Report	User creates a report on the Reports tab. Record includes the name of the report and the report type.
Update Report Job	User edits a report job. Record includes the report name, the job name, the report type, and scheduling information.
View Report	User views a report on the Report tab. Record includes the name of the report and the report type.
Delete Reports	User deletes a report on the Report tab. Record includes the report name and the report type.

**Table 117:** *Options that appear on the Report tab*

**Options that appear on the Ticketing tab**

Table describes the options that appear on the Ticketing tab of the Auditing Setup window.

<b>This option...</b>	<b>Adds a record to the Audit log when the following occurs:</b>
Create New Ticket	User creates a ticket on the Ticket tab. Record includes the ticket name.
Update Ticket	User updates a ticket. Record includes the ticket name.
Create New Auto Ticketing Rule	User adds an auto ticket rule for a group. Record includes the rule addition ID and the user who created the rule.
Update Auto Ticketing Rule	User modifies an auto ticket rule for a group. Record includes the rule modification ID and the user who created the rule.
Delete Auto Ticketing Rule	User deletes an auto ticket rule for a group. Record includes the rule deletion ID and the user who deleted the rule.
Update Ticketing Setup	User views a report on the Report tab. Record includes the name of the report and the report type.

*Options that appear on the Ticketing tab*

---

# Configuring the SiteProtector System to Log Actions

**Introduction** This topic provides the procedure for configuring audit options in the SiteProtector system.

**Procedure** To configure the SiteProtector system to log actions:

1. Open the Console, and then select **Tools**→**Auditing Setup**.  
The Auditing Setup window appears.
2. Select the audit category you want to open from the left pane, and then do one of the following:
  - Select one or more of the actions listed.
  - Select the **Select All** box to enable all actions in this category.
3. Click **OK**.



# Troubleshooting



## Chapter 25

# Troubleshooting

## Overview

### Introduction

This chapter provides descriptions and solutions for some of the issues you may encounter as you work with the SiteProtector system. It is not intended to represent a complete list of potential SiteProtector system issues.

### Knowledgebase and IBM ISS Customer Support

For the most complete and up-to-date list of SiteProtector system issues, see the IBM ISS Knowledgebase at <http://www.iss.net/support/knowledgebase/>. If the Knowledgebase does not help you resolve your issue, contact IBM ISS Customer Support.

### In this chapter

This chapter contains the following topics:

Topic	Page
Issues Related to Agents and Components	344
Issues Related to Operating a SiteProtector System	351
Issues Related to Reporting Module	353
Issues Related to Low Memory	354
Issues Related to Configuring and Updating the SiteProtector System	355

## Issues Related to Agents and Components

**Introduction** This topic provides solutions to issues that you might encounter when setting up agents.

### Unknown System Scanner vulnerability assessment application status

**Description:** The SiteProtector system shows the status of System Scanner vulnerability assessment application as *Unknown*. The correct status for System Scanner vulnerability assessment application is *Not Managed* because you cannot manage these agents in the SiteProtector system.

**Solution:** To return the System Scanner agent to *Not Managed* status, restart the SiteProtector system Application Server service.

### Agent/SiteProtector system communication failure

**Description:** Network Sensor or Server Sensor fails to communicate with the SiteProtector system on a system where a System Scanner Databridge is also installed. If you installed a databridge before you installed Network Sensor or Server Sensor, then the agents cannot communicate with the SiteProtector system. The event log creates the following message when the SiteProtector system attempts to communicate with these agents:

```
ns60_computername_w2k) - OnError from 172.16.3.69: The currently selected provider does not support the requested cryptographic algorithm at the selected strength/length. [ID=0xc7280003]
```

**Solution:** Install Network Sensor and Server Sensor before you install the System Scanner Databridge. If you have already installed the System Scanner Databridge, remove it, and then reinstall it.

### Error when downloading agent logs

**Description:** The SiteProtector system issues the following error message when you attempt to download logs on a Network Sensor that is running on a Unix operating system:

```
Get files failed on Sensor #<sensor number>. 0 of 1 files transferred.
Get file <file name> failed. The current session user does not have
permission to perform the specified operation on the specified path.
Please edit the access control file on the remote server and add the
necessary permissions for the session. This problem is due to an incorrect
permission contained in the iss.access file of the sensor's daemon.
```

**Note:** The error message may also appear for Server Sensor.

**Solution:** Correct this issue as follows:

1. Access the iss.access file in the issDaemon folder, and then modify the following sections in the file:

**Note:** The following text is an example. The path on your computer may be slightly different.

<b>Before edit</b>	<pre>[/opt/ISS/issSensors/network_sensor_1/Logs/]; ACL1 =S Role=Default FilePerms=RD DirPerms=R;</pre>
<b>After edit</b>	<pre>[/opt/ISS/issSensors/network_sensor_1/Logs/]; ACL1 =S Role=Default FilePerms=RD DirPerms=R Recursive;</pre>

2. Stop, and then restart the issDaemon service.



<b>Network Sensor: keys not automatically distributed</b>	<p><b>Description:</b> The following message appears under the <b>EC Public Keys sent</b> row when you click <b>Details</b> for Solaris RealSecure Network 7.0.</p> <p>EC Public Keys sent: No - Error checking encryption algorithms on sensor, RSA is not supported. No encryption key(include directory) found on sensor.</p> <p>This message indicates that the encryption key exchange between the SiteProtector system and the Solaris RealSecure Network 7.0 is not functioning. This issue also causes the RealSecure Network to display a status of <b>Offline</b>. To fix the issue, you must manually send the keys from the SiteProtector system to the RealSecure Network agent.</p> <p><b>Solution:</b> Manually distribute the keys. See “Manually Distributing Keys” on page 282.</p>
<b>Deleted or expired Event Collector password</b>	<p><b>Description:</b> The Event Collector username/password was deleted, changed, or has expired. The Event Collector cannot communicate with the Site Database.</p> <p><b>Solution:</b> Reset the Event Collector password. See “Resetting Component Passwords” on page 246.</p>
<b>Deleted or expired Application Server password</b>	<p><b>Description:</b> The Application Server service fails to start.</p> <p><b>Solution:</b> Reset the Application Server password. See “Resetting Component Passwords” on page 246.</p>
<b>Deleted or expired Agent Manager password</b>	<p><b>Description:</b> The Agent Manager service fails to start.</p> <p><b>Solution:</b> Reset the Agent Manager password. See “Resetting Component Passwords” on page 246.</p>
<b>Unknown or Not Responding agent status</b>	<p><b>Description:</b> The agent status is <i>Unknown</i> or <i>Not Responding</i>.</p> <p><b>Solution:</b> Verify that all the required encryption keys are present on the agent computer. See “Distributing Keys to SiteProtector System Components” on page 250.</p>
<b>Inaccessible file structure and application registry– Windows 2000 OS</b>	<p><b>Description:</b> When you install the SiteProtector system Console, the file structure and the application registry may not be accessible for some users and groups that have limited access privileges.</p> <p><b>Solution:</b> To change SiteProtector system Console access permission on the Windows 2000 operating system:</p> <ol style="list-style-type: none"> <li>1. Open Windows Explorer.</li> <li>2. Navigate to the location where the SiteProtector system Console is installed. The default location is: <code>\Program Files\ISS\SiteProtector\Console</code></li> <li>3. Right-click the <b>Console</b> folder, and then select <b>Properties</b>. The folder’s properties window appears.</li> <li>4. Select the <b>Security</b> tab.</li> <li>5. Click <b>Add</b>.</li> </ol>

The Select Users, Computers, or Groups window appears.

6. Select the users and/or groups for which you want to add permissions, and then click **Add**.
7. Click **OK**.

The Select Users, Computers, or Groups window closes.

8. Select each user and/or group you added, and then ensure that they have, at least, the following permissions:

For file folders:

- Modify
- Read & Execute
- List Folder Contents
- Read
- Write

9. Click **Apply**, and then click **OK**.
10. Run the registry editor program, `regedt32.exe`.
11. Select the window titled **HKEY\_LOCAL\_MACHINE on Local Machine**, and then follow the steps in the table to set the permissions:

Navigate to this path...	then follow these steps...
HKEY_LOCAL_MACHINE\Software\ISS\SiteProtector\Console	<ol style="list-style-type: none"> <li>1. After navigating to the path, click the Console folder.</li> <li>2. Select <b>Security</b> → <b>Permissions</b>. The Permissions for Console window appears.</li> <li>3. Click <b>Add</b>. The Select Users or Groups window appears.</li> <li>4. Enter the account names for which you want to add permissions. <b>Note:</b> You can select <b>Check Names</b> to verify names.</li> <li>5. Click <b>OK</b>. The Select Users or Groups window closes.</li> <li>6. Check the permissions for each user. <b>Important:</b> You must set Read Permissions for this registry key.</li> <li>7. Click <b>OK</b> to complete the operation. The Permissions for Console window closes.</li> </ol>

Navigate to this path...	then follow these steps...
<p>HKEY_LOCAL_MACHINE\Software\ISS\JRE1.6.0_03</p>	<ol style="list-style-type: none"> <li>1. After navigating to the path, click the JRE1.6.0_03 folder.</li> <li>2. Select <b>Security</b> → <b>Permissions</b>. The Permissions for JRE1.6.0_03 window appears.</li> <li>3. Click <b>Add</b>. The Select Users or Groups window appears.</li> <li>4. Enter the account names for which you want to add permissions. <b>Note:</b> You can select <b>Check Names</b> to verify names.</li> <li>5. Click <b>OK</b>. The Select Users or Groups window closes.</li> <li>6. Check the permissions for each user. <b>Important:</b> You must set Read Permissions for this registry key.</li> <li>7. Click <b>OK</b> to complete the operation. The Permissions for JRE1.6.0_03 window closes.</li> </ol>
<p>HKEY_LOCAL_MACHINE\Software\ISS\RealSecure</p>	<ol style="list-style-type: none"> <li>1. After navigating to the path, click the RealSecure folder.</li> <li>2. Select <b>Security</b> → <b>Permissions</b>. The Permissions for RealSecure window appears.</li> <li>3. Click <b>Add</b>. The Select Users or Groups window appears.</li> <li>4. Enter the account names for which you want to add permissions. <b>Note:</b> You can select <b>Check Names</b> to verify names.</li> <li>5. Click <b>OK</b>. The Select Users or Groups window closes.</li> <li>6. Check the permissions for each user. <b>Important:</b> You must set Read Permissions for this registry key.</li> <li>7. Click <b>OK</b> to complete the operation. The Permissions for RealSecure window closes.</li> </ol>

Navigate to this path...	then follow these steps...
HKEY_LOCAL_MACHINE\Software\ISS\RealSecure\6.5\nPolicyEditor	<ol style="list-style-type: none"> <li>1. After navigating to the path, click the PolicyEditor folder.</li> <li>2. Select <b>Security</b> → <b>Permissions</b>. The Permissions for PolicyEditor window appears.</li> <li>3. Click <b>Add</b>. The Select Users or Groups window appears.</li> <li>4. Enter the account names for which you want to add permissions. <b>Note:</b> You can select <b>Check Names</b> to verify names.</li> <li>5. Click <b>OK</b>. The Select Users or Groups window closes.</li> <li>6. Check the permissions for each user. <b>Important:</b> You must set Read and Full Control Permissions for this registry key.</li> <li>7. Click <b>OK</b> to complete the operation. The Permissions for PolicyEditor window closes.</li> </ol>

**Inaccessible file structure and application registry—Windows 2003 or XP Operating Systems**

**Description:** When you install the SiteProtector system Console on the Windows 2003 or XP operating system, the file structure and the application registry may not be accessible for some users and groups that have limited access privileges.

To change SiteProtector system Console access permission on the Windows 2003 and XP operating system:

1. Open Windows Explorer.
2. Navigate to the location where the SiteProtector system Console is installed.  
The default location is:  
`\Program Files\ISS\SiteProtector\Console`
3. Right-click the **Console** folder, and then select **Properties**.  
The folder’s properties window appears.
4. Select the **Security** tab.
5. Click **Add**.  
The Select Users or Groups window appears.
6. Type in the names of the users and/or groups for which you want to add permissions, and then click **OK**.  
The Select Users or Groups window closes.
7. Select each user and/or group you added, and then ensure that they have, at least, the following permissions:  
For file folders:
  - Modify
  - Read & Execute
  - List Folder Contents
  - Read

■ Write

8. Click **Apply**, and then click **OK**.
9. Run the registry editor program, `regedit.exe`.

The Registry Editor window appears.

10. Select **HKEY\_LOCAL\_MACHINE on Local Machine**, and then follow the steps in the table to set the permissions:

Navigate to this path...	then follow these steps...
<p>HKEY_LOCAL_MACHINE\Software\ISS\SiteProtector\Console</p>	<ol style="list-style-type: none"> <li>1. After navigating to the path, right-click the Console folder, and then select <b>Permissions</b>. The Permissions for Console window appears.</li> <li>2. Click <b>Add</b>. The Select Users or Groups window appears.</li> <li>3. Enter the account names for which you want to add permissions. <b>Note:</b> You can select <b>Check Names</b> to verify names.</li> <li>4. Click <b>OK</b>. The Select Users or Groups window closes.</li> <li>5. Check the permissions for each user. <b>Important:</b> You must set Read Permissions for this registry key.</li> <li>6. Click <b>OK</b> to complete the operation. The Permissions for Console window closes.</li> </ol>
<p>HKEY_LOCAL_MACHINE\Software\ISS\JRE1.6.0_03</p>	<ol style="list-style-type: none"> <li>1. After navigating to the path, right-click JRE1.6.0_03 folder, and then select <b>Permissions</b>. The Permissions for JRE1.6.0_03 window appears.</li> <li>2. Click <b>Add</b>. The Select Users or Groups window appears.</li> <li>3. Enter the account names for which you want to add permissions. <b>Note:</b> You can select <b>Check Names</b> to verify names.</li> <li>4. Click <b>OK</b>. The Select Users or Groups window closes.</li> <li>5. Check the permissions for each user. <b>Important:</b> You must set Read Permissions for this registry key.</li> <li>6. Click <b>OK</b> to complete the operation. The Permissions for JRE1.6.0_03 window closes.</li> </ol>

Navigate to this path...	then follow these steps...
<p>HKEY_LOCAL_MACHINE\Software\ISS\RealSecure</p>	<ol style="list-style-type: none"> <li>1. After navigating to the path, right-click the RealSecure folder, and then select <b>Permissions</b>. The Permissions for RealSecure window appears.</li> <li>2. Click <b>Add</b>. The Select Users or Groups window appears.</li> <li>3. Enter the account names for which you want to add permissions. <b>Note:</b> You can select <b>Check Names</b> to verify names.</li> <li>4. Click <b>OK</b>. The Select Users or Groups window closes.</li> <li>5. Check the permissions for each user. <b>Important:</b> You must set Read Permissions for this registry key.</li> <li>6. Click <b>OK</b> to complete the operation. The Permissions for RealSecure window closes.</li> </ol>
<p>HKEY_LOCAL_MACHINE\Software\ISS\RealSecure\6.5\PolicyEditor</p>	<ol style="list-style-type: none"> <li>1. After navigating to the path, right-click the PolicyEditor folder, and then select <b>Permissions</b>. The Permissions for PolicyEditor window appears.</li> <li>2. Click <b>Add</b>. The Select Users, Computers, or Groups window appears.</li> <li>3. Enter the account names for which you want to add permissions. <b>Note:</b> You can select <b>Check Names</b> to verify names.</li> <li>4. Click <b>OK</b>. The Select Users or Groups window closes.</li> <li>5. Check the permissions for each user. <b>Important:</b> You must set Read and Full Control Permissions for this registry key.</li> <li>6. Click <b>OK</b> to complete the operation. The Permissions for PolicyEditor window closes.</li> </ol>

---

# Issues Related to Operating a SiteProtector System

**Introduction** This topic provides solutions to issues that you might encounter as you are operating the SiteProtector system.

## Cannot log on to the SiteProtector system

**Description:** When you attempt to connect to a Site, the SiteProtector system displays a Certificate Incompatibility message.

**Explanation:** The Certificate Incompatibility message appears when you try to connect to the server, but the certificate validation process determines a discrepancy in the certificate assigned to the server.

**Solution:** Record the information displayed in the Certificate Incompatibility message and contact your System Administrator to determine if the certificates have been updated.

- If your System Administrator confirms that they have updated the certificates, click **Valid**. The newly updated certificate will replace the previous certificate in the key store for that server.
- If your System Administrator verifies that they have *not* updated certificates, then click **Invalid**. The System Administrator should then contact IBM ISS Technical Support for assistance.

**Note:** The purpose of certificates is to alert you to attacks. Accepting an unknown certificate could make you vulnerable to attacks.

## Computer absent from Active Directory

**Description:** Your computer appears in a domain and the DNS, but it does not appear in the Active Directory grouping tree.

**Solution:** Your computer may not have an assigned DNS Server name in the Active Directory object. If this is the case, then the SiteProtector system cannot resolve a name for your computer.

To verify that your computer has an assigned DNS name:

1. On the Domain Controller computer, access Administrative Tools.
2. Select **Active Directory Users and Computer**.
3. In the left pane, locate the computer that does not appear in the Active Directory listing.
4. Right-click the computer name, and then select **Properties**.  
The *Computer\_Name* **Properties** window appears.
5. Does the full DNS name appear in the **DNS name** box?
  - If *yes*, then call IBM ISS Technical Support to help you with this issue.
  - If *no*, then go to the next step.
6. Go to the computer that does not appear in the Active Directory listing.
7. Right-click My Computer, and then select **Properties**.  
The System Properties window appears.
8. Manually change the **Full computer name** in System Properties to reflect the complete name of the computer.

**Note:** The procedure to change the name that appears in the **Full computer name** field depends on your operating system version. See your operating system documentation for information about how to change your computer name.



---

## Issues Related to Reporting Module

### Introduction

This topic provides descriptions and solutions for some of the issues you may encounter while working with the reporting module.

### Cannot view a report

**Description:** The SiteProtector system displays the following error when you try to view a report:

The requested URL could not be retrieved.

This error can occur when you log on to the SiteProtector system Console using a Netbios computer name, but your Internet Explorer application cannot resolve by Netbios name. Your Internet Explorer application may be set to use a proxy, but the proxy server is not configured to resolve the Netbios address.

**Solution:** Log out of the SiteProtector system Console, and then log on using either the fully qualified domain name (FQDN) or the IP address of the SiteProtector system application server.

## Issues Related to Low Memory

### Introduction

This topic provides descriptions and solutions for some of the issues you may encounter due to a lack of memory on your SiteProtector system.

### Importing a large application list

**Description:** If you import an application list containing more than 8000 entries into the global application list or into a policy, then an out of memory error can appear when you attempt to edit the global application list.

**Solution:** Perform the following procedure:

1. Click **Start** on the taskbar, and then select **Run**.

The Run window appears.

2. Type `regedit` in the **Open** box.

The Registry Editor application appears.

3. In the left pane, navigate the following path:

`HKEY_LOCAL_MACHINE\SOFTWARE\ISS\CPE\Parameters`

4. Edit the string value for `MaxHeap` to reflect the following:

`-Xmx<size in megabytes>M`

**Note:** IBM ISS recommends that you start with a value of 128, and then increase the value, if necessary, until the application runs. For example, type `-Xmx128M` to set the heap size to 128 megabytes.

### Multiple console connections

**Description:** Your SiteProtector system may generate an "out of memory" error on the Application Server if any of the following occur:

- Multiple Consoles are simultaneously retrieving asset information from a Site.
- You have increased the default value for the maximum number of rows that The SiteProtector system displays.
- You are running very large, scheduled reports.

**Note:** This is also applicable to the SiteProtector system Web Portal.

**Solution:** Perform the following procedure:

1. On the application server, click **Start** on the taskbar, and then select **Run**.

The Run window appears.

2. Type `regedit` in the **Open** box.

The Registry Editor application appears.

3. In the left pane, navigate the following path:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\issSPAppService\Parameters`

4. Edit the string value for `MaxHeap` to reflect the following:

`-Xmx<size in megabytes>M`

**Note:** IBM ISS recommends that you start with a value of 384, and then increase the value, if necessary, until the application runs. For example, type `-Xmx384M` to set the heap size to 384 megabytes.

# Issues Related to Configuring and Updating the SiteProtector System

- Introduction** This topic provides descriptions and solutions for some of the issues you may encounter when updating your SiteProtector system.
- Missing or invalid license key errors**
- Description:** After you add a license, the features do not appear, and errors related to a missing or invalid license appear.
- Solution:** The Sensor Controller polls for license changes every 60 seconds, so the change may not appear immediately.
- Press the F5 key to refresh the licensing information. You can also wait 60 seconds, and then re-open the Add License window to see if the feature columns are populated. If the feature columns are populated, the license key has been successfully imported.
- SQL Agent not running**
- Description:** If the SQL Server Agent is not running on the SQL server that hosts the SiteProtector system database, the updates will fail.
- Solution:** Restart the SQL Server Agent, and then try to apply the update again.
- Job ownership**
- Description:** If SiteProtector system jobs are not owned by a user with the proper privileges, you may not be able to apply updates to your SiteProtector system database.
- Solution:**
- Make IssApp the owner of these jobs:
    - Check Sensor Controller in RealSecureDB
    - Load Sensor Data and Post Process in RealSecureDB
  - Make a user with the sysadmin system role owner of these jobs:
    - Database Configuration Manager in RealSecureDB
    - Automated Maintenance in RealSecureDB
    - Maintain DB Health in RealSecureDB
  - Apply the update.
- Missing license files**
- Description:** When trying to download update files, you receive one of the following error messages regarding missing license files:
- Update file upload cancelled at user request.
  - Sensor controller unable to automatically obtain file ( Warning: Not having a valid license, precludes downloading XPU. Prompting for valid XPU file on your system. [ID=0xc7420051] )
  - There are no appropriate licenses in SiteProtector to satisfy export requirements. You will not be able to obtain X-Press Updates for SiteProtector. Please contact our worldwide IBM ISS Licensing personnel at licenses@iss.net.
- Solution:** Add a valid license. See “Setting Up Licenses” on page 49.



# Index

## a

- Active Directory
  - creating groups with 308
  - missing computer 351
- Additional SiteProtector Modules 18
- Agent Manager
  - assigning agents to 70
  - creating accounts 69
  - resetting passwords 247
- Agent Manager accounts 69
- agents
  - assigning Agent Managers to 70
  - assigning Event Collectors to 123
- Analysis view
  - setting data update options 47
- Asset Event Details report 326
- Asset Event Summary report 326
- Asset table 297
- Asset view
  - setting default view options 44
- assets
  - adding to groups 225, 301, 303, 311
  - organizing 223
- Attack Incidents report 328
- Attack Status Summary report 328
- Attack Trend report 328
- Attacks by Group report 326
- authentication
  - two-factor 39
- automatic grouping of assets 225
- Auto-Refresh
  - turning on and off 30

## c

- compliance and summary reports
  - descriptions 325
- components
  - illus* 14
- configuration
  - illus* 14

## d

- daily frequency parameter, Event Collector failover 125
- Debug messages
  - turn on in logs 32
- Default view in Console
  - setting 30
- Desktop
  - installing 270
- Desktop agents
  - assigning to a Desktop Controller 70
- discovery scans
  - host information generated 311
  - running 311
- documentation
  - controlling storage and access 33
  - SiteProtector Help 10
  - SiteProtector Installation Guide 10
  - SiteProtector Supported Agents and Appliances 10
  - SiteProtector System Requirements 10
  - SiteProtector User Guide for Security Managers 9

## e

- Error messages
  - turn on in logs 32
- Event Collector
  - resetting passwords 247
- Event Collectors
  - assigning agents to 123
  - daily frequency parameter 125
  - WAITFORDELAY parameter 125
- event logging, enabling 129
- Event Viewer
  - setting up 129

## f

- Fatal messages
  - turn on in logs 32

## g

- Grid lines

- turning on and off 30
- groups
  - adding assets to 225, 303, 308
  - automatic grouping of assets 225
  - creating 301
  - organizing 223
  - System Scanner 228

## **h**

- Help, SiteProtector, content of 10
- Host Assessment Detail report 325
- Host Assessment Summary report 325

## **i**

- IBM Internet Security Systems
  - technical support 11
  - Web site 11
- IBM ISS Technical Support 11
- Info messages
  - turn on in logs 32
- Installation Guide, content of 10

## **l**

- Log level
  - setting 32
- Log output
  - choosing format 32
- logging options 35–39

## **o**

- Operating System Summary by Host report 325
- Operating System Summary report 325

## **p**

- password maintenance utilities 246
  - Agent Manager utility 246
  - Event Collector utility 246
  - SecurityFusion module utility 246

## **r**

- Recursion
  - turning on and off 30
- Refresh interval

- setting 30
- removing an update 291
- Reporting Module
  - description of 18
- Reporting tab
  - compliance and summary reports 325
  - creating a report 329
  - summary and compliance reports 325
  - viewing a report 329
- reports
  - compliance and summary 325
  - creating 322
  - summary and compliance 325
- reports, by category
  - assessment
    - Host Assessment Detail 325
    - Host Assessment Summary 325
    - Operating System Summary 325
    - Operating System Summary by Host 325
    - Service Summary 325
    - Service Summary by Host 325
    - Top Vulnerabilities 325
    - Vulnerabilities by Group 326
    - Vulnerabilities by Host 326
    - Vulnerability by OS 326
    - Vulnerability Counts 326
    - Vulnerability Counts by Host 326
    - Vulnerability Detail by Host 326
    - Vulnerability Names by Host 326
    - Vulnerability Remedies by Host 326
    - Vulnerability Summary by Host 326
- asset
  - Asset Event Details 326
  - Asset Event Summary 326
- attack activity
  - Attacks by Group 326
  - Top Attacks 327
  - Top Sources of Attack 327
  - Top Targets of Attack 327
- audit activity 327
- content filtering
  - Top Web Categories 327
  - Web Requests 327
- management
  - Attack Incidents 328
  - Attack Status Summary 328
  - Attack Trend 328
  - Virus Activity Trend 328
  - Vulnerability Trend 328
- ticketing
  - Ticket Summary 328
  - Ticket Time Tracking 328
- virus activity
  - Top Virus Activity 328

- Virus Activity by Group 328
- resetting component passwords
  - Agent Manager 247
  - Event Collector 247
  - SecurityFusion module 248
  - tools for 246
- roles, installation requirements 161
- Rows displayed
  - setting 30

## S

- scans
  - asset discovery, for 311
- secondary Event Collector, configuring 125
- SecureSync
  - description of 18
- security documentation
  - storing and accessing locally 33
- SecurityFusion Module
  - resetting passwords 248
- SecurityFusion module
  - description of 18
- sensors
  - downloading new 271
- Service Summary by Host report 325
- Service Summary report 325
- Site database
  - Asset table 297
- Site servers, assets, as 297
- SiteProtector
  - add-on modules 18
  - architecture of 14
  - communication channels used in 14
  - components of 15
  - description of 14
  - setup process 19–20
  - stages of setup process 20
- SiteProtector components
  - descriptions of 15
- SiteProtector Policies and Responses Configuration Guide 10
- SiteProtector setup process
  - agent setup stage 258
  - checklist for configuring and updating 27
  - configuration and updates stage 26
  - group setup stage 212
- Summary view
  - changing information displayed on 42

- information displayed on 40
- Supported Agents and Appliances, address of 10
- System Requirements, address of 10
- System Scanner
  - group 228

## t

- technical support, IBM Internet Security Systems 11
- Third-Party Module
  - description of 18
- Ticket Summary report 328
- Ticket Time Tracking report 328
- Time format
  - setting 30
- Time zone
  - setting 30
- Top Attacks report 327
- Top Sources of Attack report 327
- Top Targets of Attack report 327
- Top Virus Activity report 328
- Top Vulnerabilities report 325
- Top Web Categories report 327
- two-factor authentication 39

## u

- updates, *See* XPUs
- user accounts
  - for SiteProtector components 246
- user roles
  - Security Manager tasks, for 10

## v

- Virus Activity by Group report 328
- Virus Activity Trend report 328
- Vulnerabilities by Group report 326
- Vulnerabilities by Host report 326
- Vulnerability by OS report 326
- Vulnerability Counts by Host report 326
- Vulnerability Counts report 326
- Vulnerability Detail by Host report 326
- Vulnerability Names by Host report 326
- Vulnerability Remedies by Host report 326
- Vulnerability Summary by Host report 326
- Vulnerability Trend report 328

## W

WAITFORDELAY parameter, Event Collector  
    failover 125

Warning messages  
    turn on in logs 32

Web Requests report 327

Web site, IBM Internet Security Systems 11

## X

X-Press Updates, *See* XPU

XPU  
    removing an update 291